Internet Engineering Task Force (IETF)
Request for Comments: 7105
Category: Standards Track
ISSN: 2070-1721

M. Thomson
Mozilla
J. Winterbottom
Unaffiliated

January 2014

Using Device-Provided Location-Related Measurements in Location Configuration Protocols

Abstract

This document describes a protocol for a Device to provide location-related measurement data to a Location Information Server (LIS) within a request for location information. Location-related measurement information provides observations concerning properties related to the position of a Device; this information could be data about network attachment or about the physical environment. A LIS is able to use the location-related measurement data to improve the accuracy of the location estimate it provides to the Device. A basic set of location-related measurements are defined, including common modes of network attachment as well as assisted Global Navigation Satellite System (GNSS) parameters.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7105.

Table of Contents

1. Introduction

A Location Configuration Protocol (LCP) provides a means for a Device to request information about its physical location from an access network. A Location Information Server (LIS) is the server that provides location information that is available due to the knowledge it has about the network and physical environment.

As a part of the access network, the LIS is able to acquire measurement results related to Device location from network elements. The LIS also has access to information about the network topology that can be used to turn measurement data into location information. This information can be further enhanced with information acquired from the Device itself.

A Device is able to make observations about its network attachment, or its physical environment. The location-related measurement data might be unavailable to the LIS; alternatively, the LIS might be able to acquire the data, but at a higher cost in terms of time or some other metric. Providing measurement data gives the LIS more options in determining location; this could in turn improve the quality of

the service provided by the LIS. Improvements in accuracy are one potential gain, but improved response times and lower error rates are also possible.

This document describes a means for a Device to report location-related measurement data to the LIS. Examples based on the HTTP-Enabled Location Delivery (HELD) [RFC5985] location configuration protocol are provided.

2. Conventions Used in This Document

The terms "LIS" and "Device" are used in this document in a manner consistent with the usage in [RFC5985].

This document also uses the following definitions:

Location Measurement: An observation about the physical properties of a particular Device's position in time and space. The result of a location measurement -- "location-related measurement data", or simply "measurement data" given sufficient context -- can be used to determine the location of a Device. Location-related measurement data does not directly identify a Device, though it could do so indirectly. Measurement data can change with time if the location of the Device also changes.

Location-related measurement data does not necessarily contain location information directly, but it can be used in combination with contextual knowledge and/or algorithms to derive location information. Examples of location-related measurement data are radio signal strength or timing measurements, Ethernet switch identifiers, and port identifiers.

Location-related measurement data can be considered sighting information, based on the definition in [RFC3693].

Location Estimate: An approximation of where the Device is located. Location estimates are derived from location measurements. Location estimates are subject to uncertainty, which arises from errors in measurement results.

GNSS: Global Navigation Satellite System. A satellite-based system that provides positioning and time information -- for example, the US Global Positioning System (GPS) or the European Galileo system.

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].

3. Location-Related Measurements in LCPs

This document defines a standard container for the conveyance of location-related measurement parameters in location configuration protocols. This is an XML container that identifies parameters by type and allows the Device to provide the results of any measurement it is able to perform. A set of measurement schemas are also defined that can be carried in the generic container.

A simple example of measurement data conveyance is illustrated by the example message in Figure 1. This shows a HELD location request message with an Ethernet switch and port measurement taken using the Link-Layer Discovery Protocol (LLDP) [IEEE.8021AB].

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <locationType exact="true">civic</locationType>
  <measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
        time="2008-04-29T14:33:58">
    <lldp xmlns="urn:ietf:params:xml:ns:geopriv:lm:lldp">
      <chassis type="4">0a01003c</chassis>
      <port type="6">c2</port>
    </lldp>
  </measurements>
</locationRequest>
```

Figure 1: HELD Location Request with Measurement Data

This LIS can ignore measurement data that it does not support or understand. The measurements defined in this document follow this rule: extensions that could result in backward incompatibility MUST be added as new measurement definitions rather than extensions to existing types.

Multiple sets of measurement data, either of the same type or from different sources, can be included in the "measurements" element. See Section 4.1.1 for details on repetition of this element.

A LIS can choose to use or ignore location-related measurement data in determining location, as long as rules regarding use and retention (Section 6) are respected. The "method" parameter in the Presence Information Data Format - Location Object (PIDF-LO) [RFC4119] SHOULD be adjusted to reflect the method used. A correct "method" can assist location recipients in assessing the quality (both accuracy and integrity) of location information, though there could be reasons to withhold information about the source of data.

Measurement data is typically only used to serve the request in which it is included. There may be exceptions, particularly with respect to location URIs. Section 6 provides more information on usage rules.

Location-related measurement data need not be provided exclusively by Devices. A third-party location requester (for example, see [RFC6155]) can request location information using measurement data, if the requester is able to acquire measurement data and authorized to distribute it. There are specific privacy considerations relating to the use of measurements by third parties, which are discussed in Section 6.4.

Location-related measurement data and its use present a number of privacy and security challenges. These are described in more detail in Sections 6 and 7.

4. Location-Related Measurement Data Types

A common container is defined for the expression of location measurement data, as well as a simple means of identifying specific types of measurement data for the purposes of requesting them.

The following example shows a measurement container with measurement time and expiration time included. A WiFi measurement is enclosed.

```
<lm:measurements xmlns:lm="urn:ietf:params:xml:ns:geopriv:lm"
          time="2008-04-29T14:33:58"
          expires="2008-04-29T17:33:58">
  <wifi xmlns="urn:ietf:params:xml:ns:geopriv:lm:wifi">
    <ap serving="true">
      <bssid>00-12-F0-A0-80-EF</bssid>
      <ssid>wlan-home</ssid>
    </ap>
  </wifi>
</lm:measurements>
```

Figure 2: Measurement Example

4.1. Measurement Container

The "measurements" element is used to encapsulate measurement data that is collected at a certain point in time. It contains time-based attributes that are common to all forms of measurement data, and it permits the inclusion of arbitrary measurement data. The elements that are included within the "measurements" element are generically referred to as "measurement elements".

This container can be added to a request for location information in any protocol capable of carrying XML, such as a HELD location request [RFC5985].

4.1.1. Time of Measurement

The "time" attribute records the time that the measurement or observation was made. This time can be different from the time that the measurement information was reported. Time information can be used to populate a timestamp on the location result or to determine if the measurement information is used.

The "time" attribute SHOULD be provided whenever possible. This allows a LIS to avoid selecting an arbitrary timestamp. Exceptions to this, where omitting time might make sense, include relatively static types of measurement (for instance, the DSL measurements in Section 5.6) or for legacy Devices that don't record time information (such as the Home Location Register/Home Subscriber Server for cellular).

The "time" attribute is attached to the root "measurement" element. Multiple measurements can often be given the same timestamp, even when the measurements were not actually taken at the same time (consider a set of measurements taken sequentially, where the difference in time between observations is not significant). Measurements cannot be grouped if they have different types or if there is a need for independent time values on each measurement. In these instances, multiple measurement sets are necessary.

4.1.2. Expiry Time on Location-Related Measurement Data

A Device is able to indicate an expiry time in the location measurement using the "expires" attribute. Nominally, this attribute indicates how long information is expected to be valid, but it can also indicate a time limit on the retention and use of the measurement data. A Device can use this attribute to request that the LIS not retain measurement data beyond the indicated time.

> Note: Movement of the Device might result in the measurement data being invalidated before the expiry time.

A Device is advised to set the "expires" attribute to the earlier of the time that measurements are likely to be unusable and the time that it desires to have measurements discarded by the LIS. A Device that does not desire measurement data to be retained can omit the "expires" attribute. Section 6 describes more specific rules regarding measurement data retention.

4.2. RMS Error and Number of Samples

Often a measurement is taken more than once. Reporting the average of a number of measurement results mitigates the effects of random errors that occur in the measurement process.

Reporting each measurement individually can be the most effective method of reporting multiple measurements. This is achieved by providing multiple measurement elements for different times.

The alternative is to aggregate multiple measurements and report a mean value across the set of measurements. Additional information about the distribution of the results can be useful in determining location uncertainty.

Two attributes are provided for use on some measurement values:

rmsError: The root-mean-squared (RMS) error of the set of measurement values used in calculating the result. RMS error is expressed in the same units as the measurement, unless otherwise stated. If an accurate value for the RMS error is not known, this value can be used to indicate an upper bound or estimate for the RMS error.

samples: The number of samples that were taken in determining the measurement value. If omitted, this value can be assumed to be large enough that the RMS error is an indication of the standard deviation of the sample set.

For some measurement techniques, measurement error is largely dependent on the measurement technique employed. In these cases, measurement error is largely a product of the measurement technique and not the specific circumstances, so the RMS error does not need to be actively measured. A fixed value MAY be provided for the RMS error where appropriate.

The "rmsError" and "samples" elements are added as attributes of specific measurement data types.

4.2.1. Time RMS Error

Measurement of time can be significant in certain circumstances. The GNSS measurements included in this document are one such case where a small error in time can result in a large error in location. Factors such as clock drift and errors in time synchronization can result in small, but significant, time errors. Including an indication of the quality of time measurements can be helpful.

A "timeError" attribute MAY be added to the "measurement" element to indicate the RMS error in time. "timeError" indicates an upper bound on the time RMS error in seconds.

The "timeError" attribute does not apply where multiple samples of a measurement are taken over time. If multiple samples are taken, each SHOULD be included in a different "measurement" element.

4.3. Measurement Request

A measurement request is used by a protocol peer to describe a set of measurement data that it desires. A "measurementRequest" element is defined that can be included in a protocol exchange.

For instance, a LIS can use a measurement request in HELD responses. If the LIS is unable to provide location information, but it believes that a particular measurement type would enable it to provide a location, it can include a measurement request in an error response.

The "measurement" element of the measurement request identifies the type of measurement that is requested. The "type" attribute of this element indicates the type of measurement, as identified by an XML qualified name. A "samples" attribute MAY be used to indicate how many samples of the identified measurement are requested.

The "measurement" element can be repeated to request multiple (or alternative) measurement types.

Additional XML content might be defined for a particular measurement type that is used to further refine a request. These elements either constrain what is requested or specify non-mandatory components of the measurement data that are needed. These are defined along with the specific measurement type.

In the HELD protocol, the inclusion of a measurement request in an error response with a code of "locationUnknown" indicates that providing measurements would increase the likelihood of a subsequent request being successful.

The following example shows a HELD error response that indicates that WiFi measurement data would be useful if a later request were made. Additional elements indicate that received signal strength for an 802.11n access point is requested.

```
<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
   code="locationUnknown">
  <message xml:lang="en">Insufficient measurement data</message>
  <measurementRequest
  xmlns="urn:ietf:params:xml:ns:geopriv:lm"
  xmlns:wifi="urn:ietf:params:xml:ns:geopriv:lm:wifi">
    <measurement type="wifi:wifi">
      <wifi:type>n</wifi:type>
      <wifi:parameter context="ap">wifi:rcpi</wifi:parameter>
    </measurement>
  </measurementRequest>
</error>
```

Figure 3: HELD Error Requesting Measurement Data

A measurement request that is included in other HELD messages has undefined semantics and can be safely ignored. Other specifications might define semantics for measurement requests under other conditions.

4.4. Identifying Location Provenance

An extension is made to the PIDF-LO [RFC4119] that allows a location recipient to identify the source (or sources) of location information and the measurement data that was used to determine that location information.

The "source" element is added to the "geopriv" element of the PIDF-LO. This element does not identify specific entities. Instead, it identifies the type of measurement source.

The following values are defined for the "source" element:

lis: Location information is based on measurement data that the LIS or sources that it trusts have acquired. This label MAY be used if measurement data provided by the Device has been completely validated by the LIS.

device: A LIS MUST include this value if the location information is based (in whole or in part) on measurement data provided by the Device and if the measurement data isn’t completely validated.

other: Location information is based on measurement data that a third party has provided. This might be an authorized third party that uses identity parameters [RFC6155] or any other entity. The LIS MUST include this, unless the third party is trusted by the LIS to provide measurement data.

No assertion is made about the veracity of the measurement data from sources other than the LIS. A combination of tags MAY be included to indicate that measurement data from multiple types of sources was used.

For example, the first tuple of the following PIDF-LO indicates that measurement data from a LIS and a Device was combined to produce the result; the second tuple was produced by the LIS alone.

```
  <presence xmlns="urn:ietf:params:xml:ns:pidf"
        xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
        xmlns:gml="http://www.opengis.net/gml"
        xmlns:gs="http://www.opengis.net/pidflo/1.0"
        xmlns:lmsrc="urn:ietf:params:xml:ns:pidf:geopriv10:lmsrc"
        entity="pres:lm@example.com">
    <tuple id="deviceLoc">
      <status>
        <gp:geopriv>
          <gp:location-info>
            <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
              <gml:pos>7.34324 134.47162</gml:pos>
              <gs:radius uom="urn:ogc:def:uom:EPSG::9001">
                850.24
              </gs:radius>
            </gs:Circle>
          </gp:location-info>
          <gp:usage-rules/>
          <gp:method>OTDOA</gp:method>
          <lmsrc:source>lis device</lmsrc:source>
        </gp:geopriv>
      </status>
    </tuple>
    <tuple id="lisLoc">
      <status>
        <gp:geopriv>
          <gp:location-info>
            <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
              <gml:pos>7.34379 134.46484</gml:pos>
              <gs:radius uom="urn:ogc:def:uom:EPSG::9001">
                9000
              </gs:radius>
            </gs:Circle>
```

```
            </gp:location-info>
            <gp:usage-rules/>
            <gp:method>Cell</gp:method>
            <lmsrc:source>lis</lmsrc:source>
          </gp:geopriv>
        </status>
      </tuple>
    </presence>
```

PIDF-LO Document with Source Labels

5. Location-Related Measurement Data Types

This document defines location-related measurement data types for a range of common network types.

All included measurement data definitions allow for arbitrary extension in the corresponding schema. New parameters that are applicable to location determination are added as new XML elements in a unique namespace, not by adding elements to an existing namespace.

5.1. LLDP Measurements

Link-Layer Discovery Protocol (LLDP) [IEEE.8021AB] messages are sent between adjacent nodes in an IEEE 802 network (e.g., wired Ethernet, WiFi, 802.16). These messages all contain identification information for the sending node; the identification information can be used to determine location information. A Device that receives LLDP messages can report this information as a location-related measurement to the LIS, which is then able to use the measurement data in determining the location of the Device.

> Note: The LLDP extensions defined in LLDP Media Endpoint Discovery (LLDP-MED) [ANSI-TIA-1057] provide the ability to acquire location information directly from an LLDP endpoint. Where this information is available, it might be unnecessary to use any other form of location configuration.

Values are provided as hexadecimal sequences. The Device MUST report the values directly as they were provided by the adjacent node. Attempting to adjust or translate the type of identifier is likely to cause the measurement data to be useless.

Where a Device has received LLDP messages from multiple adjacent nodes, it should provide information extracted from those messages by repeating the "lldp" element.

An example of an LLDP measurement is shown in Figure 4. This shows an adjacent node (chassis) that is identified by the IP address 192.0.2.45 (hexadecimal c000022d), and the port on that node is numbered using an agent circuit ID [RFC3046] of 162 (hexadecimal a2).

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <lldp xmlns="urn:ietf:params:xml:ns:geopriv:lm:lldp">
    <chassis type="4">c000022d</chassis>
    <port type="6">a2</port>
  </lldp>
</measurements>
```

Figure 4: LLDP Measurement Example

IEEE 802 Devices that are able to obtain information about adjacent network switches and their attachment to them by other means MAY use this data type to convey this information.

5.2. DHCP Relay Agent Information Measurements

The DHCP Relay Agent Information option [RFC3046] provides measurement data about the network attachment of a Device. This measurement data can be included in the "dhcp-rai" element.

The elements in the DHCP relay agent information options are opaque data types assigned by the DHCP relay agent. The three items MAY be omitted if unknown: circuit identifier ("circuit", circuit [RFC3046], or Interface-Id [RFC3315]), remote identifier ("remote", Remote ID [RFC3046], or remote-id [RFC4649]), and subscriber identifier ("subscriber", subscriber-id [RFC3993], or Subscriber-ID [RFC4580]). The DHCPv6 remote-id has an associated enterprise number [IANA.enterprise] as an XML attribute.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <dhcp-rai xmlns="urn:ietf:params:xml:ns:geopriv:lm:dhcp">
    <giaddr>192.0.2.158</giaddr>
    <circuit>108b</circuit>
  </dhcp-rai>
</measurements>
```

Figure 5: DHCP Relay Agent Information Measurement Example

The "giaddr" element is specified as a dotted quad IPv4 address or an RFC 4291 [RFC4291] IPv6 address, using the forms defined in [RFC3986]; IPv6 addresses SHOULD use the form described in [RFC5952]. The enterprise number is specified as a decimal integer. All other information is included verbatim from the DHCP request in hexadecimal format.

The "subscriber" element could be considered sensitive. This information MUST NOT be provided to a LIS that is not authorized to receive information about the access network. See Section 7.1.3 for more details.

5.3. 802.11 WLAN Measurements

In WiFi, or 802.11 [IEEE.80211], networks, a Device might be able to provide information about the access point (AP) to which it is attached, or other WiFi points it is able to see. This is provided using the "wifi" element, as shown in Figure 6, which shows a single complete measurement for a single access point.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2011-04-29T14:33:58">
  <wifi xmlns="urn:ietf:params:xml:ns:geopriv:lm:wifi">
    <nicType>Intel(r)PRO/Wireless 2200BG</nicType>
    <ap serving="true">
      <bssid>AB-CD-EF-AB-CD-EF</bssid>
      <ssid>example</ssid>
      <channel>5</channel>
      <location>
        <gml:Point xmlns:gml="http://opengis.net/gml">
          <gml:pos>-34.4 150.8</gml:pos>
        </gml:Point>
      </location>
      <type>a</type>
      <band>5</band>
      <regclass country="AU">2</regclass>
      <antenna>2</antenna>
      <flightTime rmsError="4e-9" samples="1">2.56e-9</flightTime>
      <apSignal>
        <transmit>23</transmit>
        <gain>5</gain>
        <rcpi dBm="true" rmsError="12" samples="1">-59</rcpi>
        <rsni rmsError="15" samples="1">23</rsni>
      </apSignal>
      <deviceSignal>
        <transmit>10</transmit>
        <gain>9</gain>
        <rcpi dBm="true" rmsError="9.5" samples="1">-98.5</rcpi>
```

```
            <rsni rmsError="6" samples="1">7.5</rsni>
          </deviceSignal>
        </ap>
      </wifi>
    </measurements>
```

Figure 6: 802.11 WLAN Measurement Example

A "wifi" element is made up of one or more access points, and a "nicType" element, which MAY be omitted. Each access point is described using the "ap" element, which is comprised of the following fields:

bssid: The Basic Service Set (BSS) identifier. In an Infrastructure BSS network, the bssid is the 48-bit MAC address of the access point.

The "verified" attribute of this element describes whether the Device has verified the MAC address or it authenticated the access point or the network operating the access point (for example, a captive portal accessed through the access point has been authenticated). This attribute defaults to a value of "false" when omitted.

ssid: The service set identifier (SSID) for the wireless network served by the access point.

The SSID is a 32-octet identifier that is commonly represented as an ASCII [ASCII] or UTF-8 [RFC3629] encoded string. To represent octets that cannot be directly included in an XML element, escaping is used. Sequences of octets that do not represent a valid UTF-8 encoding can be escaped using a backslash ('\') followed by two case-insensitive hexadecimal digits representing the value of a single octet.

The canonical or value-space form of an SSID is a sequence of up to 32 octets that is produced from the concatenation of UTF-8 encoded sequences of unescaped characters and octets derived from escaped components.

channel: The channel number (frequency) on which the access point operates.

location: The location of the access point, as reported by the access point. This element contains any valid location, using the rules for a "location-info" element, as described in [RFC5491].

type: The network type for the network access. This element includes the alphabetic suffix of the 802.11 specification that introduced the radio interface, or PHY, e.g., "a", "b", "g", or "n".

band: The frequency band for the radio, in gigahertz (GHz). 802.11 [IEEE.80211] specifies PHY layers that use 2.4, 3.7, and 5 gigahertz frequency bands.

regclass: The operating class (regulatory domain and class in older versions of 802.11); see Annex E of [IEEE.80211]. The "country" attribute optionally includes the applicable two-character country identifier (dot11CountryString), which can be followed by an 'O', 'I', or 'X'. The element text content includes the value of the regulatory class: an 8-bit integer in decimal form.

antenna: The antenna identifier for the antenna that the access point is using to transmit the measured signals.

flightTime: Flight time is the difference between the time of departure (TOD) of signal from a transmitting station and time of arrival (TOA) of signal at a receiving station, as defined in [IEEE.80211]. Measurement of this value requires that stations synchronize their clocks. This value can be measured by an access point or Device; because the flight time is assumed to be the same in either direction -- aside from measurement errors -- only a single element is provided. This element permits the use of the "rmsError" and "samples" attributes. RMS error might be derived from the reported RMS error in TOD and TOA.

apSignal: Measurement information for the signal transmitted by the access point, as observed by the Device. Some of these values are derived from 802.11v [IEEE.80211] messages exchanged between the Device and access point. The contents of this element include:

transmit: The transmit power reported by the access point, in dBm.

gain: The gain of the access point antenna reported by the access point, in dB.

rcpi: The received channel power indicator for the access point signal, as measured by the Device. This value SHOULD be in units of dBm (with RMS error in dB). If power is measured in a different fashion, the "dBm" attribute MUST be set to "false". Signal strength reporting on current hardware uses a range of different mechanisms; therefore, the value of the "nicType" element SHOULD be included if the units are not known to be in

dBm, and the value reported by the hardware should be included without modification. This element permits the use of the "rmsError" and "samples" attributes.

rsni: The received signal-to-noise indicator in dB. This element permits the use of the "rmsError" and "samples" attributes.

deviceSignal: Measurement information for the signal transmitted by the Device, as reported by the access point. This element contains the same child elements as the "ap" element, with the access point and Device roles reversed.

The only mandatory element in this structure is "bssid".

The "nicType" element is used to specify the make and model of the wireless network interface in the Device. Different 802.11 chipsets report measurements in different ways, so knowing the network interface type aids the LIS in determining how to use the provided measurement data. The content of this field is unconstrained, and no mechanisms are specified to ensure uniqueness. This field is unlikely to be useful, except under tightly controlled circumstances.

5.3.1. WiFi Measurement Requests

Two elements are defined for requesting WiFi measurements in a measurement request:

type: The "type" element identifies the desired type (or types that are requested).

parameter: The "parameter" element identifies measurements that are requested for each measured access point. An element is identified by its qualified name. The "context" parameter can be used to specify if an element is included as a child of the "ap" or "device" elements; omission indicates that it applies to both.

Multiple types or parameters can be requested by repeating either element.

5.4. Cellular Measurements

Cellular Devices are common throughout the world, and base station identifiers can provide a good source of coarse location information. Cellular measurements can be provided to a LIS run by the cellular operator, or may be provided to an alternative LIS operator that has access to one of several global cell-id to location mapping databases.

A number of advanced location determination methods have been developed for cellular networks. For these methods, a range of measurement parameters can be collected by the network, Device, or both in cooperation. This document includes a basic identifier for the wireless transmitter only; future efforts might define additional parameters that enable more accurate methods of location determination.

The cellular measurement set allows a Device to report to a LIS any LTE (Figure 7), UMTS (Figure 8), GSM (Figure 9), or CDMA (Figure 10) cells that it is able to observe. Cells are reported using their global identifiers. All Third Generation Partnership Project (3GPP) cells are identified by a public land mobile network (PLMN), which comprises a mobile country code (MCC) and mobile network code (MNC); specific fields are added for each network type.

Formats for 3GPP cell identifiers are described in [TS.3GPP.23.003]. Bit-level formats for CDMA cell identifiers are described in [TIA-2000.5]; decimal representations are used.

MCC and MNC are provided as decimal digit sequences; a leading zero in an MCC or MNC is significant. All other values are decimal integers.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <cellular xmlns="urn:ietf:params:xml:ns:geopriv:lm:cell">
    <servingCell>
      <mcc>465</mcc><mnc>20</mnc><eucid>80936424</eucid>
    </servingCell>
    <observedCell>
      <mcc>465</mcc><mnc>06</mnc><eucid>10736789</eucid>
    </observedCell>
  </cellular>
</measurements>
```

Long term evolution (LTE) cells are identified by a 28-bit cell identifier (eucid).

Figure 7: Example LTE Cellular Measurement

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <cellular xmlns="urn:ietf:params:xml:ns:geopriv:lm:cell">
    <servingCell>
      <mcc>465</mcc><mnc>20</mnc>
      <rnc>2000</rnc><cid>65000</cid>
    </servingCell>
    <observedCell>
      <mcc>465</mcc><mnc>06</mnc>
      <lac>16383</lac><cid>32767</cid>
    </observedCell>
  </cellular>
</measurements>
```

Universal mobile telephony service (UMTS) cells are identified by a 12- or 16-bit radio network controller (rnc) id and a 16-bit cell id (cid).

Figure 8: Example UMTS Cellular Measurement

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <cellular xmlns="urn:ietf:params:xml:ns:geopriv:lm:cell">
    <servingCell>
      <mcc>465</mcc><mnc>06</mnc>
      <lac>16383</lac><cid>32767</cid>
    </servingCell>
  </cellular>
</measurements>
```

Global System for Mobile communication (GSM) cells are identified by a 16-bit location area code (lac) and a 16-bit cell id (cid).

Figure 9: Example GSM Cellular Measurement

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <cellular xmlns="urn:ietf:params:xml:ns:geopriv:lm:cell">
    <servingCell>
      <sid>15892</sid><nid>4723</nid><baseid>12</baseid>
    </servingCell>
    <observedCell>
      <sid>15892</sid><nid>4723</nid><baseid>13</baseid>
    </observedCell>
  </cellular>
</measurements>
```

Code division multiple access (CDMA) cells are not identified by a PLMN; instead, these use a 15-bit system id (sid), a 16-bit network id (nid), and a 16-bit base station id (baseid).

Figure 10: Example CDMA Cellular Measurement

In general, a cellular Device will be attached to the cellular network, so the notion of a serving cell exists. Cellular networks also provide overlap between neighboring sites, so a mobile Device can hear more than one cell. The measurement schema supports sending both the serving cell and any other cells that the mobile might be able to hear. In some cases, the Device could simply be listening to cell information without actually attaching to the network; mobiles without a SIM are an example of this. In this case, the Device could report cells it can hear without identifying any particular cell as a serving cell. An example of this is shown in Figure 11.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <cellular xmlns="urn:ietf:params:xml:ns:geopriv:lm:cell">
    <observedCell>
      <mcc>465</mcc><mnc>20</mnc>
      <rnc>2000</rnc><cid>65000</cid>
    </observedCell>
    <observedCell>
      <mcc>465</mcc><mnc>06</mnc>
      <lac>16383</lac><cid>32767</cid>
    </observedCell>
  </cellular>
</measurements>
```

Figure 11: Example Observed Cellular Measurement

5.4.1. Cellular Measurement Requests

Two elements can be used in measurement requests for cellular measurements:

type: A label indicating the type of identifier to provide: one of "gsm", "umts", "lte", or "cdma".

network: The network portion of the cell identifier. For 3GPP networks, this is the combination of MCC and MNC; for CDMA, this is the network identifier.

Multiple identifier types or networks can be identified by repeating either element.

5.5. GNSS Measurements

A Global Navigation Satellite System (GNSS) uses orbiting satellites to transmit signals. A Device with a GNSS receiver is able to take measurements from the satellite signals. The results of these measurements can be used to determine time and the location of the Device.

Determining location and time in autonomous GNSS receivers follows three steps:

Signal acquisition: During the signal acquisition stage, the receiver searches for the repeating code that is sent by each GNSS satellite. Successful operation typically requires measurement data for a minimum of 5 satellites. At this stage, measurement data is available to the Device.

Navigation message decode: Once the signal has been acquired, the receiver then receives information about the configuration of the satellite constellation. This information is broadcast by each satellite and is modulated with the base signal at a low rate; for instance, GPS sends this information at about 50 bits per second.

Calculation: The measurement data is combined with the data on the satellite constellation to determine the location of the receiver and the current time.

A Device that uses a GNSS receiver is able to report measurements after the first stage of this process. A LIS can use the results of these measurements to determine a location. In the case where there are fewer results available than the optimal minimum, the LIS might be able to use other sources of measurement information and combine these with the available measurement data to determine a position.

Note: The use of different sets of GNSS assistance data can reduce the amount of time required for the signal acquisition stage and obviate the need for the receiver to extract data on the satellite constellation. Provision of assistance data is outside the scope of this document.

Figure 12 shows an example of GNSS measurement data. The measurement shown is for the GPS satellite system and includes measurement data for three satellites only.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58" timeError="2e-5">
  <gnss xmlns="urn:ietf:params:xml:ns:geopriv:lm:gnss"
    system="gps" signal="L1">
    <sat num="19">
      <doppler>499.9395</doppler>
      <codephase rmsError="1.6e-9">0.87595747</codephase>
      <cn0>45</cn0>
    </sat>
    <sat num="27">
      <doppler>378.2657</doppler>
      <codephase rmsError="1.6e-9">0.56639479</codephase>
      <cn0>52</cn0>
    </sat>
    <sat num="20">
      <doppler>-633.0309</doppler>
      <codephase rmsError="1.6e-9">0.57016835</codephase>
      <cn0>48</cn0>
    </sat>
  </gnss>
</measurements>
```

Figure 12: Example GNSS Measurement

Each "gnss" element represents a single set of GNSS measurement data, taken at a single point in time. Measurements taken at different times can be included in different "gnss" elements to enable iterative refinement of results.

GNSS measurement parameters are described in more detail in the following sections.

5.5.1. GNSS: System Type and Signal

The GNSS measurement structure is designed to be generic and to apply to different GNSS types. Different signals within those systems are also accounted for and can be measured separately.

The GNSS type determines the time system that is used. An indication of the type of system and signal can ensure that the LIS is able to correctly use measurements.

Measurements for multiple GNSS types and signals can be included by repeating the "gnss" element.

This document creates an IANA registry for GNSS types. Two satellite systems are registered by this document: GPS [GPS.ICD] and Galileo [Galileo.ICD]. Details for the registry are included in Section 9.1.

5.5.2. Time

Each set of GNSS measurements is taken at a specific point in time. The "time" attribute is used to indicate the time that the measurement was acquired, if the receiver knows how the time system used by the GNSS relates to UTC time.

Alternative to (or in addition to) the measurement time, the "gnssTime" element MAY be included. The "gnssTime" element includes a relative time in milliseconds using the time system native to the satellite system. For the GPS satellite system, the "gnssTime" element includes the time of week in milliseconds. For the Galileo system, the "gnssTime" element includes the time of day in milliseconds.

The accuracy of the time measurement provided is critical in determining the accuracy of the location information derived from GNSS measurements. The receiver SHOULD indicate an estimated time error for any time that is provided. An RMS error can be included for the "gnssTime" element, with a value in milliseconds.

5.5.3. Per-Satellite Measurement Data

Multiple satellites are included in each set of GNSS measurements using the "sat" element. Each satellite is identified by a number in the "num" attribute. The satellite number is consistent with the identifier used in the given GNSS.

Both the GPS and Galileo systems use satellite numbers between 1 and 64.

The GNSS receiver measures the following parameters for each satellite:

doppler: The observed Doppler shift of the satellite signal, measured in meters per second. This is converted from a value in Hertz by the receiver to allow the measurement to be used without

knowledge of the carrier frequency of the satellite system. This value permits the use of RMS error attributes, also measured in meters per second.

codephase: The observed code phase for the satellite signal, measured in milliseconds. This is converted from the system-specific value of chips or wavelengths into a system-independent value. Larger values indicate larger distances from satellite to receiver. This value permits the use of RMS error attributes, also measured in milliseconds.

cn0: The signal-to-noise ratio for the satellite signal, measured in decibel-Hertz (dB-Hz). The expected range is between 20 and 50 dB-Hz.

mp: An estimation of the amount of error that multipath signals contribute in meters. This parameter MAY be omitted.

cq: An indication of the carrier quality. Two attributes are included: "continuous" (which can be either "true" or "false") and "direct" (which can be either "direct" or "inverted"). This parameter MAY be omitted.

adr: The accumulated Doppler range, measured in meters. This parameter MAY be omitted and is not useful unless multiple sets of GNSS measurements are provided or differential positioning is being performed.

All values are converted from measures native to the satellite system to generic measures to ensure consistency of interpretation. Unless necessary, the schema does not constrain these values.

5.5.4. GNSS Measurement Requests

Measurement requests can include a "gnss" element, which includes the "system" and "signal" attributes. Multiple elements can be included to indicate requests for GNSS measurements from multiple systems or signals.

5.6. DSL Measurements

Digital Subscriber Line (DSL) networks rely on a range of network technologies. DSL deployments regularly require cooperation between multiple organizations. These fall into two broad categories: infrastructure providers and Internet service providers (ISPs). For the same end user, an infrastructure and Internet service can be provided by different entities. Infrastructure providers manage the bulk of the physical infrastructure, including cabling. End users

obtain their service from an ISP, which manages all aspects visible to the end user, including IP address allocation and operation of a LIS. See [DSL.TR025] and [DSL.TR101] for further information on DSL network deployments and the parameters that are available.

Exchange of measurement information between these organizations is necessary for location information to be correctly generated. The ISP LIS needs to acquire location information from the infrastructure provider. However, since the infrastructure provider could have no knowledge of Device identifiers, it can only identify a stream of data that is sent to the ISP. This is resolved by passing measurement data relating to the Device to a LIS operated by the infrastructure provider.

5.6.1. L2TP Measurements

The Layer 2 Tunneling Protocol (L2TP) [RFC2661] is a common means of linking the infrastructure provider and the ISP. The infrastructure provider LIS requires measurement data that identifies a single L2TP tunnel, from which it can generate location information. Figure 13 shows an example L2TP measurement.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <dsl xmlns="urn:ietf:params:xml:ns:geopriv:lm:dsl">
    <l2tp>
      <src>192.0.2.10</src>
      <dest>192.0.2.61</dest>
      <session>528</session>
    </l2tp>
  </dsl>
</measurements>
```

Figure 13: Example DSL L2TP Measurement

5.6.2. RADIUS Measurements

When authenticating network access, the infrastructure provider might employ a RADIUS [RFC2865] proxy at the DSL Access Module (DSLAM) or Access Node (AN). These messages provide the ISP RADIUS server with an identifier for the DSLAM or AN, plus the slot and port to which the Device is attached. These data can be provided as a measurement that allows the infrastructure provider LIS to generate location information.

The format of the AN, slot, and port identifiers is not defined in the RADIUS protocol. The slot and port together identify a circuit on the AN, analogous to the circuit identifier in [RFC3046]. These items are provided directly, as they would be in the RADIUS message. An example is shown in Figure 14.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <dsl xmlns="urn:ietf:params:xml:ns:geopriv:lm:dsl">
    <an>AN-7692</an>
    <slot>3</slot>
    <port>06</port>
  </dsl>
</measurements>
```

Figure 14: Example DSL RADIUS Measurement

5.6.3. Ethernet VLAN Tag Measurements

For Ethernet-based DSL access networks, the DSLAM or AN provides two VLAN tags on packets. A C-TAG is used to identify the incoming residential circuit, while the S-TAG is used to identify the DSLAM or AN. The C-TAG and S-TAG together can be used to identify a single point of network attachment. An example is shown in Figure 15.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <dsl xmlns="urn:ietf:params:xml:ns:geopriv:lm:dsl">
    <stag>613</stag>
    <ctag>1097</ctag>
  </dsl>
</measurements>
```

Figure 15: Example DSL VLAN Tag Measurement

Alternatively, the C-TAG can be replaced by data on the slot and port to which the Device is attached. This information might be included in RADIUS requests that are proxied from the infrastructure provider to the ISP RADIUS server.

5.6.4. ATM Virtual Circuit Measurements

An ATM virtual circuit can be employed between the ISP and infrastructure provider. Providing the virtual port ID (VPI) and virtual circuit ID (VCI) for the virtual circuit gives the infrastructure provider LIS the ability to identify a single data stream. A sample measurement is shown in Figure 16.

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
      time="2008-04-29T14:33:58">
  <dsl xmlns="urn:ietf:params:xml:ns:geopriv:lm:dsl">
    <vpi>55</vpi>
    <vci>6323</vci>
  </dsl>
</measurements>
```

Figure 16: Example DSL ATM Measurement

6. Privacy Considerations

Location-related measurement data can be as privacy sensitive as location information [RFC6280].

Measurement data is effectively equivalent to location information if the contextual knowledge necessary to generate one from the other is readily accessible. Even where contextual knowledge is difficult to acquire, there can be no assurance that an authorized recipient of the contextual knowledge is also authorized to receive location information.

In order to protect the privacy of the subject of location-related measurement data, measurement data MUST be protected with the same degree of protection as location information. The confidentiality and authentication provided by Transport Layer Security (TLS) MUST be used in order to convey measurement data over HELD [RFC5985]. Other protocols MUST provide comparable guarantees.

6.1. Measurement Data Privacy Model

It is not necessary to distribute measurement data in the same fashion as location information. Measurement data is less useful to location recipients than location information. A simple distribution model is described in this document.

In this simple model, the Device is the only entity that is able to distribute measurement data. To use an analogy from the GEOPRIV architecture, the Device -- as the Location Generator or the Measurement Data Generator -- is the sole entity that can act in the role of both Rule Maker and Location Server.

A Device that provides location-related measurement data MUST only do so as explicitly authorized by a Rule Maker. This depends on having an interface that allows Rule Makers (for instance, users or administrators) to control where and how measurement data is provided.

No entity is permitted to redistribute measurement data. The Device directs other entities regarding how measurement data is used and retained.

The GEOPRIV model [RFC6280] protects the location of a Target using direction provided by a Rule Maker. For the purposes of measurement data distribution, this model relies on the assumptions made in Section 3 of HELD [RFC5985]. These assumptions effectively declare the Device to be a proxy for both Target and Rule Maker.

6.2. LIS Privacy Requirements

A LIS MUST NOT reveal location-related measurement data to any other entity. A LIS MUST NOT reveal location information based on measurement data to any other entity unless directed to do so by the Device.

By adding measurement data to a request for location information, the Device implicitly grants permission for the LIS to generate the requested location information using the measurement data. Permission to use this data for any other purpose is not implied.

As long as measurement data is only used in serving the request that contains it, rules regarding data retention are not necessary. A LIS MUST discard location-related measurement data after servicing a request, unless the Device grants permission to use that information for other purposes.

6.3. Measurement Data and Location URIs

A LIS MAY use measurement data provided by the Device to serve requests to location URIs, if the Device permits it. A Device permits this by including measurement data in a request that explicitly requests a location URI. By requesting a location URI,

the Device grants permission for the LIS to use the measurement data in serving requests to that location URI. The LIS cannot provide location recipients with measurement data, as defined in Section 6.1.

> Note: In HELD, the "any" type is not an explicit request for a location URI, though a location URI might be provided.

The usefulness of measurement data that is provided in this fashion is limited. The measurement data is only valid at the time that it was acquired by the Device. At the time that a request is made to a location URI, the Device might have moved, rendering the measurement data incorrect.

A Device is able to explicitly limit the time that a LIS retains measurement data by adding an expiry time to the measurement data. A LIS MUST NOT retain location-related measurement data in memory, storage, or logs beyond the time indicated in the "expires" attribute (Section 4.1.2). A LIS MUST NOT retain measurement data if the "expires" attribute is absent.

6.4. Measurement Data Provided by a Third Party

An authorized third-party request for the location of a Device (see [RFC6155]) can include location-related measurement data. This is possible where the third party is able to make observations about the Device.

A third party that provides measurement data MUST be authorized to provide the specific measurement for the identified Device. Either a third party MUST be trusted by the LIS for the purposes of providing measurement data of the provided type, or the measurement data MUST be validated (see Section 7.2.1) before being used.

How a third party authenticates its identity or gains authorization to use measurement data is not covered by this document.

7. Security Considerations

The use of location-related measurement data has privacy considerations that are discussed in Section 6.

7.1. Threat Model

The threat model for location-related measurement data concentrates on the Device providing falsified, stolen, or incorrect measurement data.

A Device that provides location-related measurement data might use data to:

- acquire the location of another Device, without authorization;
- extract information about network topology; or
- coerce the LIS into providing falsified location information based on the measurement data.

Location-related measurement data describes the physical environment or network attachment of a Device. A third-party adversary in the proximity of the Device might be able to alter the physical environment such that the Device provides measurement data that is controlled by the third party. This might be used to indirectly control the location information that is derived from measurement data.

7.1.1. Acquiring Location Information without Authorization

Requiring authorization for location requests is an important part of privacy protections of a location protocol. A location configuration protocol usually operates under a restricted policy that allows a requester to obtain their own location. HELD identity extensions [RFC6155] allow other entities to be authorized, conditional on a Rule Maker providing sufficient authorization.

The intent of these protections is to ensure that a location recipient is authorized to acquire location information. Location-related measurement data could be used by an attacker to circumvent such authorization checks if the association between measurement data and Target Device is not validated by a LIS.

A LIS can be coerced into providing location information for a Device that a location recipient is not authorized to receive. A request identifies one Device (implicitly or explicitly), but measurement data is provided for another Device. If the LIS does not check that the measurement data is for the identified Device, it could incorrectly authorize the request.

By using unverified measurement data to generate a response, the LIS provides information about a Device without appropriate authorization.

The feasibility of this attack depends on the availability of information that links a Device with measurement data. In some cases, measurement data that is correlated with a Target is readily available. For instance, LLDP measurements (Section 5.1) are

broadcast to all nodes on the same network segment. An attacker on that network segment can easily gain measurement data that relates a Device with measurements.

For some types of measurement data, it's necessary for an attacker to know the location of the Target in order to determine what measurements to use. This attack is meaningless for types of measurement data that require that the attacker first know the location of the Target before measurement data can be acquired or fabricated. GNSS measurements (Section 5.5) share this trait with many wireless location determination methods.

7.1.2. Extracting Network Topology Data

Allowing requests with measurements might be used to collect information about network topology.

Network topology can be considered sensitive information by a network operator for commercial or security reasons. While it is impossible to completely prevent a Device from acquiring some knowledge of network topology if a location service is provided, a network operator might desire to limit how much of this information is made available.

Mapping a network topology does not require that an attacker be able to associate measurement data with a particular Device. If a requester is able to try a number of measurements, it is possible to acquire information about network topology.

It is not even necessary that the measurements are valid; random guesses are sufficient, provided that there is no penalty or cost associated with attempting to use the measurements.

7.1.3. Exposing Network Topology Data

A Device could reveal information about a network to entities outside of that network if it provides location measurement data to a LIS that is outside of that network. With the exception of GNSS measurements, the measurements in this document provide information about an access network that could reveal topology information to an unauthorized recipient.

A Device MUST NOT provide information about network topology without a clear signal that the recipient is authorized. A LIS that is discovered using DHCP as described in LIS discovery [RFC5986] can be considered to be authorized to receive information about the access network.

7.1.4. Lying by Proxy

Location information, which includes measurement data, is a function of its inputs. Thus, falsified measurement data can be used to alter the location information that is provided by a LIS.

Some types of measurement data are relatively easy to falsify in a way that causes the resulting location information to be selected with little or no error. For instance, GNSS measurements are easy to use for this purpose because all the contextual information necessary to calculate a position using measurements is broadcast by the satellites [HARPER].

An attacker that falsifies measurement data gains little if they are the only recipient of the result. The attacker knows that the location information is bad. The attacker only gains if the information can somehow be attributed to the LIS by another location recipient. By coercing the LIS into providing falsified location information, any credibility that the LIS might have -- that the attacker does not -- is gained by the attacker.

A third party that is reliant on the integrity of the location information might base an evaluation of the credibility of the information on the source of the information. If that third party is able to attribute location information to the LIS, then an attacker might gain.

Location information that is provided to the Device without any means to identify the LIS as its source is not subject to this attack. The Device is identified as the source of the data when it distributes the location information to location recipients.

Location information is attributed to the LIS either through the use of digital signatures or by having the location recipient directly interact with the LIS. A LIS that digitally signs location information becomes identifiable as the source of the data. Similarly, the LIS is identified as a source of data if a location recipient acquires information directly from a LIS using a location URI.

7.1.5. Measurement Replay

The values of some measured properties do not change over time for a single location. The time invariance of network properties is often a direct result of the practicalities of operating the network. Limiting the changes to a network ensures greater consistency of service. A largely static network also greatly simplifies the data management tasks involved with providing a location service.

However, time-invariant properties allow for simple replay attacks, where an attacker acquires measurements that can later be used without being detected as being invalid.

Measurement data is frequently an observation of a time-invariant property of the environment at the subject location. For measurements of this nature, nothing in the measurement itself is sufficient proof that the Device is present at the resulting location. Measurement data might have been previously acquired and reused.

For instance, the identity of a radio transmitter, if broadcast by that transmitter, can be collected and stored. An attacker that wishes it known that they exist at a particular location can claim to observe this transmitter at any time. Nothing inherent in the claim reveals it to be false.

7.1.6. Environment Spoofing

Some types of measurement data can be altered or influenced by a third party so that a Device unwittingly provides falsified data. If it is possible for a third party to alter the measured phenomenon, then any location information that is derived from this data can be indirectly influenced.

Altering the environment in this fashion might not require involvement with either a Device or LIS. Measurement that is passive -- where the Device observes a signal or other phenomenon without direct interaction -- is most susceptible to alteration by third parties.

Measurement of radio signal characteristics is especially vulnerable, since an adversary need only be in the general vicinity of the Device and be able to transmit a signal. For instance, a GNSS spoofer is able to produce fake signals that claim to be transmitted by any satellite or set of satellites (see [GPS.SPOOF]).

Measurements that require direct interaction increase the complexity of the attack. For measurements relating to the communication medium, a third party cannot avoid direct interaction; they need only be on the communications path (that is, man in the middle).

Even if the entity that is interacted with is authenticated, this does not provide any assurance about the integrity of measurement data. For instance, the Device might authenticate the identity of a radio transmitter through the use of cryptographic means and obtain signal strength measurements for that transmitter. Radio signal

strength is trivial for an attacker to increase simply by receiving and amplifying the raw signal; it is not necessary for the attacker to be able to understand the signal content.

> Note: This particular "attack" is more often completely legitimate. Radio repeaters are a commonplace mechanism used to increase radio coverage.

Attacks that rely on altering the observed environment of a Device require countermeasures that affect the measurement process. For radio signals, countermeasures could include the use of authenticated signals, or altered receiver design. In general, countermeasures are highly specific to the individual measurement process. An exhaustive discussion of these issues is left to the relevant literature for each measurement technology.

A Device that provides measurement data is assumed to be responsible for applying appropriate countermeasures against this type of attack.

Where a Device is the sole recipient of location information derived from measurement data, a LIS might choose to provide location information without any validation. The responsibility for ensuring the veracity of the measurement data lies with the Device.

Measurement data that is susceptible to this sort of influence SHOULD be treated as though it were produced by an untrusted Device for those cases where a location recipient might attribute the location information to the LIS. GNSS measurements and radio signal strength measurements can be affected relatively cheaply, though almost all other measurement types can be affected with varying costs to an attacker, with the largest cost often being a requirement for physical access. To the extent that it is feasible, measurement data SHOULD be subjected to the same validation as for other types of attacks that rely on measurement falsification.

> Note: Altered measurement data might be provided by a Device that has no knowledge of the alteration. Thus, an otherwise trusted Device might still be an unreliable source of measurement data.

7.2. Mitigation

The following measures can be applied to limit or prevent attacks. The effectiveness of each depends on the type of measurement data and how that measurement data is acquired.

Two general approaches are identified for dealing with untrusted measurement data:

1. Require independent validation of measurement data or the location information that is produced.

2. Identify the types of sources that provided the measurement data from which that location information was derived.

This section goes into more detail on the different forms of validation in Sections 7.2.1, 7.2.2, and 7.2.3. The impact of attributing location information to sources is discussed in more detail in Section 7.2.4.

Any costs in validation are balanced against the degree of integrity desired from the resulting location information.

7.2.1. Measurement Validation

Recognizing that measurement data has been falsified is difficult in the absence of integrity mechanisms.

Independent confirmation of the veracity of measurement data ensures that the measurement is accurate and that it applies to the correct Device. When it’s possible to gather the same measurement data from a trusted and independent source without undue expense, the LIS can use the trusted data in place of what the untrusted Device has sent. In cases where that is impractical, the untrusted data can provide hints that allow corroboration of the data (see Section 7.2.1.1).

Measurement information might not contain any inherent indication that it is falsified. In addition, it can be difficult to obtain information that would provide any degree of assurance that the measurement device is physically at any particular location. Measurements that are difficult to verify require other forms of assurance before they can be used.

7.2.1.1. Effectiveness

Measurement validation MUST be used if measurement data for a particular Device can be easily acquired by unauthorized location recipients, as described in Section 7.1.1. This prevents unauthorized access to location information using measurement data.

Validation of measurement data can be significantly more effective than independent acquisition of the same. For instance, a Device in a large Ethernet network could provide a measurement indicating its point of attachment using LLDP measurements. For a LIS, acquiring

the same measurement data might require a request to all switches in that network. With the measurement data, validation can target the identified switch with a specific query.

Validation is effective in identifying falsified measurement data (Section 7.1.4), including attacks involving replay of measurement data (Section 7.1.5). Validation also limits the amount of network topology information (Section 7.1.2) made available to Devices to that portion of the network topology to which they are directly attached.

Measurement validation has no effect if the underlying environment is being altered (Section 7.1.6).

7.2.1.2. Limitations (Unique Observer)

A Device is often in a unique position to make a measurement. It alone occupies the point in space-time that the location determination process seeks to determine. The Device becomes a unique observer for a particular property.

The ability of the Device to become a unique observer makes the Device invaluable to the location determination process. As a unique observer, it also makes the claims of a Device difficult to validate and easy to spoof.

As long as no other entity is capable of making the same measurements, there is also no other entity that can independently check that the measurements are correct and applicable to the Device. A LIS might be unable to validate all or part of the measurement data it receives from a unique observer. For instance, a signal strength measurement of the signal from a radio tower cannot be validated directly.

Some portion of the measurement data might still be independently verified, even if all information cannot. In the previous example, the radio tower might be able to provide verification that the Device is present if it is able to observe a radio signal sent by the Device.

If measurement data can only be partially validated, the extent to which it can be validated determines the effectiveness of validation against these attacks.

The advantage of having the Device as a unique observer is that it makes it difficult for an attacker to acquire measurements without the assistance of the Device. Attempts to use measurements to gain unauthorized access to measurement data (Section 7.1.1) are largely ineffectual against a unique observer.

7.2.2. Location Validation

Location information that is derived from location-related measurement data can also be verified against trusted location information. Rather than validating inputs to the location determination process, suspect locations are identified at the output of the process.

Trusted location information is acquired using sources of measurement data that are trusted. Untrusted location information is acquired using measurement data provided from untrusted sources, which might include the Device. These two locations are compared. If the untrusted location agrees with the trusted location, the untrusted location information is used.

Algorithms for the comparison of location information are not included in this document. However, a simple comparison for agreement might require that the untrusted location be entirely contained within the uncertainty region of the trusted location.

There is little point in using a less accurate, less trusted location. Untrusted location information that has worse accuracy than trusted information can be immediately discarded. There are multiple factors that affect accuracy, uncertainty and currency being the most important. How location information is compared for accuracy is not defined in this document.

7.2.2.1. Effectiveness

Location validation limits the extent to which falsified -- or erroneous -- measurement data can cause an incorrect location to be reported.

Location validation can be more efficient than validation of inputs, particularly for a unique observer (Section 7.2.1.2).

Validating location ensures that the Device is at or near the resulting location. Location validation can be used to limit or prevent all of the attacks identified in this document.

7.2.2.2. Limitations

The trusted location that is used for validation is always less accurate than the location that is being checked. The amount by which the untrusted location is more accurate, is the same amount that an attacker can exploit.

For example, a trusted location might indicate an uncertainty region with a radius of five kilometers. An untrusted location that describes a 100-meter uncertainty within the larger region might be accepted as more accurate. An attacker might still falsify measurement data to select any location within the larger uncertainty region. While the 100-meter uncertainty that is reported seems more accurate, a falsified location could be anywhere in the five-kilometer region.

Where measurement data might have been falsified, the actual uncertainty is effectively much higher. Local policy might allow differing degrees of trust to location information derived from untrusted measurement data. This might be a boolean operation with only two possible outcomes: untrusted location information might be used entirely or not at all. Alternatively, untrusted location information could be combined with trusted location information using different weightings, based on a value set in local policy.

7.2.3. Supporting Observations

Replay attacks using previously acquired measurement data are particularly hard to detect without independent validation. Rather than validate the measurement data directly, supplementary data might be used to validate measurements or the location information derived from those measurements.

These supporting observations could be used to convey information that provides additional assurance that measurement data from the Device was acquired at a specific time and place. In effect, the Device is requested to provide proof of its presence at the resulting location.

For instance, a Device that measures attributes of a radio signal could also be asked to provide a sample of the measured radio signal. If the LIS is able to observe the same signal, the two observations could be compared. Providing that the signal cannot be predicted in advance by the Device, this could be used to support the claim that the Device is able to receive the signal. Thus, the Device is likely to be within the range that the signal is transmitted. A LIS could use this to attribute a higher level of trust in the associated measurement data or resulting location.

7.2.3.1. Effectiveness

The use of supporting observations is limited by the ability of the LIS to acquire and validate these observations. The advantage of selecting observations independent of measurement data is that observations can be selected based on how readily available the data is for both LIS and Device. The amount and quality of the data can be selected based on the degree of assurance that is desired.

The use of supporting observations is similar to both measurement validation and location validation. All three methods rely on independent validation of one or more properties. The applicability of each method is similar.

The use of supporting observations can be used to limit or prevent all of the attacks identified in this document.

7.2.3.2. Limitations

The effectiveness of the validation method depends on the quality of the supporting observation: how hard it is for the entity performing the validation to obtain the data at a different time or place, how difficult it is to guess, and what other costs might be involved in acquiring this data.

In the example of an observed radio signal, requesting a sample of the signal only provides an assurance that the Device is able to receive the signal transmitted by the measured radio transmitter. This only provides some assurance that the Device is within range of the transmitter.

As with location validation, a Device might still be able to provide falsified measurements that could alter the value of the location information as long as the result is within this region.

Requesting additional supporting observations can reduce the size of the region over which location information can be altered by an attacker, or increase trust in the result, but each additional measurement imposes an acquisition cost. Supporting observations contribute little or nothing toward the primary goal of determining the location of the Device.

7.2.4. Attribution

Lying by proxy (Section 7.1.4) relies on the location recipient being able to attribute location information to a LIS. The effectiveness of this attack is negated if location information is explicitly attributed to a particular source.

This requires an extension to the location object that explicitly identifies the source (or sources) of each item of location information.

Rather than relying on a process that seeks to ensure that location information is accurate, this approach instead provides a location recipient with the information necessary to reach their own conclusion about the trustworthiness of the location information.

Including an authenticated identity for all sources of measurement data presents a number of technical and operational challenges. It is possible that the LIS has a transient relationship with a Device. A Device is not expected to share authentication information with a LIS. There is no assurance that Device identification is usable by a potential location recipient. Privacy concerns might also prevent the sharing of identification information, even if it were available and usable.

Identifying the type of measurement source allows a location recipient to make a decision about the trustworthiness of location information without depending on having authenticated identity information for each source. An element for this purpose is defined in Section 4.4.

When including location information that is based on measurement data from sources that might be untrusted, a LIS SHOULD include alternative location information that is derived from trusted sources of measurement data. Each item of location information can then be labeled with the source of that data.

A location recipient that is able to identify a specific source of measurement data (whether it be LIS or Device) can use this information to attribute location information to either entity or to both entities. The location recipient is then better able to make decisions about trustworthiness based on the source of the data.

A location recipient that does not understand the "source" element is unable to make this distinction. When constructing a PIDF-LO document, trusted location information MUST be placed in the PIDF-LO so that it is given higher priority to any untrusted location information according to Rule #8 of [RFC5491].

Attribution of information does nothing to address attacks that alter the observed parameters that are used in location determination (Section 7.1.6).

7.2.5. Stateful Correlation of Location Requests

Stateful examination of requests can be used to prevent a Device from attempting to map network topology using requests for location information (Section 7.1.2).

Simply limiting the rate of requests from a single Device reduces the amount of data that a Device can acquire about network topology. A LIS could also make observations about the movements of a Device. A Device that is attempting to gather topology information is likely to be assigned a location that changes significantly between subsequent requests, possibly violating physical laws (or lower limits that might still be unlikely) with respect to speed and acceleration.

7.3. An Unauthorized or Compromised LIS

A compromised LIS, or a compromise in LIS discovery [RFC5986], could lead to an unauthorized entity obtaining measurement data. This information could then be used or redistributed. A Device MUST ensure that it authenticates a LIS, as described in Section 9 of [RFC5985].

An entity that is able to acquire measurement data can, in addition to using those measurements to learn the location of a Device, also use that information for other purposes. This information can be used to provide insight into network topology (Section 7.1.2).

Measurement data might also be exploited in other ways. For example, revealing the type of 802.11 transceiver that a Device uses could allow an attacker to use specific vulnerabilities to attack a Device. Similarly, revealing information about network elements could enable targeted attacks on that infrastructure.

8. Measurement Schemas

The schemas are broken up into their respective functions. A base container schema into which all measurements are placed is defined, including the definition of a measurement request (Section 8.1). A PIDF-LO extension is defined in a separate schema (Section 8.2). A basic Types Schema contains common definitions, including the "rmsError" and "samples" attributes, plus types for IPv4, IPv6, and MAC addresses (Section 8.3). Each of the specific measurement types is defined in a separate schema.

8.1. Measurement Container Schema

```
<?xml version="1.0"?>
<xs:schema
    xmlns:lm="urn:ietf:params:xml:ns:geopriv:lm"
    xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="urn:ietf:params:xml:ns:geopriv:lm"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:lm">
    </xs:appinfo>
    <xs:documentation
        source="http://www.rfc-editor.org/rfc/rfc7105.txt">
        This schema defines a framework for location measurements.
    </xs:documentation>
  </xs:annotation>

 <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>

  <xs:element name="measurements">
    <xs:complexType>
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence>
        <xs:any namespace="##other" processContents="lax"
                minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="time" type="xs:dateTime"/>
          <xs:attribute name="timeError" type="bt:positiveDouble"/>
          <xs:attribute name="expires" type="xs:dateTime"/>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>

  <xs:element name="measurementRequest"
          type="lm:measurementRequestType"/>
  <xs:complexType name="measurementRequestType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:sequence>
          <xs:element ref="lm:measurement"
                      minOccurs="0" maxOccurs="unbounded"/>
```

```
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:element name="measurement" type="lm:measurementType"/>
    <xs:complexType name="measurementType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="type" type="xs:QName" use="required"/>
          <xs:attribute name="samples" type="xs:positiveInteger"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <!-- PIDF-LO extension for source -->
    <xs:element name="source" type="lm:sourceType"/>
    <xs:simpleType name="sourceType">
      <xs:list>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="lis"/>
            <xs:enumeration value="device"/>
            <xs:enumeration value="other"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:list>
    </xs:simpleType>
  </xs:schema>
```

Measurement Container Schema

8.2. Measurement Source Schema

```
<?xml version="1.0"?>
<xs:schema
    xmlns:lmsrc="urn:ietf:params:xml:ns:pidf:geopriv10:lmsrc"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10:lmsrc"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:pidf:geopriv10:lmsrc">
    </xs:appinfo>
    <xs:documentation
        source="http://www.rfc-editor.org/rfc/rfc7105.txt">
        This schema defines an extension to PIDF-LO that indicates
        the type of measurement source that produced the measurement
        data used in generating the associated location information.
    </xs:documentation>
  </xs:annotation>

  <xs:element name="source" type="lmsrc:sourceType"/>
  <xs:simpleType name="sourceType">
    <xs:list>
      <xs:simpleType>
        <xs:restriction base="xs:token">
          <xs:enumeration value="lis"/>
          <xs:enumeration value="device"/>
          <xs:enumeration value="other"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:list>
  </xs:simpleType>
</xs:schema>
```

Measurement Source PIDF-LO Extension Schema

8.3. Base Types Schema

Note that the pattern rules in the following schema wrap due to length constraints. None of the patterns contain whitespace.

```
<?xml version="1.0"?>
<xs:schema
  xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:lm:basetypes">
    </xs:appinfo>
    <xs:documentation
        source="http://www.rfc-editor.org/rfc/rfc7105.txt">
        This schema defines a set of base type elements.
    </xs:documentation>
  </xs:annotation>

  <xs:simpleType name="byteType">
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="255"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="twoByteType">
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="65535"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="nonNegativeDouble">
    <xs:restriction base="xs:double">
      <xs:minInclusive value="0.0"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="positiveDouble">
    <xs:restriction base="bt:nonNegativeDouble">
      <xs:minExclusive value="0.0"/>
    </xs:restriction>
  </xs:simpleType>
```

```
<xs:complexType name="doubleWithRMSError">
  <xs:simpleContent>
    <xs:extension base="xs:double">
      <xs:attribute name="rmsError" type="bt:positiveDouble"/>
      <xs:attribute name="samples" type="xs:positiveInteger"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="nnDoubleWithRMSError">
  <xs:simpleContent>
    <xs:restriction base="bt:doubleWithRMSError">
      <xs:minInclusive value="0"/>
    </xs:restriction>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="ipAddressType">
  <xs:union memberTypes="bt:IPv6AddressType bt:IPv4AddressType"/>
</xs:simpleType>

<!-- IPv6 format definition -->
<xs:simpleType name="IPv6AddressType">
  <xs:annotation>
    <xs:documentation>
        An IP version 6 address, based on RFC 4291.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">
    <!-- Fully specified address -->
    <xs:pattern value="[0-9A-Fa-f]{1,4}(:[0-9A-Fa-f]{1,4}){7}"/>
    <!-- Double colon start -->
    <xs:pattern value=":(:[0-9A-Fa-f]{1,4}){1,7}"/>
    <!-- Double colon middle -->
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,6}
                       (:[0-9A-Fa-f]{1,4}){1}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,5}
                       (:[0-9A-Fa-f]{1,4}){1,2}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,4}
                       (:[0-9A-Fa-f]{1,4}){1,3}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,3}
                       (:[0-9A-Fa-f]{1,4}){1,4}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,2}
                       (:[0-9A-Fa-f]{1,4}){1,5}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1}
                       (:[0-9A-Fa-f]{1,4}){1,6}"/>
    <!-- Double colon end -->
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,7}:"/>
```

```
        <!-- IPv4-Compatible and IPv4-Mapped Addresses -->
        <xs:pattern value="((:(:0{1,4}){0,3}:[fF]{4})|(0{1,4}:
            (:0{1,4}){0,2}:[fF]{4})|((0{1,4}:){2}
            (:0{1,4})?:[fF]{4})|((0{1,4}:){3}:[fF]{4})
            |((0{1,4}:){4}[fF]{4})):(25[0-5]|2[0-4][0-9]|
            [0-1]?[0-9]?[0-9])\.(25[0-5]|2[0-4][0-9]|[0-1]
            ?[0-9]?[0-9])\.(25[0-5]|2[0-4][0-9]|[0-1]?
            [0-9]?[0-9])\.(25[0-5]|2[0-4][0-9]|[0-1]?
            [0-9]?[0-9])"/>
        <!-- The unspecified address -->
        <xs:pattern value="::"/>
      </xs:restriction>
    </xs:simpleType>

    <!-- IPv4 format definition -->
    <xs:simpleType name="IPv4AddressType">
      <xs:restriction base="xs:token">
        <xs:pattern value="(25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])\.
                           (25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])\.
                           (25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])\.
                           (25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])"/>
      </xs:restriction>
    </xs:simpleType>

    <!-- MAC address (EUI-48) or EUI-64 address -->
    <xs:simpleType name="macAddressType">
      <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:schema>
```

Base Types Schema

8.4. LLDP Measurement Schema

```
<?xml version="1.0"?>
<xs:schema
    xmlns:lldp="urn:ietf:params:xml:ns:geopriv:lm:lldp"
    xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:lldp"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:lm:lldp">
    </xs:appinfo>
    <xs:documentation
        source="http://www.rfc-editor.org/rfc/rfc7105.txt">
        This schema defines a set of LLDP location measurements.
    </xs:documentation>
  </xs:annotation>

 <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>

  <xs:element name="lldp" type="lldp:lldpMeasurementType"/>
  <xs:complexType name="lldpMeasurementType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:sequence>
          <xs:element name="chassis" type="lldp:lldpDataType"/>
          <xs:element name="port" type="lldp:lldpDataType"/>
          <xs:any namespace="##other" processContents="lax"
                  minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="lldpDataType">
    <xs:simpleContent>
      <xs:extension base="lldp:lldpOctetStringType">
        <xs:attribute name="type" type="bt:byteType"
                      use="required"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
```

```
     <xs:simpleType name="lldpOctetStringType">
       <xs:restriction base="xs:hexBinary">
         <xs:minLength value="1"/>
         <xs:maxLength value="255"/>
       </xs:restriction>
     </xs:simpleType>
   </xs:schema>
```

LLDP Measurement Schema

8.5. DHCP Measurement Schema

```
   <?xml version="1.0"?>
   <xs:schema
       xmlns:dhcp="urn:ietf:params:xml:ns:geopriv:lm:dhcp"
       xmlns:xs="http://www.w3.org/2001/XMLSchema"
       xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
       targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:dhcp"
       elementFormDefault="qualified"
       attributeFormDefault="unqualified">

     <xs:annotation>
       <xs:appinfo
           source="urn:ietf:params:xml:schema:geopriv:lm:dhcp">
       </xs:appinfo>
       <xs:documentation
           source="http://www.rfc-editor.org/rfc/rfc7105.txt">
           This schema defines a set of DHCP location measurements.
       </xs:documentation>
     </xs:annotation>

    <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>

     <!-- DHCP Relay Agent Information option -->
     <xs:element name="dhcp-rai" type="dhcp:dhcpType"/>
     <xs:complexType name="dhcpType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
           <xs:sequence>
             <xs:element name="giaddr" type="bt:ipAddressType"/>
             <xs:element name="circuit"
                         type="xs:hexBinary" minOccurs="0"/>
             <xs:element name="remote"
                         type="dhcp:dhcpRemoteType" minOccurs="0"/>
             <xs:element name="subscriber"
                         type="xs:hexBinary" minOccurs="0"/>
```

```
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="dhcpRemoteType">
      <xs:simpleContent>
        <xs:extension base="xs:hexBinary">
          <xs:attribute name="enterprise" type="xs:positiveInteger"
                        use="optional"/>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>
  </xs:schema>
```

DHCP Measurement Schema

8.6. WiFi Measurement Schema

```
  <?xml version="1.0"?>
  <xs:schema
      xmlns:wifi="urn:ietf:params:xml:ns:geopriv:lm:wifi"
      xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
      xmlns:gml="http://www.opengis.net/gml"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:wifi"
      elementFormDefault="qualified"
      attributeFormDefault="unqualified">

    <xs:annotation>
      <xs:appinfo
          source="urn:ietf:params:xml:schema:geopriv:lm:wifi">
        802.11 location measurements
      </xs:appinfo>
      <xs:documentation
          source="http://www.rfc-editor.org/rfc/rfc7105.txt">
          This schema defines a basic set of 802.11 location
          measurements.
      </xs:documentation>
    </xs:annotation>
```

```
    <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>
     <xs:import namespace="http://www.opengis.net/gml"/>

     <xs:element name="wifi" type="wifi:wifiNetworkType"/>

     <xs:complexType name="wifiNetworkType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
           <xs:sequence>
             <xs:element name="nicType" type="xs:token"
                         minOccurs="0"/>
             <xs:element name="ap" type="wifi:wifiType"
                         maxOccurs="unbounded"/>
           </xs:sequence>
           <xs:anyAttribute namespace="##any" processContents="lax"/>
         </xs:restriction>
       </xs:complexContent>
     </xs:complexType>

     <xs:complexType name="wifiType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
           <xs:sequence>
             <xs:element name="bssid" type="wifi:bssidType"/>
             <xs:element name="ssid" type="wifi:ssidType"
                         minOccurs="0"/>
             <xs:element name="channel" type="xs:nonNegativeInteger"
                         minOccurs="0"/>
             <xs:element name="location" minOccurs="0"
                         type="xs:anyType"/>
             <xs:element name="type" type="wifi:networkType"
                         minOccurs="0"/>
             <xs:element name="regclass" type="wifi:regclassType"
                         minOccurs="0"/>
             <xs:element name="antenna" type="wifi:octetType"
                         minOccurs="0"/>
             <xs:element name="flightTime" minOccurs="0"
                         type="bt:nnDoubleWithRMSError"/>
             <xs:element name="apSignal" type="wifi:signalType"
                         minOccurs="0"/>
             <xs:element name="deviceSignal" type="wifi:signalType"
                         minOccurs="0"/>
             <xs:any namespace="##other" processContents="lax"
                     minOccurs="0" maxOccurs="unbounded"/>
           </xs:sequence>
           <xs:attribute name="serving" type="xs:boolean"
                         default="false"/>
           <xs:anyAttribute namespace="##any" processContents="lax"/>
```

```
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="bssidType">
    <xs:simpleContent>
      <xs:extension base="bt:macAddressType">
        <xs:attribute name="verified" type="xs:boolean"
                      default="false"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <!-- Note that this pattern does not prevent multibyte UTF-8
       sequences that result in an SSID longer than 32 octets. -->
  <xs:simpleType name="ssidType">
    <xs:restriction base="xs:token">
      <xs:pattern value="(\\[\da-fA-F]{2}|[^\\]){0,32}"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="networkType">
    <xs:restriction base="xs:token">
      <xs:pattern value="[a-zA-Z]+"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="regclassType">
    <xs:simpleContent>
      <xs:extension base="wifi:octetType">
        <xs:attribute name="country">
          <xs:simpleType>
            <xs:restriction base="xs:token">
              <xs:pattern value="[A-Z]{2}[OIX]?"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:simpleType name="octetType">
    <xs:restriction base="xs:nonNegativeInteger">
      <xs:maxInclusive value="255"/>
    </xs:restriction>
  </xs:simpleType>
```

```
    <xs:complexType name="signalType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence>
            <xs:element name="transmit" type="xs:double"
                        minOccurs="0"/>
            <xs:element name="gain" type="xs:double" minOccurs="0"/>
            <xs:element name="rcpi" type="wifi:rssiType"
                        minOccurs="0"/>
            <xs:element name="rsni" type="bt:doubleWithRMSError"
                        minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="rssiType">
      <xs:simpleContent>
        <xs:extension base="bt:doubleWithRMSError">
          <xs:attribute name="dBm" type="xs:boolean" default="true"/>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>

    <!-- Measurement Request elements -->
    <xs:element name="type" type="wifi:networkType"/>
    <xs:element name="parameter" type="wifi:parameterType"/>

    <xs:complexType name="parameterType">
      <xs:simpleContent>
        <xs:extension base="xs:QName">
          <xs:attribute name="context" use="optional">
            <xs:simpleType>
              <xs:restriction base="xs:token">
                <xs:enumeration value="ap"/>
                <xs:enumeration value="device"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:attribute>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>
  </xs:schema>
```

WiFi Measurement Schema

8.7. Cellular Measurement Schema

```
<?xml version="1.0"?>
<xs:schema
    xmlns:cell="urn:ietf:params:xml:ns:geopriv:lm:cell"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:cell"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:lm:cell">
    </xs:appinfo>
    <xs:documentation
        source="http://www.rfc-editor.org/rfc/rfc7105.txt">
        This schema defines a set of cellular location measurements.
    </xs:documentation>
  </xs:annotation>

  <xs:element name="cellular" type="cell:cellularType"/>

  <xs:complexType name="cellularType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:sequence>
          <xs:choice>
            <xs:element name="servingCell" type="cell:cellType"/>
            <xs:element name="observedCell" type="cell:cellType"/>
          </xs:choice>
          <xs:element name="observedCell" type="cell:cellType"
                      minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##any" processContents="lax"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="cellType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:choice>
          <xs:sequence>
            <xs:element name="mcc" type="cell:mccType"/>
            <xs:element name="mnc" type="cell:mncType"/>
            <xs:choice>
              <xs:sequence>
                <xs:choice>
```

```
                    <xs:element name="rnc" type="cell:cellIdType"/>
                    <xs:element name="lac" type="cell:cellIdType"/>
                  </xs:choice>
                  <xs:element name="cid" type="cell:cellIdType"/>
                </xs:sequence>
                <xs:element name="eucid" type="cell:cellIdType"/>
              </xs:choice>
              <xs:any namespace="##other" processContents="lax"
                      minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:sequence>
              <xs:element name="sid" type="cell:cellIdType"/>
              <xs:element name="nid" type="cell:cellIdType"/>
              <xs:element name="baseid" type="cell:cellIdType"/>
              <xs:any namespace="##other" processContents="lax"
                      minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:choice>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:simpleType name="mccType">
      <xs:restriction base="xs:token">
        <xs:pattern value="[0-9]{3}"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="mncType">
      <xs:restriction base="xs:token">
        <xs:pattern value="[0-9]{2,3}"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="cellIdType">
      <xs:restriction base="xs:nonNegativeInteger">
        <xs:maxInclusive value="268435455"/> <!-- 2^28 (eucid) -->
      </xs:restriction>
    </xs:simpleType>

    <!-- Measurement Request elements -->
    <xs:element name="type" type="cell:typeType"/>
    <xs:simpleType name="typeType">
      <xs:restriction base="xs:token">
        <xs:enumeration value="gsm"/>
        <xs:enumeration value="umts"/>
```

```
        <xs:enumeration value="lte"/>
        <xs:enumeration value="cdma"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:element name="network" type="cell:networkType"/>
    <xs:complexType name="networkType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:choice>
            <xs:sequence>
              <xs:element name="mcc" type="cell:mccType"/>
              <xs:element name="mnc" type="cell:mncType"/>
            </xs:sequence>
            <xs:element name="nid" type="cell:cellIdType"/>
          </xs:choice>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:schema>
```

Cellular Measurement Schema

8.8. GNSS Measurement Schema

```
  <?xml version="1.0"?>
  <xs:schema
      xmlns:gnss="urn:ietf:params:xml:ns:geopriv:lm:gnss"
      xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:gnss"
      elementFormDefault="qualified"
      attributeFormDefault="unqualified">

    <xs:annotation>
      <xs:appinfo
          source="urn:ietf:params:xml:schema:geopriv:lm:gnss">
      </xs:appinfo>
      <xs:documentation
          source="http://www.rfc-editor.org/rfc/rfc7105.txt">
          This schema defines a set of GNSS location measurements.
      </xs:documentation>
    </xs:annotation>
```

```
    <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>

     <!-- GNSS -->
     <xs:element name="gnss" type="gnss:gnssMeasurementType">
       <xs:unique name="gnssSatellite">
         <xs:selector xpath="sat"/>
         <xs:field xpath="@num"/>
       </xs:unique>
     </xs:element>

     <xs:complexType name="gnssMeasurementType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
           <xs:sequence>
             <xs:element name="gnssTime" type="bt:nnDoubleWithRMSError"
                         minOccurs="0"/>
             <xs:element name="sat" type="gnss:gnssSatelliteType"
                         minOccurs="1" maxOccurs="64"/>
             <xs:any namespace="##other" processContents="lax"
                     minOccurs="0" maxOccurs="unbounded"/>
           </xs:sequence>
           <xs:attribute name="system" type="xs:token" use="required"/>
           <xs:attribute name="signal" type="xs:token"/>
           <xs:anyAttribute namespace="##any" processContents="lax"/>
         </xs:restriction>
       </xs:complexContent>
     </xs:complexType>

     <xs:complexType name="gnssSatelliteType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
           <xs:sequence>
             <xs:element name="doppler" type="bt:doubleWithRMSError"/>
             <xs:element name="codephase"
                         type="bt:nnDoubleWithRMSError"/>
             <xs:element name="cn0" type="bt:nonNegativeDouble"/>
             <xs:element name="mp" type="bt:positiveDouble"
                         minOccurs="0"/>
             <xs:element name="cq" type="gnss:codePhaseQualityType"
                         minOccurs="0"/>
             <xs:element name="adr" type="xs:double" minOccurs="0"/>
           </xs:sequence>
           <xs:attribute name="num" type="xs:positiveInteger"
                         use="required"/>
         </xs:restriction>
       </xs:complexContent>
     </xs:complexType>
```

```
     <xs:complexType name="codePhaseQualityType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
           <xs:attribute name="continuous" type="xs:boolean"
                         default="true"/>
           <xs:attribute name="direct" use="required">
             <xs:simpleType>
               <xs:restriction base="xs:token">
                 <xs:enumeration value="direct"/>
                 <xs:enumeration value="inverted"/>
               </xs:restriction>
             </xs:simpleType>
           </xs:attribute>
         </xs:restriction>
       </xs:complexContent>
     </xs:complexType>
   </xs:schema>
```

GNSS Measurement Schema

8.9. DSL Measurement Schema

```
   <?xml version="1.0"?>
   <xs:schema
       xmlns:dsl="urn:ietf:params:xml:ns:geopriv:lm:dsl"
       xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
       xmlns:xs="http://www.w3.org/2001/XMLSchema"
       targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:dsl"
       elementFormDefault="qualified"
       attributeFormDefault="unqualified">

     <xs:annotation>
       <xs:appinfo
           source="urn:ietf:params:xml:schema:geopriv:lm:dsl">
         DSL measurement definitions
       </xs:appinfo>
       <xs:documentation
           source="http://www.rfc-editor.org/rfc/rfc7105.txt">
           This schema defines a basic set of DSL location measurements.
       </xs:documentation>
     </xs:annotation>
```

```
    <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>

     <xs:element name="dsl" type="dsl:dslVlanType"/>
     <xs:complexType name="dslVlanType">
       <xs:complexContent>
         <xs:restriction base="xs:anyType">
           <xs:choice>
             <xs:element name="l2tp">
               <xs:complexType>
                 <xs:complexContent>
                   <xs:restriction base="xs:anyType">
                     <xs:sequence>
                       <xs:element name="src" type="bt:ipAddressType"/>
                       <xs:element name="dest" type="bt:ipAddressType"/>
                       <xs:element name="session"
                                   type="xs:nonNegativeInteger"/>
                     </xs:sequence>
                   </xs:restriction>
                 </xs:complexContent>
               </xs:complexType>
             </xs:element>
             <xs:sequence>
               <xs:element name="an" type="xs:token"/>
               <xs:group ref="dsl:dslSlotPort"/>
             </xs:sequence>
             <xs:sequence>
               <xs:element name="stag" type="dsl:vlanIDType"/>
               <xs:choice>
                 <xs:sequence>
                   <xs:element name="ctag" type="dsl:vlanIDType"/>
                   <xs:group ref="dsl:dslSlotPort" minOccurs="0"/>
                 </xs:sequence>
                 <xs:group ref="dsl:dslSlotPort"/>
               </xs:choice>
             </xs:sequence>
             <xs:sequence>
               <xs:element name="vpi" type="bt:byteType"/>
               <xs:element name="vci" type="bt:twoByteType"/>
             </xs:sequence>
             <xs:any namespace="##other" processContents="lax"
                     minOccurs="0" maxOccurs="unbounded"/>
           </xs:choice>
           <xs:anyAttribute namespace="##other" processContents="lax"/>
         </xs:restriction>
       </xs:complexContent>
     </xs:complexType>
```

```
    <xs:simpleType name="vlanIDType">
      <xs:restriction base="xs:nonNegativeInteger">
        <xs:maxInclusive value="4095"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:group name="dslSlotPort">
      <xs:sequence>
        <xs:element name="slot" type="xs:token"/>
        <xs:element name="port" type="xs:token"/>
      </xs:sequence>
    </xs:group>
  </xs:schema>
```

DSL Measurement Schema

9. IANA Considerations

This section creates a registry for GNSS types (Section 5.5) and registers the namespaces and schemas defined in Section 8.

9.1. IANA Registry for GNSS Types

This document establishes a new IANA registry for "Global Navigation Satellite System (GNSS)" types. The registry includes tokens for the GNSS type and for each of the signals within that type. Referring to [RFC5226], this registry operates under "Specification Required" rules. The IESG will appoint an Expert Reviewer who will advise IANA promptly on each request for a new or updated GNSS type.

Each entry in the registry requires the following information:

GNSS Name: the name of the GNSS

Brief Description: a brief description of the GNSS

GNSS Token: a token that can be used to identify the GNSS

Signals: a set of tokens that represent each of the signals that the system provides

Documentation Reference: a reference to one or more stable, public specifications that outline usage of the GNSS, including (but not limited to) signal specifications and time systems

The registry initially includes two registrations:

GNSS Name: Global Positioning System (GPS)

Brief Description: a system of satellites that use spread-spectrum transmission, operated by the US military for commercial and military applications

GNSS Token: gps

Signals: L1, L2, L1C, L2C, L5

Documentation Reference: Navstar GPS Space Segment/Navigation User Interface [GPS.ICD]

GNSS Name: Galileo

Brief Description: a system of satellites that operate in the same spectrum as GPS, operated by the European Union for commercial applications

GNSS Token: galileo

Signals: L1, E5A, E5B, E5A+B, E6

Documentation Reference: Galileo Open Service Signal In Space Interface Control Document (SIS ICD) [Galileo.ICD]

9.2. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:pidf:geopriv10:lmsrc

This section registers a new XML namespace, "urn:ietf:params:xml:ns:pidf:geopriv10:lmsrc", as per the guidelines in [RFC3688].

URI: urn:ietf:params:xml:ns:pidf:geopriv10:lmsrc

Registrant Contact: IETF, GEOPRIV working group (geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>Measurement Source for PIDF-LO</title>
  </head>
```

```
    <body>
      <h1>Namespace for Location Measurement Source</h1>
      <h2>urn:ietf:params:xml:ns:pidf:geopriv10:lmsrc</h2>
      <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
         RFC 7105</a>.</p>
    </body>
  </html>
    END
```

9.3. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm

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

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

Registrant Contact: IETF, GEOPRIV working group (geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>Measurement Container</title>
    </head>
    <body>
      <h1>Namespace for Location Measurement Container</h1>
      <h2>urn:ietf:params:xml:ns:geopriv:lm</h2>
      <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
         RFC 7105</a>.</p>
    </body>
  </html>
    END
```

9.4. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm:basetypes

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

URI: urn:ietf:params:xml:ns:geopriv:lm:basetypes

Registrant Contact: IETF, GEOPRIV working group
(geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>Base Device Types</title>
  </head>
  <body>
    <h1>Namespace for Base Types</h1>
    <h2>urn:ietf:params:xml:ns:geopriv:lm:basetypes</h2>
    <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
       RFC 7105</a>.</p>
  </body>
</html>
  END
```

9.5. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm:lldp

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

URI: urn:ietf:params:xml:ns:geopriv:lm:lldp

Registrant Contact: IETF, GEOPRIV working group
(geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>LLDP Measurement Set</title>
  </head>
```

```
      <body>
        <h1>Namespace for LLDP Measurement Set</h1>
        <h2>urn:ietf:params:xml:ns:geopriv:lm:lldp</h2>
        <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
           RFC 7105</a>.</p>
      </body>
    </html>
      END
```

9.6. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm:dhcp

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

URI: urn:ietf:params:xml:ns:geopriv:lm:dhcp

Registrant Contact: IETF, GEOPRIV working group (geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>DHCP Measurement Set</title>
      </head>
      <body>
        <h1>Namespace for DHCP Measurement Set</h1>
        <h2>urn:ietf:params:xml:ns:geopriv:lm:dhcp</h2>
        <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
           RFC 7105</a>.</p>
      </body>
    </html>
      END
```

9.7. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm:wifi

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

URI: urn:ietf:params:xml:ns:geopriv:lm:wifi

Registrant Contact: IETF, GEOPRIV working group
(geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>WiFi Measurement Set</title>
  </head>
  <body>
    <h1>Namespace for WiFi Measurement Set</h1>
    <h2>urn:ietf:params:xml:ns:geopriv:lm:wifi</h2>
    <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
       RFC 7105</a>.</p>
  </body>
</html>
  END
```

9.8. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm:cell

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

URI: urn:ietf:params:xml:ns:geopriv:lm:cell

Registrant Contact: IETF, GEOPRIV working group
(geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>Cellular Measurement Set</title>
  </head>
```

```
        <body>
          <h1>Namespace for Cellular Measurement Set</h1>
          <h2>urn:ietf:params:xml:ns:geopriv:lm:cell</h2>
          <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
             RFC 7105</a>.</p>
        </body>
      </html>
        END
```

9.9. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm:gnss

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

URI: urn:ietf:params:xml:ns:geopriv:lm:gnss

Registrant Contact: IETF, GEOPRIV working group (geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>GNSS Measurement Set</title>
        </head>
        <body>
          <h1>Namespace for GNSS Measurement Set</h1>
          <h2>urn:ietf:params:xml:ns:geopriv:lm:gnss</h2>
          <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
             RFC 7105</a>.</p>
        </body>
      </html>
        END
```

9.10. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:lm:dsl

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

URI: urn:ietf:params:xml:ns:geopriv:lm:dsl

Registrant Contact: IETF, GEOPRIV working group
(geopriv@ietf.org), Martin Thomson (martin.thomson@gmail.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>DSL Measurement Set</title>
  </head>
  <body>
    <h1>Namespace for DSL Measurement Set</h1>
    <h2>urn:ietf:params:xml:ns:geopriv:lm:dsl</h2>
    <p>See <a href="http://www.rfc-editor.org/rfc/rfc7105.txt">
       RFC 7105</a>.</p>
  </body>
</html>
  END
```

9.11. XML Schema Registration for Measurement Source Schema

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

URI: urn:ietf:params:xml:schema:pidf:geopriv10:lmsrc

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

Schema: The XML for this schema can be found in Section 8.2 of this document.

9.12. XML Schema Registration for Measurement Container Schema

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

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

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

Schema: The XML for this schema can be found in Section 8.1 of this document.

9.13. XML Schema Registration for Base Types Schema

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

URI: urn:ietf:params:xml:schema:geopriv:lm:basetypes

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

Schema: The XML for this schema can be found in Section 8.3 of this document.

9.14. XML Schema Registration for LLDP Schema

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

URI: urn:ietf:params:xml:schema:geopriv:lm:lldp

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

Schema: The XML for this schema can be found in Section 8.4 of this document.

9.15. XML Schema Registration for DHCP Schema

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

URI: urn:ietf:params:xml:schema:geopriv:lm:dhcp

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

Schema: The XML for this schema can be found in Section 8.5 of this document.

9.16. XML Schema Registration for WiFi Schema

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

URI: urn:ietf:params:xml:schema:geopriv:lm:wifi

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

Schema: The XML for this schema can be found in Section 8.6 of this document.

9.17. XML Schema Registration for Cellular Schema

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

URI: urn:ietf:params:xml:schema:geopriv:lm:cell

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

Schema: The XML for this schema can be found in Section 8.7 of this document.

9.18. XML Schema Registration for GNSS Schema

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

URI: urn:ietf:params:xml:schema:geopriv:lm:gnss

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

Schema: The XML for this schema can be found in Section 8.8 of this document.

9.19. XML Schema Registration for DSL Schema

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

URI: urn:ietf:params:xml:schema:geopriv:lm:dsl

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

Schema: The XML for this schema can be found in Section 8.9 of this document.

10. Acknowledgements

Thanks go to Simon Cox for his comments relating to terminology; his comments have helped ensure that this document is aligned with ongoing work in the Open Geospatial Consortium (OGC). Thanks to Neil Harper for his review and comments on the GNSS sections of this

document. Thanks to Noor-E-Gagan Singh, Gabor Bajko, Russell Priebe, and Khalid Al-Mufti for their significant input to, and suggestions for, improving the 802.11 measurements. Thanks to Cullen Jennings for feedback and suggestions. Bernard Aboba provided review and feedback on a range of measurement data definitions. Mary Barnes and Geoff Thompson provided a review and corrections. David Waitzman and John Bressler both noted shortcomings with 802.11 measurements. Keith Drage and Darren Pawson provided expert LTE knowledge.

11. References

11.1. Normative References

[ASCII] ANSI, "US-ASCII. Coded Character Set - 7-Bit American Standard Code for Information Interchange. Standard ANSI X3.4-1986", 1986.

[GPS.ICD] "Navstar GPS Space Segment/Navigation User Interface", ICD GPS-200, April 2000.

[Galileo.ICD] GJU, "Galileo Open Service Signal In Space Interface Control Document (SIS ICD)", May 2006.

[IANA.enterprise] IANA, "Private Enterprise Numbers", 2014, <http://www.iana.org/assignments/enterprise-numbers>.

[IEEE.80211] IEEE, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2012, March 2012.

[IEEE.8021AB] IEEE, "IEEE Standard for Local and Metropolitan Area Networks, Station and Media Access Control Connectivity Discovery", IEEE Std 802.1AB-2009, September 2009.

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

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[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.

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

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

[RFC3993] Johnson, R., Palaniappan, T., and M. Stapp, "Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", RFC 3993, March 2005.

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

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

[RFC4580] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option", RFC 4580, June 2006.

[RFC4649] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option", RFC 4649, August 2006.

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

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

[RFC5985] Barnes, M., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, September 2010.

[RFC5986] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", RFC 5986, September 2010.

[TIA-2000.5] TIA/EIA, "Upper Layer (Layer 3) Signaling Standard for cdma2000(R) Spread Spectrum Systems", TR-45.5 / TSG-C TIA-2000.5-E / C.S0005-E v1.0, September 2009.

[TS.3GPP.23.003]
3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 12.0.0, September 2013, <http://www.3gpp.org/ftp/Specs/html-info/23003.htm>.

11.2. Informative References

[ANSI-TIA-1057]
ANSI/TIA, "Link Layer Discovery Protocol for Media Endpoint Devices", TIA 1057, April 2006.

[DSL.TR025]
Wang, R., "Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL", September 1999.

[DSL.TR101]
Cohen, A. and E. Shrum, "Migration to Ethernet-Based DSL Aggregation", April 2006.

[GPS.SPOOF]
Scott, L., "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Signals", ION-GNSS Portland, Oregon, 2003.

[HARPER] Harper, N., "Server-side GPS and Assisted-GPS in Java", December 2009.

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

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

[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.

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

[RFC6155] Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)", RFC 6155, March 2011.

[RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, July 2011.

Authors' Addresses

Martin Thomson
Mozilla
Suite 300
650 Castro Street
Mountain View, CA 94041
US

EMail: martin.thomson@gmail.com

James Winterbottom
Unaffiliated
AU

EMail: a.james.winterbottom@gmail.com