GEOPRIV
Internet-Draft
Expires: August 15, 2006

H. Schulzrinne
Columbia U.
H. Tschofenig
Siemens
J. Morris
CDT
J. Cuellar
Siemens
J. Polk
Cisco

February 11, 2006

A Document Format for Expressing Privacy Preferences for Location Information

draft-ietf-geopriv-policy-08.txt

Status of this Memo

Copyright Notice

Abstract

This document defines an authorization policy language for controling access to location information. It extends the authorization framework of the common policy markup language to provide location-specific access control.

Table of Contents

1. Introduction

Location information needs to be protected against unauthorized access to preserve the privacy of the subject of the location information. In [RFC3693], a protocol-independent model for access to geographic information was defined. The model includes a Location Generator (LG) that produces Location Information (LI), a Location Server (LS) that authorizes access to LI, a location recipient (LR) that requests and receives information, and a Rulemaker (RM) that provides authorization policy rules. An authorization policy is a set of rules that regulate an entity's activities with respect to privacy-sensitive information such as location information. The data object containing LI is referred to as Location Object (LO).

The basic rule set defined in PIDF-LO [RFC4119] can restrict how long the receiver can retain the information and it can prohibitfurther distribution of the information. It does not allow to customize information to specific receivers, for example. This document describes an enhanced rule set that provides richer constraints on the distribution of LOs.

We refer to any entity that uses the rules in this document to restrict the retention or distribution of information as a Rule Enforcer (RE). The rule set allows the RE 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 limited.

The sequence of operations is as follows. The location server receives a query for location information for a particular Target, via the using protocol. 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. All matching rules are combined according to a merging algorithm described in [I-D.ietf-geopriv-common-policy]. The resulting rule is applied to the location data, yielding a possibly modified location object that is delivered to the location recipient.

This document does not describe or mandate the protocol used to deliver location information from the location server to the location recipient, nor the protocol to update the policies or the protocol that is used by the location generator to convey location information

to the location server.

This document extends the framework defined in [I-D.ietf-geopriv-common-policy]. That document provides an abstract framework for expressing authorization policy rules. As specified there, each such rule consists of conditions, actions and transformations.'Conditions determine under which circumstances the location server is permitted to perform actions and transformations. Transformations regulate how a location server handles location objects; it might limit when and how data and policy can be distributed and may modify the information elements that are returned to the requestor, e.g., reducing the granularity of location information).

The XML schema in Section 10 extends the XML-based authorization framework (see [I-D.ietf-geopriv-common-policy]) by introducing new members of the condition and transformation substitution groups defined there. The schema does not define new actions. To express civic location information, it makes use of that schema in [RFC4119] that defines the 'civicAddress' complex type.

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 [RFC2119].

This document reuses the terminology of [RFC3693], e.g., the terms Location Server (LS) and Location Recipient (LR). This document and the common policy document [I-D.ietf-geopriv-common-policy] share the following terminology:

Presentity or target: RFC 3693 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. In a presence system, the target is the presentity.

Watcher or Location Recipient: The receiver of location information is the Location Recipient (LR) in the terminology of RFC 3693. A watcher, i.e., an entity that requests presence information about a presentity, is a location recipient in presence systems.

Authorization policy: An authorization policy is given by a rule set. A rule set contains an unordered list of rules. A rule has a conditions, an actions and a transformations part.

Permission: The term permission indicates the action and transformation components of a rule.

The terms 'authorization policy', 'policy' and 'rule set' are used interchangeable. The terms 'authorization policy rule', 'policy rule' and 'rule' are used interchangeable.

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

The geo privacy policy markup language refers to the authorization language defined in this document. The common policy markup language refers to the authorization language described in [I-D.ietf-geopriv-common-policy].

3. Basic Data Model and Processing

Since the geo privacy policy markup language defined in Section 10 extends the common policy markup language in [I-D.ietf-geopriv-common-policy], this document adopts the basic data model as introduced in Section 6 of [I-D.ietf-geopriv-common-policy].

4. Rule Transport

The XML data format of the GEOPRIV location object is specified in[RFC4119]. The definition of the location object there allows enhanced authorization policies associated to the location object to be referenced via a URL in the 'ruleset-reference' element containing an URI that indicates where a rule set related to the location object can be found.

One of the transformations of the rule set is the removal of the rule set described here before transmission. Only the whole rule set can be removed and not individual elements such as only some conditions. Before transmitting the rules to the location recipient, unless explicitly permitted by the authorization policy, the rule set MUST be removed from the location object, since the rule set might disclose which entities the rule maker trusts (see Section 8).

5. Securing the Location Object

The GEOPRIV requirements document [RFC3693] addresses the minimal security protection required for the LO, namely mutual end-point authentication, data object integrity, data object confidentiality and replay protection. As proposed in[RFC4119], S/MIME SHOULD be used. Protection for the location object also includes an attached rule set.

Protection is likely to be necessary against adversaries who eavesdrop on the communication between the location server and the location recipient or the location generator and the location server, who tamper with the location object or who replay previously recorded location objects. Securing the communication between rule maker and location server depends on the protocol which is used to perform the desired actions (e.g., https). The communication between the location generator and the location server can also be secured using channel security.

If the location object is integrity and confidentiality-protected, then the receiving entity (location server or location recipient) has to be able to decrypt and to verify the location object. Since the authorization policy rules described in this document allow the modification of the location object, by granularity reduction or by setting flags, it is not possible to forward the location object without reapplying the cryptographic protection. This applies especially to the location server as it is not the final consumer of the location object.

When the location server protects the location object for transmission to the location recipient after successful authorization, then the authenticated identity can be used to select a security association to apply proper protection of the location object. Securing the location object for multiple recipients is currently not provided.

Instead of encrypting the location object, the location generator could digitally sign the location object, offering integrity protection, but no confidentiality. However, if the location server needs to modify the location object, it would have to break the digital signature and then apply its own digital signature.

Since the location object is generally distributed to more than one location recipient, the location generator lacks the necessary information about the recipient and thus cannot usually apply confidentially protection.

By default, the location server re-signs location objects if the

signed location object has been modified according to the rule set. If the location server receives a location object that it cannot decrypt, it discards it if and only if the rule requires modification of the content.

6. Conditions

This section describes the location-specific conditions in a rule, namely the civic and geo-spatial location conditions. The XML elements and attributes shown below are defined by the XML schema in Section 10.

6.1. Civic Location Condition

The <civic-loc-condition> element matches if the current location of the target matches all the values specified in the child elements of this element. The <civic-loc-condition> is of the 'civicAddress' complex type defined in [RFC4119]. It includes a number of fields, including the country, expressed as a two-letter ISO 3166 code, and the administrative units A1 through A6 of [I-D.ietf-geopriv-dhcp-civil]. This designation offers street-level precision.

If the civic location of the target is not known, rules that contain a civic location condition never match. This case may occur, for example, if location information has been removed by earlier transmitters of location information or if only the geospatial location is known.

If any of the elements <A1> through <A6> are specified, <country> MUST also be specified. The schema does not enforce that the specification uniquely identifies a particular location. For example, it would be possible to omit the region and match only on city name, so that any city sharing that name within a country would match. This feature is primarily designed to deal with users that may not know the administrative divisions between county and city level. For example, many users may not know the county for cities in the United States.

6.2. Geospatial Location Condition

The geospatial location condition allows to make authorization decisions based on the current geospatial location of the target. A rule matches if the current location of the Target is contained in either the identified polygon (see Section 6.2.1) or between a range

of altitude values (see Section 6.2.2).

6.2.1. Polygon

The condition matches if the longitude and latitude values of the polygon, interpreted as x and y coordinates on a plane, enclose the current location of the target.

There are a number of algorithms for determining whether a point is

inside a polygon. A common algorithm draws a ray from the test point to the right. The test point is inside if and only if the ray intersects the line segments making up the polygon an odd number of times.

The listed points, which constitute the polygon, MUST be listed as they appear in a clockwise direction all the way around the perimeter of the single plane shape. This is the defined concept of a "Ring" within GML [GML]. The final point MUST be a repeat of the first point listed to enclose the polygon.

6.2.2. Altitude

The altitude condition matches if the target altitude is defined and falls between the low and high altitude stated in the rule, measured in meters above the WGS84 sphere. If either element is omitted, the altitude range is an open range.

7. Actions

According to the common policy framework [I-D.ietf-geopriv-common-policy], actions and transformations included in a rule determine which operations the location server MUST execute after having received a location data access request from a location recipient that matches all conditions of this rule. Transformations regulate the location server operations that directly influence the handling of location information. Actions, on the other hand, specify all remaining types of operations the location server is obliged to execute, i.e., all operations that are not of transformation type. This document does not define new, location-specific actions.

8. Transformations

This policy markup language defines several elements by means of which rulemakers can specify transformations. These transformations determine whether the location server may distribute the location object at all and, if so, limits the accuracy of the location object passed by the location server to the recipient.

All transformations defined in this section are privacy-safe in the sense that if the evaluation of the authorization policy related to a given location object does not produce an explicit transformation instruction, the location server MUST execute the transformation in question to ensure minimal discloure of privacy-sensitive information.

Extensions to this document may define other transformations.

8.1. Distribution Transformation

This transformation can be specified by means of the <distribution-transformation> element whose value is of boolean type. A location server is allowed to distribute this location object if and only if all of the following conditions are satisfied:

1. the authorization policy related to the location object contains a rule with a <distribution-transformation> element,

2. at least one of the rules safisfying (1) matches, and

3. the combined value of this permission is 'true' (see [I-D.ietf-geopriv-common-policy] for the term 'combined value').

In all other cases, the location server MUST NOT distribute the location object in question. In particular, this also comprises the case of an authorization policy that does not contain a rule with a <distribution-transformation> element.

8.2. Retention Transformation

This transformation can be specified by means of the <retention-transformation> element whose value is of integer type. A location server is allowed to retain a location object for the maximum retention time after receiving the location object, if and only if all of the following conditions are satisfied:

1. the authorization policy related to the location object contains a rule with a <retention-transformation> element,

2. at least one of the rules satisfying (1) matches, and

3. the combined value of this permission is the retention time.

In all other cases, the location server MUST delete the location object immediately after completing the service that makes use of the location object, such as delivering it to current subscribers in a presence system.

8.3. Keep Rules Transformation

This transformation can be specified by means of the <keep-rules-transformation> element whose value is of boolean type. For a location object subject to this rule, a location server is allowed to keep all authorization policy rules in the location object when delivering it to the location recipient if and only if all of the following econditions are satisfied:

1. the authorization policy related to the location object contains a rule with a <keep-rules-transformation> element,

2. at least one of the rules satisfying (1) matches, and

3. the combined value of this permission is 'true'.

In all other cases, the location server MUST remove all authorization policy rules from the location object. The rules are referenced from PDIF-LO via the 'ruleset-reference' element either using a URI or a CID URI scheme as described in Section 2.2.2 of [RFC4119].

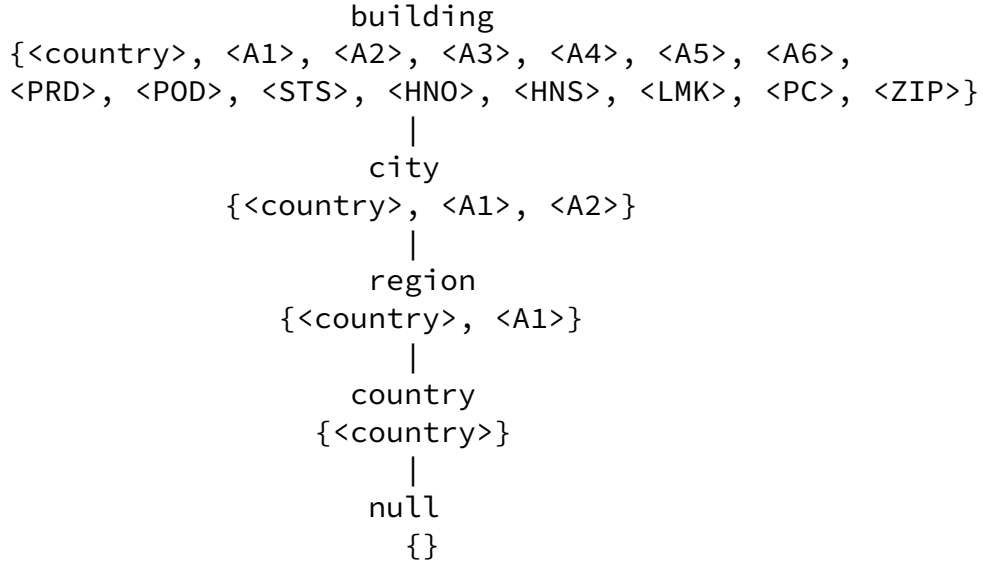
The reference to the ruleset is removed and no rules are carried as MIME bodies (in case of CID URIs).

8.4. Civic Location Transformation

The civic location transformation can be specified by means of the <civic-loc-transformation> element to restrict the level of civic location information the LS is permitted to provide. From lowest to highest level, the names of these levels are: 'null', 'country', 'region', 'city', 'building', 'full'. Each level is given by a set of civic location data items such as <country> and <A1>, ..., <A6>, as defined in [RFC4119]. 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:

full
{<country>, <A1>, <A2>, <A3>, <A4>, <A5>, <A6>, <PRD>, <POD>,
<STS>, <HNO>, <HNS>, <LMK>, <LOC>, <PC>, <NAM>, <FLR>, <ZIP>}
|



With respect to a given LO, a LS is permitted to pass civic location information corresponding to the given LO on at the level L (L = 'country', 'region', 'city', 'building', or 'full'), if and only if all of the following conditions are satisfied:

1. the authorization policy related to the LO contains a rule with a <civic-loc-transformation> element,

2. at least one of the rules satisfying 1) matches, and

3. the combined value of this permission is the level L.

In all other cases, including the case in which no rule of the authorization policy related to the given location object contains a <civic-loc-transformation> element, the location server MUST remove all civic location information from the LO before passing it on, thereby providing the 'null' level of civic location information.

8.5. Geospatial Location Transformation

The geospatial location transformation can be specified by means of the <geospatial-loc-transformation> element to restrict the resolution of the geospatial location information to the value provided in the <latitude-resolution>, <longitude-resolution> and <altitude-resolution> child elements of the <geospatial-loc-transformation> element. The resolution is specified as a positive, non-zero number r. If n is the nominal coordinate value (longitude or latitude), the rounded value is computed as

floor(n/r + 0.5) * r.

For example, if the latitude is n=38.89868 and r=0.01, the latitude value rendered to the recipient of the location object is 38.90. If the longitude is n=77.03723 and r=0.01, the longitude is rendered as 77.04. This computation also works for r that are not integer powers of 10 or r > 1. For example, to round longitude to timezone accuracy, one would use r=15 and obtain a value of 75 in this example.

For a given LO, a LS is allowed to pass the longitude or latitude value corresponding to the given LO on at the resolution value r, if and only if all of the following conditions are satisfied:

1. the authorization policy related to the location object contains a rule with a <geospatial-loc-transformation> element that has a <latitude> element,

2. at least one of the rules satisfying (1) matches, and

3. the combined value of this permission is r.

In all other cases, the LS MUST remove the coordinate value from the geospatial location information.

9. Example

This section gives two simple examples for authorization policy rules that make use of the civic and the geospatial location condition.

9.1. Rule Example with Civic Location Condition

This example illustrates a single rule that employs the civic location condition which matches if the current location of the target is inside the area specified by the child elements of the <civic-loc-condition> element. The syntax of this content complies with the 'civicAddress' complex type defined in [RFC4119]. In this example, requests match only if the Target is at his main office in a Siemens site in Munich.

The rule is valid for one year as specified by the <validity> element. No actions are imposed on LSs. The <transformations> section indicates that LSs are allowed to distribute the LOs with authorization policy included and the full set of civic location information, and to pass latitude and longitude values of geospatial location information on at quite a high level of resolution. Since the policy does not contain a rule with a <retention-transformation>, LSs have to delete LOs immediately upon service completion.

```
<?xml version="1.0" encoding="UTF-8"?>
<cp:ruleset
    xmlns:cp="urn:ietf:params:xml:ns:common-policy"
    xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <cp:rule id="AA56i09">
        <cp:conditions>


            <cp:validity>
                <cp:from>2004-11-01T00:00:00+01:00</cp:from>
                <cp:until>2005-11-01T00:00:00+01:00</cp:until>
            </cp:validity>

            <gp:civic-loc-condition>
                <gp:country>DE</gp:country>
                <gp:A1>Bavaria</gp:A1>
                <gp:A3>Munich</gp:A3>
                <gp:A4>Perlach</gp:A4>
                <gp:A6>Otto-Hahn-Ring</gp:A6>
                <gp:HNO>6</gp:HNO>
            </gp:civic-loc-condition>


        </cp:conditions>

        <cp:actions/>


        <cp:transformations>
            <gp:distribution-transformation>true
            </gp:distribution-transformation>
```

```
            <gp:keep-rules-transformation>true
            </gp:keep-rules-transformation>
            <gp:civic-loc-transformation>full
            </gp:civic-loc-transformation>
            <gp:geospatial-loc-transformation>
                <gp:lat-resolution>0.00001</gp:lat-resolution>
                <gp:lon-resolution>0.00001</gp:lon-resolution>
            </gp:geospatial-loc-transformation>
        </cp:transformations>
    </cp:rule>
</cp:ruleset>
```


9.2. Rule Example with Geospatial Location Information

This example illustrates a rule that employs the geospatial location condition. The rule matches if the current location of the target is inside the area specified by the <point> child elements of the <polygon> element. The individual points of the polygon have to be interpreted as points of the WGS-84 coordinate reference system, as specified by the value of the 'crsName' attribute of the <polygon> element. This coordinate reference systems is also used by GPS. The given four points specify a quadrangle on the surface of the rotational ellipoid being part of the WGS-84 system, corresponding to a certain area in Washington, DC, USA.

The transformation part of the example rule allows the location server to distribute location objects from which all authorization policy rules or pointers to them have been removed. The location server is permitted to retain the location objects related to the target for at most one hour. They are allowed to provide civic location information about the target at city level of precision, and geospatial location information at roughly the first decimal of precision.

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

```
      xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

      <cp:rule id="BB56A09">

        <cp:conditions>

          <cp:validity>
            <cp:from>2004-11-01T00:00:00+01:00</cp:from>
            <cp:until>2005-11-01T00:00:00+01:00</cp:until>
          </cp:validity>

          <gp:geospatial-loc-condition>
            <gp:polygon
              crsName="urn:ietf:params:xml:ns:geopriv-policy:crs:wgs84">
              <gp:point>
                <gp:lat>38.8986</gp:lat>
                <gp:lon>-77.03724</gp:lon>
              </gp:point>
              <gp:point>
                <gp:lat>38.8986</gp:lat>
                <gp:lon>-77.03722</gp:lon>
```



```
              </gp:point>
              <gp:point>
                <gp:lat>38.8987</gp:lat>
                <gp:lon>-77.03722</gp:lon>
              </gp:point>
              <gp:point>
                <gp:lat>38.8987</gp:lat>
                <gp:lon>-77.03724</gp:lon>
              </gp:point>
            </gp:polygon>
          </gp:geospatial-loc-condition>

        </cp:conditions>

        <cp:transformations>

          <gp:distribution-transformation>
            true
          </gp:distribution-transformation>
```

```
        <gp:keep-rules-transformation>
          false
        </gp:keep-rules-transformation>

        <gp:retention-transformation>
          3600
        </gp:retention-transformation>

        <gp:civic-loc-transformation>city</gp:civic-loc-transformation>

        <gp:geospatial-loc-transformation>
          <gp:lat-resolution>0.2</gp:lat-resolution>
          <gp:lon-resolution>0.1</gp:lon-resolution>
        </gp:geospatial-loc-transformation>

      </cp:transformations>

    </cp:rule>

  </cp:ruleset>
```

The next ruleset indicates that the target has to be at an altitude between 1500 and 4000 meters in order for this rule to match.

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



```
    xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <cp:rule id="BB56A19">

      <cp:conditions>

        <cp:validity>
          <cp:from>2004-11-01T00:00:00+01:00</cp:from>
          <cp:until>2005-11-01T00:00:00+01:00</cp:until>
        </cp:validity>
```

```
        <gp:geospatial-loc-condition>
           <gp:altitude>
               <gp:min>1500.0</gp:min>
               <gp:max>4000.0</gp:max>
           </gp:altitude>
        </gp:geospatial-loc-condition>

      </cp:conditions>

      <cp:transformations>

        <gp:distribution-transformation>
          true
        </gp:distribution-transformation>

        <gp:keep-rules-transformation>
          false
        </gp:keep-rules-transformation>

        <gp:retention-transformation>
          3600
        </gp:retention-transformation>

        <gp:civic-loc-transformation>city</gp:civic-loc-transformation>

        <gp:geospatial-loc-transformation>
          <gp:lat-resolution>0.3</gp:lat-resolution>
          <gp:lon-resolution>0.2</gp:lon-resolution>
        </gp:geospatial-loc-transformation>

      </cp:transformations>

    </cp:rule>

  </cp:ruleset>
```


10. XML Schema

This section presents the XML schema that defines the geo policy language described in the previous sections. The policy markup language introduced by this schema extends the common policy markup

language (see[I-D.ietf-geopriv-common-policy]) by introducing new members of the 'condition' and 'transformation' substitution groups whose heads (namely the elements <condition> and <transformation>) are specified by the common policy schema ([I-D.ietf-geopriv-common-policy]).

To express civic location conditions, it imports the 'civicAddress' complex type as defined in [RFC4119].

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:geopriv-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geopriv-policy"
  xmlns:cp="urn:ietf:params:xml:ns:common-policy"
  xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civilLoc"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <!-- Geopriv conditions -->
  <xs:element name="civic-loc-condition" type="cl:civilAddress"/>

  <xs:element name="geospatial-loc-condition">
    <xs:complexType>
      <xs:choice>

        <xs:element name="polygon">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="point"
                minOccurs="3" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="lat" type="xs:double"/>
                    <xs:element name="lon" type="xs:double"/>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
            <xs:attribute name="crsName" type="xs:anyURI"/>
          </xs:complexType>
        </xs:element>
```

```
      <xs:element name="altitude">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="min" type="xs:double"/>
            <xs:element name="max" type="xs:double"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>

      <xs:any namespace="##other" processContents="lax"/>

    </xs:choice>
  </xs:complexType>
</xs:element>

<!-- Geopriv transformations -->

<xs:element name="distribution-transformation"
  type="xs:boolean" />

<xs:element name="retention-transformation"
  type="xs:integer" />

<xs:element name="keep-rules-transformation" type="xs:boolean" />

<xs:element name="civic-loc-transformation">
  <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:restriction>
  </xs:simpleType>
</xs:element>

<xs:element name="geospatial-loc-transformation">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="lat-resolution" type="xs:double"
        minOccurs="0" maxOccurs="1" />
      <xs:element name="lon-resolution" type="xs:double"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="alt-resolution" type="xs:double"
        minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
```

```
    </xs:element>

  </xs:schema>
```

11. Security Considerations

This document aims to make it simple for users to prevent the unintended disclosure of private information to third parties. Security threats are described in [RFC3694] and are applicable to this draft as well. Security requirements are addressed in [RFC3693]. Section 5 addresses issues of protecting the policy rules within the location object and location information itself. Aspects of combining permissions in cases of multiple occurrence are treated in [I-D.ietf-geopriv-common-policy]). How the behavior of location servers can be regulated in terms of location object handling in a privacy-safe fashion is specified in Section 8.

12. References

12.1. Normative References

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

[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.

12.2. Informative 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-common-policy] Schulzrinne, H., "A Document Format for Expressing Privacy Preferences", draft-ietf-geopriv-common-policy-06 (work in progress), October 2005.

[I-D.ietf-geopriv-dhcp-civil] Schulzrinne, H., "Dynamic Host Configuration Protocol

(DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", draft-ietf-geopriv-dhcp-civil-09 (work in progress), January 2006.

[I-D.ietf-simple-xcap] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", draft-ietf-simple-xcap-08 (work in progress), October 2005.

[RFC2518] Goland, Y., Whitehead, E., Faizi, A., Carter, S., and D. Jensen, "HTTP Extensions for Distributed Authoring -- WEBDAV", RFC 2518, February 1999.

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

[RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based

Location Configuration Information", RFC 3825, July 2004.

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

Appendix A. Contributors

We would like to thank Christian Guenther for his help with an earlier version of this document.

Appendix B. 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.

Authors' Addresses

Henning Schulzrinne
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
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.