

GEOPRIV
Internet-Draft
Intended status: Standards Track
Expires: August 13, 2009

H. Schulzrinne, Ed.
Columbia University
H. Tschofenig, Ed.
Nokia Siemens Networks
J. Morris
CDT
J. Cuellar
Siemens
J. Polk
Cisco
February 9, 2009

Geolocation Policy: A Document Format for Expressing Privacy Preferences
for Location Information
draft-ietf-geopriv-policy-20.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](http://www.rfc-editor.org/rfc/rfc2119.txt) and [BCP 79](http://www.rfc-editor.org/rfc/rfc2119.txt).

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

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

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

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

This Internet-Draft will expire on August 13, 2009.

Copyright Notice

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

This document is subject to [BCP 78](http://www.ietf.org/rfc/rfc2119.txt) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document defines an authorization policy language for controlling access to location information. It extends the Common Policy authorization framework to provide location-specific access control. More specifically, this document defines condition elements specific to location information in order to restrict access based on the current location of the Target. Furthermore, it offers location-specific transformation elements to reduce the granularity of the returned location information.

Table of Contents

1.	Introduction	5
2.	Terminology	7
3.	Generic Processing	9
3.1.	Structure of Geolocation Authorization Documents	9
3.2.	Rule Transport	9
4.	Location-specific Conditions	10
4.1.	Geodetic Location Condition Profile	10
4.2.	Civic Location Condition Profile	11
5.	Actions	12
6.	Transformations	13
6.1.	Set Retransmission-Allowed	13
6.2.	Set Retention-Expiry	13
6.3.	Set Note-Well	13
6.4.	Keep Ruleset Reference	14
6.5.	Provide Location	14
6.5.1.	Civic Location Profile	15
6.5.2.	Geodetic Location Profile	16
7.	Examples	17
7.1.	Rule Example with Civic Location Condition	17
7.2.	Rule Example with Geodetic Location Condition	18
7.3.	Rule Example with Civic and Geodetic Location Condition	18
7.4.	Rule Example with Location-based Transformations	19
8.	XML Schema for Basic Location Profiles	21
9.	XML Schema for Geolocation Policy	22
10.	XCAP Usage	24
10.1.	Application Unique ID	24
10.2.	XML Schema	24
10.3.	Default Namespace	24
10.4.	MIME Type	24
10.5.	Validation Constraints	24
10.6.	Data Semantics	24
10.7.	Naming Conventions	24
10.8.	Resource Interdependencies	25
10.9.	Authorization Policies	25

<u>11.</u>	<u>IANA Considerations</u>	<u>26</u>
<u>11.1.</u>	<u>Geolocation Policy XML Schema Registration</u>	<u>26</u>
<u>11.2.</u>	<u>Geolocation Policy Namespace Registration</u>	<u>26</u>
<u>11.3.</u>	<u>Geolocation Policy Location Profile Registry</u>	<u>27</u>
<u>11.4.</u>	<u>Basic Location Profile XML Schema Registration</u>	<u>27</u>
<u>11.5.</u>	<u>Basic Location Profile Namespace Registration</u>	<u>28</u>
<u>11.6.</u>	<u>XCAP Application Usage ID</u>	<u>28</u>
<u>12.</u>	<u>Internationalization Considerations</u>	<u>30</u>
<u>13.</u>	<u>Security Considerations</u>	<u>31</u>
<u>14.</u>	<u>References</u>	<u>33</u>
<u>14.1.</u>	<u>Normative References</u>	<u>33</u>
<u>14.2.</u>	<u>Informative References</u>	<u>33</u>
<u>Appendix A.</u>	<u>Acknowledgments</u>	<u>35</u>
	<u>Authors' Addresses</u>	<u>36</u>

1. Introduction

Location information needs to be protected against unauthorized access to preserve the privacy of humans. In [RFC 3693](#) [[RFC3693](#)], a protocol-independent model for access to geographic information is defined. The model includes a Location Generator (LG) that determines location information, a Location Server (LS) that authorizes access to location information, a Location Recipient (LR) that requests and receives location information, and a Rule Maker (RM) that writes authorization policies. An authorization policy is a set of rules that regulates an entity's activities with respect to privacy-sensitive information, such as location information.

The data object containing location information in the context of this document is referred to as a Location Object (LO). The basic rule set defined in the Presence Information Data Format Location Object (PIDF-LO) [[RFC4119](#)] can restrict how long the Location Recipient is allowed to retain the information, and it can prohibit further distribution. It also contains a reference to an enhanced rule set and a human readable privacy policy. The basic rule set, however, does not allow to control access to location information based on specific Location Recipients. This document describes an enhanced rule set that provides richer constraints on the distribution of LOs.

The rule set allows the entity that uses the rules defined in this document to restrict the retention and to enforce access restrictions on location data, including prohibiting any dissemination to particular individuals, during particular times or when the Target is located in a specific region. The RM can also stipulate that only certain parts of the Location Object are to be distributed to recipients or that the resolution of parts of the Location Object is reduced.

The typical sequence of operations is as follows. A Location Server receives a query for location information for a particular Target, via the using protocol [[RFC3693](#)]. The using protocol provides the identity of the requestor, either at the time of the query or when subscribing to the location information. The authenticated identity of the Location Recipient, together with other information provided by the using protocol or generally available to the server, is then used for searching through the rule set. If more than one rule matches the condition element, then the combined permission is evaluated according to the description in [Section 10 of \[RFC4745\]](#). The result of the rule evaluation is applied to the location information, yielding a possibly modified Location Object that is delivered to the Location Recipient.

This document does not describe the protocol used to convey location information from the Location Server to the Location Recipient (i.e., the using protocol; see [RFC 3693](#) [[RFC3693](#)]).

This document extends the Common Policy framework defined in [[RFC4745](#)]. That document provides an abstract framework for expressing authorization rules. As specified there, each such rule consists of conditions, actions and transformations. Conditions determine under which circumstances the entity executing the rules, for example a Location Server, is permitted to apply actions and transformations. Transformations regulate in a location information context how a Location Server modifies the information elements that are returned to the requestor, for example, by reducing the granularity of returned location information.

The XML schema defined in [Section 9](#) extends the Common Policy schema by introducing new child elements to the condition and transformation elements. This document does not define child elements for the action part of a rule.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

This document reuses the terminology of [RFC 3693](#) [[RFC3693](#)], such as Location Server (LS), Location Recipient (LR), Rule Maker (RM), Target, Location Generator (LG) and Location Object (LO). This document uses the following terminology:

Presentity or Target:

[RFC 3693](#) [[RFC3693](#)] uses the term Target to identify the object or person of which location information is required. The presence model described in [RFC 2778](#) [[RFC2778](#)] uses the term presentity to describe the entity that provides presence information to a presence service. A Presentity in a presence system is a Target in a location information system.

Watcher or Location Recipient:

The receiver of location information is the Location Recipient (LR) in the terminology of [RFC 3693](#) [[RFC3693](#)]. A watcher in a presence system, i.e., an entity that requests presence information about a presentity, is a Location Recipient in a location information system.

Authorization policy:

An authorization policy is given by a rule set. A rule set contains an unordered list of (policy) rules. Each rule has a condition, an action and a transformation component.

Permission:

The term permission refers to the action and transformation components of a rule.

The term 'using protocol' is defined in [[RFC3693](#)] and refers to the protocol that is used to request access to and to return privacy sensitive data items.

In this document we use the term Location Servers as the entities that evaluate the geolocation authorization policies. The

geolocation privacy architecture is, as motivated in [RFC 4079](#) [RFC4079], aligned with the presence architecture and a Presence Server is therefore an entity that distributes location information along with other presence-specific XML data elements.

3. Generic Processing

3.1. Structure of Geolocation Authorization Documents

A geolocation authorization document is an XML document, formatted according to the schema defined in [[RFC4745](#)]. Geolocation authorization documents inherit the MIME type of common policy documents, application/auth-policy+xml. As described in [[RFC4745](#)], this document is composed of rules which contain three parts - conditions, actions, and transformations. Each action or transformation, which is also called a permission, has the property of being a positive grant of information to the Location Recipient. As a result, there is a well-defined mechanism for combining actions and transformations obtained from several sources. This mechanism is privacy safe, since the lack of any action or transformation can only result in less information being presented to a Location Recipient.

3.2. Rule Transport

There are two ways how the authorization rules described in this document may be conveyed between different parties:

- o [RFC 4119](#) [[RFC4119](#)] allows enhanced authorization policies to be referenced via a Uniform Resource Locator (URL) in the 'ruleset-reference' element. The ruleset-reference' element is part of the basic rules that always travel with the Location Object.
- o Authorization policies might, for example, also be stored at a Location Server / Presence Server. The Rule Maker therefore needs to use a protocol to create, modify and delete the authorization policies defined in this document. Such a protocol is available with the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) [[RFC4825](#)].

4. Location-specific Conditions

This section describes the location-specific conditions of a rule. The `<conditions>` element contains zero, one or an unbounded number of `<location-condition>` child element(s). Providing more than one `<location-condition>` element may not be useful since all child elements of the `<conditions>` element must evaluate to TRUE in order for the `<conditions>` element to be TRUE. The `<location-condition>` element MUST contain at least one `<location>` child element. The `<location-condition>` element evaluates to TRUE if any of its child elements is TRUE, i.e., a logical OR.

The `<location>` element has three attributes, namely 'profile', 'xml:lang' and 'label'. The 'profile' attribute allows to indicate the location profile that is included as child elements in the `<location>` element and each profile needs to describe under what conditions each `<location>` element evaluates to TRUE. This document defines two location profiles, one civic and one geodetic location profile, see [Section 4.1](#) and [Section 4.2](#). The 'label' attribute allows a human readable description to be added to each `<location>` element. The 'xml:lang' attribute contains a language tag providing further information for rendering of the content of the 'label' attribute.

The `<location-condition>` and the `<location>` elements provide extension points. If an extension is not understood by the entity evaluating the rules then this rule evaluates to FALSE.

4.1. Geodetic Location Condition Profile

The geodetic location profile is identified by the token 'geodetic-condition'. Rule Makers use this profile by placing a GML [[GML](#)] `<Circle>` element within the `<location>` element (as described in Section 5.2.3 of [[I-D.ietf-geopriv-pdif-lo-profile](#)]).

The `<location>` element containing the information for the geodetic location profile evaluates to TRUE if the current location of the Target is within the described location. Note that the Target's actual location might be represented by any of the location shapes described in [[I-D.ietf-geopriv-pdif-lo-profile](#)]. If the geodetic location of the Target is unknown then the `<location>` element containing the information for the geodetic location profile evaluates to FALSE.

Implementations are REQUIRED to support the following coordinate reference system based on WGS 84 [[NIMA.TR8350.2-3e](#)] based on the European Petroleum Survey Group (EPSG) Geodetic Parameter Dataset (as formalized by the Open Geospatial Consortium (OGC)):

2D: WGS 84 (latitude, longitude), as identified by the URN "urn:ogc:def:crs:EPSG::4326". This is a two dimensional CRS.

A CRS MUST be specified using the above URN notation only, implementations do not need to support user-defined CRSs.

Implementations MUST specify the CRS using the "srsName" attribute on the outermost geometry element. The CRS MUST NOT be changed for any sub-elements. The "srsDimension" attribute MUST be omitted, since the number of dimensions in these CRSs is known.

4.2. Civic Location Condition Profile

The civic location profile is identified by the token 'civic-condition'. Rule Makers use this profile by placing a <civicAddress> element, defined in [[RFC5139](#)], within the <location> element.

All child elements of <location> element that carry civicAddress elements MUST evaluate to TRUE (i.e., logical AND) in order for the <location> element to evaluate to TRUE. For each child element, the value of that element is compared to the value of the same element in the Target's civic location. The child element evaluates to TRUE if the two values are identical based on a bit-by-bit comparison.

If the civic location of the Target is unknown, then the <location> element containing the information for the civic location profile evaluates to FALSE. This case may occur, for example, if location information has been removed by earlier transmitters of location information or if only the geodetic location is known. In general, it is RECOMMENDED behavior for a LS not to apply a translation from geodetic location to civic location (i.e., geocode the location).

5. Actions

This document does not define location-specific actions.

6. Transformations

This document defines several elements that allow Rule Makers to specify transformations that

- o reduce the accuracy of the returned location information, and
- o set the basic authorization policies carried inside the PIDF-LO.

6.1. Set Retransmission-Allowed

This element asks the LS to change or set the value of the `<retransmission-allowed>` element in the PIDF-LO. The data type of the `<set-retransmission-allowed>` element is a boolean.

If the value of the `<set-retransmission-allowed>` element is set to TRUE then the `<retransmission-allowed>` element in the PIDF-LO MUST be set to TRUE. If the value of the `<set-retransmission-allowed>` element is set to FALSE, then the `<retransmission-allowed>` element in the PIDF-LO MUST be set to FALSE.

If the `<set-retransmission-allowed>` element is absent then the value of the `<retransmission-allowed>` element in the PIDF-LO MUST be kept unchanged or, if the PIDF-LO is created for the first time, then the value MUST be set to FALSE.

6.2. Set Retention-Expiry

This transformation asks the LS to change or set the value of the `<retention-expiry>` element in the PIDF-LO. The data type of the `<set-retention-expiry>` element is an integer.

The value provided with the `<set-retention-expiry>` element indicates seconds and these seconds are added to the current date.

If the `<set-retention-expiry>` element is absent then the value of the `<retention-expiry>` element in the PIDF-LO is kept unchanged or, if the PIDF-LO is created for the first time, then the value MUST be set to the current date.

6.3. Set Note-Well

This transformation asks the LS to change or set the value of the `<note-well>` element in the PIDF-LO. The data type of the `<set-note-well>` element is a string.

The value provided with the `<set-note-well>` element contains a privacy statement as a human readable text string and an `'xml:lang'`

attribute denotes the language of the human readable text.

If the <set-note-well> element is absent, then the value of the <note-well> element in the PIDF-LO is kept unchanged or, if the PIDF-LO is created for the first time, then no content is provided for the <note-well> element.

6.4. Keep Ruleset Reference

This transformation allows to influence whether the <external-ruleset> element in the PIDF-LO carries the extended authorization rules defined in [[RFC4745](#)]. The data type of the <keep-rule-reference> element is Boolean.

If the value of the <keep-rule-reference> element is set to TRUE, then the <external-ruleset> element in the PIDF-LO is kept unchanged when included. If the value of the <keep-rule-reference> element is set to FALSE, then the <external-ruleset> element in the PIDF-LO MUST NOT contain a reference to an external rule set. The reference to the ruleset is removed and no rules are carried as MIME bodies (in case of CID URIs).

If the <keep-rule-reference> element is absent, then the value of the <external-ruleset> element in the PIDF-LO is kept unchanged when available or, if the PIDF-LO is created for the first time then the <external-ruleset> element MUST NOT be included.

6.5. Provide Location

The <provide-location> element contains child elements of a specific location profile that controls the granularity of returned location information. This document defines two location profiles, namely:

- o If the <provide-location> element has a <provide-civic> child element then civic location information is disclosed as described in [Section 6.5.1](#), subject to availability.
- o If the <provide-location> element has a <provide-geo> child element then geodetic location information is disclosed as described in [Section 6.5.2](#), subject to availability.

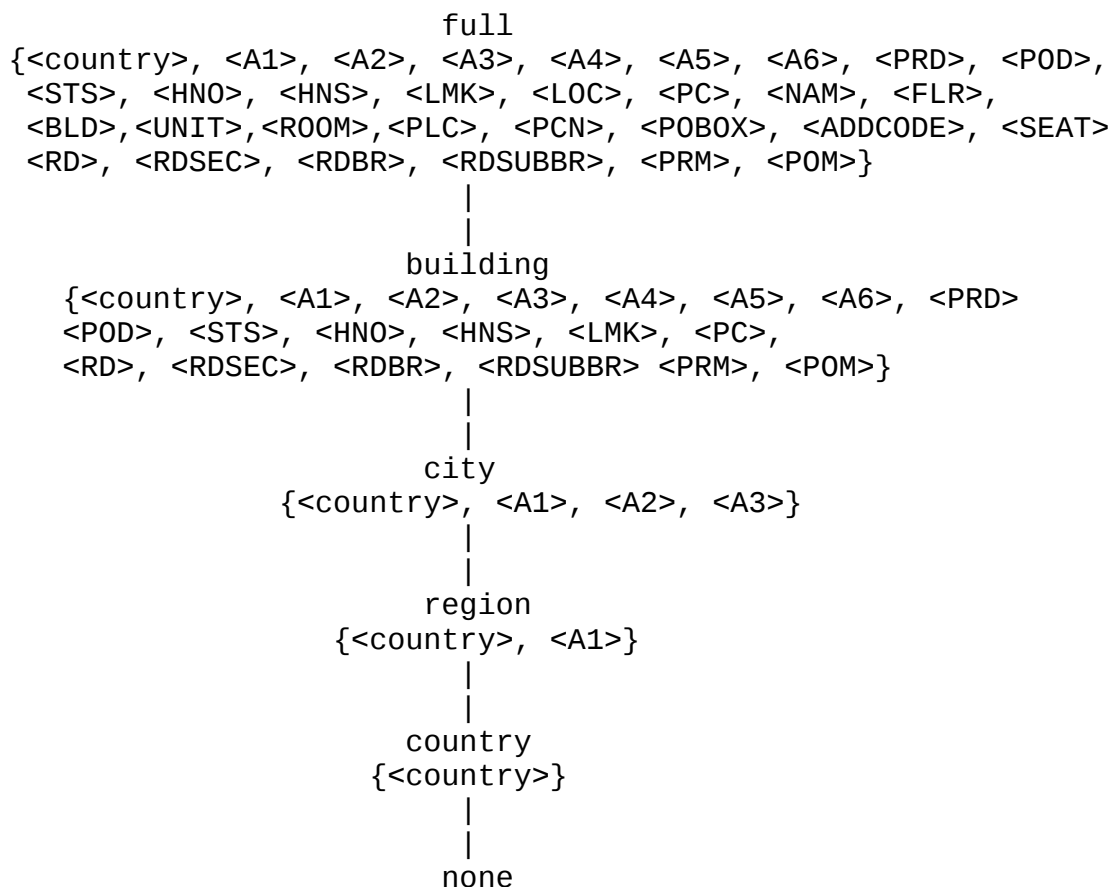
The <provide-location> element MUST contain the 'profile' attribute if it contains child elements and the 'profile' attribute MUST match with the contained child elements.

If the <provide-location> element has no child elements then civic, as well as, geodetic location information is disclosed without reducing its granularity, subject to availability. In this case the profile attribute MUST NOT be included.

6.5.1. Civic Location Profile

This profile uses the token 'civic-transformation'. This profile allows civic location transformations to be specified by means of the <provide-civic> element that restricts the level of civic location information the LS is permitted to disclose. The symbols of these levels are: 'country', 'region', 'city', 'building', 'full'. Each level is given by a set of civic location data items such as <country> and <A1>, ..., <POM>, as defined in [[RFC5139](#)]. Each level includes all elements included by the lower levels.

The 'country' level includes only the <country> element; the 'region' level adds the <A1> element; the 'city' level adds the <A2> and <A3> elements; the 'building' level and the 'full' level add further civic location data as shown below.



{}

The default value is "none".

The schema of the <provide-civic> element is defined in [Section 8](#).

[6.5.2](#). Geodetic Location Profile

This profile uses the token 'geodetic-transformation' and refers only to the Coordinate Reference System (CRS) WGS 84 (urn:ogc:def:crs:EPSG::4326, 2D). This profile allows geodetic location transformations to be specified by means of the <provide-geo> element that may restrict the returned geodetic location information based on the value provided in the 'radius' attribute. The value of the 'radius' attribute expresses the radius in meters.

The schema of the <provide-geo> element is defined in [Section 8](#).

For each rule in the policy specification containing a <provide-geo> element, the LS chooses a circle with a radius F given by the 'radius' attribute of the <provide-geo> element. The center of the circle is chosen randomly, under the constraint that the circle MUST contain the Target's location, which may be a point or another location shape. In response to queries matching this rule, the LS MUST return a shape containing this circle; while the returned shape may change from one query to another, the chosen circle remains constant as long as the Target's location (whether a point or a region) remains completely within the circle. An LS may, for example, store the location of the center or compute it based on a hash function that includes the target's identity. If the Target's location moves within the chosen circle, the LS MAY choose a new random center point, but when the Target's location moves outside the chosen circle, the LS MUST choose a new random center point.

The above-described procedure aims to satisfy the following design goals:

1. The circle returned must contain the actual location of the Target.
2. In general, no point in the circle must be more likely than others to contain the Target.
3. Repeated queries must not reveal the likely location of the Target.

[7.](#) Examples

This section provides a few examples for authorization rules using the extensions defined in this document.

[7.1.](#) Rule Example with Civic Location Condition

This example illustrates a single rule that employs the civic location condition. It matches if the current location of the Target equal the content of the child elements of the <location> element. Requests match only if the Target is at a civic location with country set to 'Germany', state (A1) set to 'Bavaria', city (A3) set to 'Munich', city division (A4) set to 'Perlach', street name (A6) set to 'Otto-Hahn-Ring' and house number (HNO) set to '6'.

No actions and transformation child elements are provided in this rule example. The actions and transformation could include presence specific information when the Geolocation Policy framework is applied to the Presence Policy framework (see [[RFC5025](#)]).

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy">

  <rule id="AA56i09">
    <conditions>
      <gp:location-condition>
        <gp:location
          profile="civic-condition"
          xml:lang="en"
          label="Siemens Neuperlach site 'Legoland'"
          xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
          <country>DE</country>
          <A1>Bavaria</A1>
          <A3>Munich</A3>
          <A4>Perlach</A4>
          <A6>Otto-Hahn-Ring</A6>
          <HNO>6</HNO>
        </gp:location>
      </gp:location-condition>
    </conditions>
    <actions/>
    <transformations/>
  </rule>
</ruleset>
```

[7.2.](#) Rule Example with Geodetic Location Condition

This example illustrates a rule that employs the geodetic location condition. The rule matches if the current location of the Target is inside the area specified by the polygon. The polygon uses the EPSG 4326 coordinate reference system. No altitude is included in this example.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset
  xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:gs="http://www.opengis.net/pidflo/1.0">

  <rule id="BB56A19">
    <conditions>
      <gp:location-condition>
        <gp:location
          xml:lang="en"
          label="Sydney Opera House"
          profile="geodetic-condition">
          <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
            <gml:pos>-33.8570029378 151.2150070761</gml:pos>
            <gs:radius uom="urn:ogc:def:uom:EPSG::9001">1500
            </gs:radius>
          </gs:Circle>
        </gp:location>
      </gp:location-condition>
    </conditions>
    <transformations/>
  </rule>
</ruleset>
```

[7.3.](#) Rule Example with Civic and Geodetic Location Condition

This example illustrates a rule that employs a mixed civic and geodetic location condition. Depending on the available type of location information, namely civic or geodetic location information, one of the location elements may match.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset
  xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:gs="http://www.opengis.net/pidflo/1.0">

  <rule id="AA56i09">
    <conditions>
      <gp:location-condition>
        <gp:location profile="civic-condition"
          xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
          <country>DE</country>
          <A1>Bavaria</A1>
          <A3>Munich</A3>
          <A4>Perlach</A4>
          <A6>Otto-Hahn-Ring</A6>
          <HNO>6</HNO>
        </gp:location>
        <gp:location profile="geodetic-condition">
          <gs:Circle srsName="urn:ogc:def:crs:EPSG::4326">
            <gml:pos>-34.410649 150.87651</gml:pos>
            <gs:radius uom="urn:ogc:def:uom:EPSG::9001">1500
              </gs:radius>
            </gs:Circle>
          </gp:location>
        </gp:location-condition>
      </conditions>
      <actions/>
      <transformations/>
    </rule>
  </ruleset>
```

[7.4.](#) Rule Example with Location-based Transformations

This example shows the transformations specified in this document. The `<provide-civic>` element indicates that the available civic location information is reduced to building level granularity. If geodetic location information is requested then a granularity reduction is provided as well.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy"
  xmlns:lp="urn:ietf:params:xml:ns:basic-location-profiles">

  <rule id="AA56i09">
    <conditions/>
    <actions/>
    <transformations>
      <gp:set-retransmission-allowed>false
      </gp:set-retransmission-allowed>
      <gp:set-retention-expiry>86400</gp:set-retention-expiry>
      <gp:set-note-well xml:lang="en">My privacy policy goes in here.
      </gp:set-note-well>
      <gp:keep-rule-reference>false
      </gp:keep-rule-reference>

      <gp:provide-location
        profile="civic-transformation">
        <lp:provide-civic>building</lp:provide-civic>
      </gp:provide-location>

      <gp:provide-location
        profile="geodetic-transformation">
        <lp:provide-geo radius="500"/>
      </gp:provide-location>

    </transformations>
  </rule>
</ruleset>
```

The following rule describes the short-hand notation for making the current location of the Target available to Location Recipients without granularity reduction.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy">

  <rule id="AA56ia9">
    <conditions/>
    <actions/>
    <transformations>
      <gp:provide-location/>
    </transformations>
  </rule>
</ruleset>
```

8. XML Schema for Basic Location Profiles

This section defines the location profiles used as child elements of the transformation element.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:basic-location-profiles"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <!-- profile="civic-transformation" -->

  <xs:element name="provide-civic" default="none">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="full"/>
        <xs:enumeration value="building"/>
        <xs:enumeration value="city"/>
        <xs:enumeration value="region"/>
        <xs:enumeration value="country"/>
        <xs:enumeration value="none"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>

  <!-- profile="geodetic-transformation" -->

  <xs:element name="provide-geo">
    <xs:complexType>
      <xs:attribute name="radius" type="xs:integer"/>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

9. XML Schema for Geolocation Policy

This section presents the XML schema that defines the Geolocation Policy schema described in this document. The Geolocation Policy schema extends the Common Policy schema (see [[RFC4745](#)]).

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:geolocation-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

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

  <!-- This import brings in the XML language attribute xml:lang-->
  <xs:import namespace="http://www.w3.org/XML/1998/namespace"
    schemaLocation="http://www.w3.org/2001/xml.xsd"/>

  <!-- Geopriv Conditions -->

  <xs:element name="location-condition"
    type="gp:locationconditionType"/>

  <xs:complexType name="locationconditionType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:choice minOccurs="1" maxOccurs="unbounded">
          <xs:element name="location" type="gp:locationType"
            minOccurs="1" maxOccurs="unbounded"/>
          <xs:any namespace="##other" processContents="lax"
            minOccurs="0" maxOccurs="unbounded"/>
        </xs:choice>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="locationType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:choice minOccurs="1" maxOccurs="unbounded">
          <xs:any namespace="##other" processContents="lax"
            minOccurs="0" maxOccurs="unbounded"/>
        </xs:choice>
        <xs:attribute name="profile" type="xs:string"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
```

```
        <xs:attribute name="label" type="xs:string"/>
        <xs:attribute ref="xml:lang" />
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

  <!-- Geopriv transformations -->
  <xs:element name="set-retransmission-allowed"
    type="xs:boolean" default="false"/>
  <xs:element name="set-retention-expiry"
    type="xs:integer" default="0"/>
  <xs:element name="set-note-well"
    type="gp:notewellType"/>
  <xs:element name="keep-rule-reference"
    type="xs:boolean" default="false"/>

  <xs:element name="provide-location"
    type="gp:providelocationType"/>

  <xs:complexType name="notewellType">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute ref="xml:lang" />
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:complexType name="providelocationType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:choice minOccurs="0" maxOccurs="unbounded">
          <xs:any namespace="##other" processContents="lax"
            minOccurs="0" maxOccurs="unbounded"/>
        </xs:choice>
        <xs:attribute name="profile" type="xs:string" />
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>

</xs:schema>
```

[10.](#) XCAP Usage

The following section defines the details necessary for clients to manipulate geolocation privacy documents from a server using XCAP. If used as part of a presence system, it uses the same AUID as those rules. See [[RFC5025](#)] for a description of the XCAP usage in context with presence authorization rules.

[10.1.](#) Application Unique ID

XCAP requires application usages to define a unique application usage ID (AUID) in either the IETF tree or a vendor tree. This specification defines the "geolocation-policy" AUID within the IETF tree, via the IANA registration in [Section 11](#).

[10.2.](#) XML Schema

XCAP requires application usages to define a schema for their documents. The schema for geolocation authorization documents is described in [Section 9](#).

[10.3.](#) Default Namespace

XCAP requires application usages to define the default namespace for their documents. The default namespace is urn:ietf:params:xml:ns:geolocation-policy.

[10.4.](#) MIME Type

XCAP requires application usages to defined the MIME type for documents they carry. Geolocation privacy authorization documents inherit the MIME type of common policy documents, application/auth-policy+xml.

[10.5.](#) Validation Constraints

This specification does not define additional constraints.

[10.6.](#) Data Semantics

This document discusses the semantics of a geolocation privacy authorization.

[10.7.](#) Naming Conventions

When a Location Server receives a request to access location information of some user foo, it will look for all documents within http://[xcaproot]/geolocation-policy/users/foo, and use all documents

found beneath that point to guide authorization policy.

[10.8.](#) Resource Interdependencies

This application usage does not define additional resource interdependencies.

[10.9.](#) Authorization Policies

This application usage does not modify the default XCAP authorization policy, which is that only a user can read, write or modify his/her own documents. A server can allow privileged users to modify documents that they do not own, but the establishment and indication of such policies is outside the scope of this document.

[11.](#) IANA Considerations

There are several IANA considerations associated with this specification.

[11.1.](#) Geolocation Policy XML Schema Registration

URI: urn:ietf:params:xml:schema:geolocation-policy

Registrant Contact: IETF Geopriv Working Group, Hannes Tschofenig (hannes.tschofenig@nsn.com).

XML: The XML schema to be registered is contained in [Section 9](#). Its first line is

```
<?xml version="1.0" encoding="UTF-8"?>
```

and its last line is

```
</xs:schema>
```

[11.2.](#) Geolocation Policy Namespace Registration

URI: urn:ietf:params:xml:ns:geolocation-policy

Registrant Contact: IETF Geopriv Working Group, Hannes Tschofenig (hannes.tschofenig@nsn.com).

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
  "http://www.w3.org/TR/xhtml1-basic/xhtml1-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
    content="text/html; charset=iso-8859-1"/>
  <title>Geolocation Policy Namespace</title>
</head>
<body>
  <h1>Namespace for Geolocation Authorization Policies</h1>
  <h2>urn:ietf:params:xml:schema:geolocation-policy</h2>
  <p>See <a href="[URL of published RFC]">RFCXXXX
    [NOTE TO IANA/RFC-EDITOR:
      Please replace XXXX with the RFC number of this
      specification.]</a>.</p>
</body>
</html>
END
```

[11.3.](#) Geolocation Policy Location Profile Registry

This document seeks to create a registry of location profile names for the Geolocation Policy framework. Profile names are XML tokens. This registry will operate in accordance with [RFC 2434](#) [[RFC2434](#)], Standards Action.

This document defines the following profile names:

geodetic-condition: Defined in [Section 4.1](#).

civic-condition: Defined in [Section 4.2](#).

geodetic-transformation: Defined in [Section 6.5.2](#).

civic-transformation: Defined in [Section 6.5.1](#).

[11.4.](#) Basic Location Profile XML Schema Registration

URI: urn:ietf:params:xml:schema:basic-location-profiles

Registrant Contact: IETF Geopriv Working Group, Hannes Tschofenig
(hannes.tschofenig@nsn.com).

XML: The XML schema to be registered is contained in [Section 8](#). Its first line is

```
<?xml version="1.0" encoding="UTF-8"?>
```

and its last line is

```
</xs:schema>
```

[11.5](#). Basic Location Profile Namespace Registration

URI: urn:ietf:params:xml:ns:basic-location-profiles

Registrant Contact: IETF Geopriv Working Group, Hannes Tschofenig (hannes.tschofenig@nsn.com).

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
    "http://www.w3.org/TR/xhtml1-basic/xhtml1-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
        content="text/html; charset=iso-8859-1"/>
  <title>Basic Location Profile Namespace</title>
</head>
<body>
  <h1>Namespace for Basic Location Profile</h1>
  <h2>urn:ietf:params:xml:ns:basic-location-profiles</h2>
  <p>See <a href="[URL of published RFC]">RFCXXXX
    [NOTE TO IANA/RFC-EDITOR:
      Please replace XXXX with the RFC number of this
      specification.]</a>.</p>
</body>
</html>
END
```

[11.6](#). XCAP Application Usage ID

This section registers an XCAP Application Usage ID (AUID) according to the IANA procedures defined in [\[RFC4825\]](#).

Name of the AUID: geolocation-policy

Description: Geolocation privacy rules are documents that describe the permissions that a Target has granted to Location Recipients that

access information about his/her geographic location.

12. Internationalization Considerations

The policies described in this document are mostly meant for machine-to-machine communications; as such, many of its elements are tokens not meant for direct human consumption. If these tokens are presented to the end user, some localization may need to occur. The policies are, however, supposed to be created with the help of humans and some of the elements and attributes are subject to internationalization considerations. The content of the <label> element is meant to be provided by a human (the Rule Maker) and also displayed to a human. Furthermore, the location condition element (using the civic location profile, see [Section 4.2](#)) and the <set-note-well> element (see [Section 6.3](#)) may contain non-US-ASCII letters.

The geolocation policies utilize XML and all XML processors are required to understand UTF-8 and UTF-16 encodings, and therefore all entities processing these policies MUST understand UTF-8 and UTF-16 encoded XML. Additionally, geolocation policy aware entities MUST NOT encode XML with encodings other than UTF-8 or UTF-16.

13. Security Considerations

This document aims to make it simple for users to prevent the unintended disclosure of private information to third parties. This is accomplished through the usage of authorization policies. Security requirements are described in [[RFC3693](#)] and a discussion of generic security threats is available with [[RFC3694](#)]. Aspects of combining permissions in cases of multiple occurrence are treated in [[RFC4745](#)]).

When the Target is moving then the location transformations reveal information when switching from one privacy region to another one. For example, when a transformation indicates that civic location is provided at a 'building' level of granularity. Hence, room numbers, floors etc. would be hidden. However, when the Target moves from one building to the next one then the movement would still be recognizable as the disclosed location information would be reflected by the new civic location information indicating the new building. With additional knowledge about building entrances and streets it would be possible to learn a certain amount of information. It is therefore important to ensure that selected privacy regions are not chosen too small when mobility is a concern and that a random number is added to the position of the Target, with an absolute value of half the privacy region. The latter aspect is only applicable for geodetic information or when geodetic information is translated to civic information by the Location Server.

There is the risk that end users are specifying their location-based policies in such a way that very small changes in location yields a significantly different level of information disclosure. For example, a user might want to set authorization policies differently when they are in a specific geographical area (e.g., at home, in the office). Location might be the only factor in the policy that triggers a very different action and transformation to be executed. The accuracy of location information is not always sufficient to unequivocally determine whether a location is within a specific boundary [[I-D.thomson-geopriv-uncertainty](#)]. In some situations uncertainty in location information could produce unexpected results from application of policy. Providing adequate user feedback about potential errors arising from these limitation can help prevent unintentional information leakage.

Users might create policies that are non-sensical. To avoid such cases the software used to create the authorization policies should perform consistency checks and when authorization policies are uploaded to the policy servers then further checks are performed. When XCAP is used to upload authorization policies then built-in features of XCAP can be utilized to convey error messages back to the

user about an error condition. [Section 8.2.5 of \[RFC4825\]](#) indicates that some degree of application specific checking is provided when authorization policies are added, modified or deleted. The XCAP protocol may return a 409 response with a response that may contain a detailed conflict report containing the <constraint-failure> element. A human readable description of the problem can be indicated in the 'phrase' attribute of that element.

14. References

14.1. Normative References

- [GML] OpenGIS, "OpenGIS Geography Markup Language (GML) Implementation Specification, Version 3.00, OGC 02 023r4", <http://www.opengeospatial.org/docs/02-023r4.pdf>, January 2003.
- [I-D.ietf-geopriv-pdif-lo-profile] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations", [draft-ietf-geopriv-pdif-lo-profile-14](#) (work in progress), November 2008.
- [NIMA.TR8350.2-3e] OpenGIS, "US National Imagery and Mapping Agency, "Department of Defense (DoD) World Geodetic System 1984 (WGS 84), Third Edition, NIMA TR8350.2", , January 2000.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.
- [RFC4745] Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences", [RFC 4745](#), February 2007.
- [RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", [RFC 5139](#), February 2008.

14.2. Informative References

- [I-D.thomson-geopriv-geo-shape] Thomson, M., "Geodetic Shapes for the Representation of Uncertainty in PIDF-LO", [draft-thomson-geopriv-geo-shape-03](#) (work in progress), December 2006.
- [I-D.thomson-geopriv-uncertainty] Thomson, M. and J. Winterbottom, "Representation of Uncertainty and Confidence in PIDF-LO", [draft-thomson-geopriv-uncertainty-02](#) (work in progress), November 2008.
- [RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#),

October 1998.

- [RFC2778] Day, M., Rosenberg, J., and H. Sugano, "A Model for Presence and Instant Messaging", [RFC 2778](#), February 2000.
- [RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", [RFC 3693](#), February 2004.
- [RFC3694] Danley, M., Mulligan, D., Morris, J., and J. Peterson, "Threat Analysis of the Geopriv Protocol", [RFC 3694](#), February 2004.
- [RFC4079] Peterson, J., "A Presence Architecture for the Distribution of GEOPRIV Location Objects", [RFC 4079](#), July 2005.
- [RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", [RFC 4119](#), December 2005.
- [RFC4825] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", [RFC 4825](#), May 2007.
- [RFC5025] Rosenberg, J., "Presence Authorization Rules", [RFC 5025](#), December 2007.

[Appendix A.](#) Acknowledgments

This document is informed by the discussions within the IETF GEOPRIV working group, including discussions at the GEOPRIV interim meeting in Washington, D.C., in 2003.

We particularly want to thank Allison Mankin <mankin@psg.com>, Randall Gellens <rg+ietf@qualcomm.com>, Andrew Newton <anewton@ecotroph.net>, Ted Hardie <hardie@qualcomm.com>, Jon Peterson <jon.peterson@neustar.biz> for their help in improving the quality of this document.

We would like to thank Christian Guenther for his help with an earlier version of this document. Furthermore, we would like to thank Johnny Vrancken for his document reviews in September 2006, December 2006 and January 2007. James Winterbottom provided a detailed review in November 2006. Richard Barnes gave a detailed review in February 2008.

This document uses text from [[I-D.thomson-geopriv-geo-shape](#)]. Therefore, we would like to thank Martin Thomson for his work in [[I-D.thomson-geopriv-geo-shape](#)]. We would also like to thank Martin Thomson, Matt Lepinski and Richard Barnes for their comments regarding the geodetic location transformation procedure. Richard provided us with a detailed text proposal.

We would like to thank Dan Romascanu, Yoshiko Chong and Jari Urpalainen for their last call comments.

Finally, we would like to thank the following individuals for their feedback as part of the IESG, GenArt, and SecDir review: Jari Arkko, Eric Gray, Russ Housley, Carl Reed, Martin Thomson, Lisa Dusseault, Chris Newman, Jon Peterson, Sam Hartman, Cullen Jennings, Tim Polk, and Brian Rosen.

Authors' Addresses

Henning Schulzrinne (editor)
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
USA

Phone: +1 212 939 7042
Email: schulzrinne@cs.columbia.edu
URI: <http://www.cs.columbia.edu/~hgs>

Hannes Tschofenig (editor)
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

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

John B. Morris, Jr.
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
USA

Email: jmorris@cdt.org
URI: <http://www.cdt.org>

Jorge R. Cuellar
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Jorge.Cuellar@siemens.com

James Polk
Cisco
2200 East President George Bush Turnpike
Richardson, Texas 75082
USA

Email: jmpolk@cisco.com