GEOPRIV WG
Internet-Draft
Expires: December 21, 2003

J. Peterson
NeuStar
June 22, 2003

A Presence-based GEOPRIV Location Object Format
draft-peterson-geopriv-pidf-lo-00

Status of this Memo

Copyright Notice

Abstract

This document describes a object format for carrying geographical information on the Internet. This location object extends the Presence Information Data Format (PIDF), which was designed for communicating privacy-sensitive presence information and has similar properties.

Table of Contents

1. Introduction

Geographical location information describes a physical position in the world that may correspond to the past, present or future location of a person or device. Numerous applications used in the Internet today benefit from sharing location information (including mapping/ navigation applications, 'friend finders' on cell phones, and so on). However, such applications may disclose the whereabouts of a person in a manner contrary to the user's preferences. Privacy lapses may result from poor protocol security (which permits eavesdroppers to capture location information), inability to articulate or accommodate user preferences, or similar defects common in existing systems. The privacy concerns surrounding the unwanted disclosure of a person's physical location are among the more serious that confront users on the Internet.

Consequently, a need has been identified to convey geographical location information within an object that includes a user's privacy and disclosure preferences and which is protected by strong cryptographic security. Previous work [11] has observed that this problem bears some resembles to the general problem of communicating and securing presence information on the Internet. Presence (which is defined in [10]) provides a real-time communications disposition to a user that have similar requirements for selective distribution and security.

Therefore, this document extends the XML-based Presence Information Data Format (PIDF [2]) to allow the encapsulation of location information within a presence document.

This document does not invent any format for location information itself. Numerous already existing formats based on civil location, spatial coordinates, and the like have been developed in other standards fora. Instead, this document defines an object that is suitable for both identifying and encapsulating pre-existing location information formats and for providing adequate security and policy controls to regulate the distribution of location information over the Internet.

The location object described in this document can be used independently of any 'using protocol' as the term is defined in the GEOPRIV requirements [8]. It is considered an advantage of this proposal that existing presence protocols (such as [13]) would natively accommodate the location object format defined in this document, and be capable of composing location information with other presence information, since this location object is an extension of PIDF. However, any protocol that can carry XML or MIME types can carry PIDF.

Some of the requirements in [8] concern data collection and usage policies associated with location objects. This document does not provide a markup suitable for a user to express the necessary privacy preferences as specified by the geopriv requirements. However, this document does demonstrate how an XML-based privacy preference document could be embedded within a PIDF document.

2. Location Object Format

2.1 Baseline PIDF Usage

The GEOPRIV requirements [8] (or REQ for short throughout this section) specify the need for a name for the person, place or thing that location information describes (REQ 2.1). PIDF has such an identifier already, since every PIDF document has "entity" attribute of the "presence" element that signifies the URI of the entity whose presence the document describes. Similarly, if location information is contained in a PIDF document, the URI in the "entity" attribute of the "presence" element indicates the target of that location information. The URI in the "entity" attribute should use the "pres" URI scheme defined in [3]. URIs can serve as "unlinkable pseudonyms" (per REQ 12).

PIDF optionally contains a "contact" element that contains a URI where the presentity can be reached by some means of communication (usually, the URI scheme in the value of the "contact" element gives some sense of how the presentity can be reached: if it uses the SIP URI scheme, for example, SIP can be used, and so on). Location information can be provided without any associated means of communication - thus, the "contact" element may or may not be present, as desired by the creator of the PIDF document.

PIDF optionally contains a "timestamp" element that designates the time at which the PIDF was created. This element corresponds to REQ 2.7a.

PIDF contains a "status" element, which is mandatory. "status" contains an optional child element "basic" that describes the presentity's communications disposition (in the very broad terms: either OPEN or CLOSED). For the purposes of this document, it is not necessary for "basic" status to be included. If, however, communications disposition is included in a PIDF document above and beyond geolocation, then "basic" status may appear in a PIDF document that uses these extensions.

PIDF also contains a "tuple" element, which is used to uniquely identify a segment of presence information so that changes to this

information can be tracked over time (as multiple notifications of presence are received).

2.2 Extensions to PIDF for Location and Privacy Policy

This XML Schema extends the "status" element of PIDF with a complex element called "geopriv". There are two major subelements that are encapsulated within geopriv: one for location information, and one for usage rules. Both of these subelements are mandatory, and are described in subsequent sections.

There are also a few other elements which are contained within the geopriv element in support of the GEOPRIV requirements.

2.2.1 'location-info' element

Each 'geopriv' element MUST contain one 'location-info' element. A 'location-info' element consists of one or more chunks of location information (per REQ 2.5). The format of the location information (REQ 2.6) is identified by the imported XML Schema describing the namespace in question. All PIDF documents that contain a 'geopriv' element MUST contain one or more import directive indicating the XML Schema(s) that will be used as geolocation formats.

In order to ensure interoperability of GEOPRIV implementations, it is necessary to select a baseline location format that all compliant implementations support (see REQ 3.1). At this time, there is not sufficient working group consensus within the GEOPRIV WG to award this distinction to any particular location format. Without applying any particular selection criteria (apart from REQs 2.5.1), this document works from the assumption that GML 3.0 [14] will be this mandatory format (MUST implement for all PIDF implementations supporting the 'geopriv' element).

The Geography Markup Language (GML) is an extraordinarily thorough and versatile system for modeling all manner of geographic topologies and objects. The simplest package for GML supporting location information is the 'feature.xsd' schema. Various format descriptions (including latitude/longitude based location information) is supported by Feature (see section 7.4.1.4 of [14] for examples). This resides here:

urn:opengis:specification:gml:schema-xsd:feature:v3.0
</xs:schema>

Note that by importing the Feature schema, necessary GML baseline schemas are transitively imported.

Complex features (such as modeling topologies and polygons, directions and vectors, temporal indications of the time for which a particular location is valid for a target) are also available in GML, but require importing additional schemas. For the purposes of this document, only support for the feature.xsd GML schema is REQUIRED.

2.2.2 'usage-rules' element

At the time this document was written, the policy requirements for GEOPRIV objects were not definitively completed. However, the 'usage-rules' element exists to satisfy REQ 2.8, and the requirements of the GEOPRIV policy requirements [9] document. Each 'geopriv' element SHOULD contain one 'usage-rules' element - Location Generators MAY not include this element ONLY IF users have specifically requested that all sub-elements given below are unnecessary to protect this Location Object.

Following to that document (Section 3.1), there are three fields that need to be expressible in Location Objects throughout their lifecycle (from Generator to Recipient): one field that limit retransmission, one that limit retention, and one that contains a reference to external rulesets. Those three fields are instantiated here by the first three elements. The fourth element provides a generic space for human-readable policy directives. Any of these fields MAY be present in a Location Object 'usage-rules' element; none are required to be.

'retransmission-allowed': When the value of this element is 'no', the Recipient of this Location Object is not permitted to share the enclosed Location Information, or the object as a whole, with other parties. When the value of this element is 'yes', sharing this Location Object or information is permitted (barring an existing agreement or obligation to the contrary). By default, the value MUST be assumed to be 'no'. Implementations MUST include this field, with a value of 'no', if the Rule Maker specifies no preference.

'retention-expires': This field specifies an absolute date at which time the Recipient is no longer permitted to possess the location information and its encapsulating Location Object - both may be retained only up until the time specified by this field. By default, the value MUST be assumed to be twenty-four hours from the 'timestamp' element in the PIDF document, if present; if the 'timestamp' element is not present, then twenty-four hours from the time at which the Location Object is received. If the value in the 'retention-expires' element has already passed when the Location Recipient receives the Location Object, the Recipient MUST discard the Location Object immediately.

'ruleset-reference': This field contains a URI to a network server that holds rules appropriate for this Location Object. This SHOULD be an HTTPS URI, and the server that holds these rules MUST authenticate any attempt to access these rules - usage rules themselves may divulge private information about a Target or Rule Maker. Location Recipients SHOULD NOT attempt to dereference this URI - it is intended only for the consumption of Location Servers.

'note-well': This field contains a block of text containing further generic privacy directives. These directives are intended to be human-readable only, not to be processed by any automaton.

2.2.3 Schema definition

Note that the XML namespace [4] for this extension to PIDF contains a version number 1.0 (as per REQ 2.10).

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:tns="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
   <xs:complexType name="geopriv">
    <xs:sequence>
      <xs:element name="location-info" type="tns:locInfoType"
         minOccurs="1" maxOccurs="1"/>
      <xs:element name="usage-rules" type="tns:locPolicyType"
         minOccurs="1" maxOccurs="1"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0"
         maxOccurs="unbounded"/>
    </xs:sequence>
   </xs:complexType>

   <xs:complexType name="locInfoType">
    <xs:sequence>
      <xs:any namespace="##other" processContents="lax" minOccurs="0"
         maxOccurs="unbounded"/>
    </xs:sequence>
   </xs:complexType>

   <xs:complexType name="locPolicyType">
    <xs:sequence>
      <xs:element name="retransmission-allowed" type="tns:retrans"
         minOccurs="0" maxOccurs="1"/>
      <xs:element name="retention-expiry" type="xs:dateTime"
```

```
            minOccurs="0" maxOccurs="1"/>
          <xs:element name="retention-expiry" type="xs:anyURI"
            minOccurs="0" maxOccurs="1"/>
          <xs:element name="note-well" type="tns:notewell"
            minOccurs="0" maxOccurs="1"/>
          <xs:any namespace="##other" processContents="lax" minOccurs="0"
            maxOccurs="unbounded"/>
        </xs:sequence>
      </xs:complexType>

        <xs:simpleType name="retrans">
          <xs:restriction base="xs:string">
            <xs:enumeration value="yes"/>
            <xs:enumeration value="no"/>
          </xs:restriction>
        </xs:simpleType>

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

    </xs:schema>
```

2.3 Example Location Object

The following XML instance document is an example of the use of a simple GML 3.0 markup with a few of the policy directives specified above within a PIDF document.

```
<?xml version="1.0" encoding="UTF-8"?>
 <presence xmlns="urn:ietf:params:xml:ns:pidf"
    xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
    xmlns:gml="urn:opengis:specification:gml:schema-xsd:feature:v3.0"
    entity="pres:geotarget@example.com">
  <tuple id="sg89ae">
   <timestamp>2003-06-22T20:57:29Z</timestamp>
   <status>
    <gp:geopriv>
      <gp:location-info>
        <gml:location>
          <gml:Point gml:id="point96" srsName="epsg:4326">
            <gml:coordinates>31:56:00S 115:50:00E</gml:coordinates>
          </gml:Point>
         </gml:location>
      </gp:location-info>
      <gp:usage-rules>
        <gp:retransmission-allowed>no</gp:retransmission-allowed>
        <gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
      </gp:usage-rules>
    </gp:geopriv>
   </status>
  </tuple>
 </presence>
```

Note that this shows a PIDF document without any MIME headers or security applied to it (see Section 4 below).

3. Carrying PIDF in a Using Protocol

A PIDF document is an XML document, and therefore PIDF might be carried in any protocol that is capable of carrying XML. A MIME type has also been registered for PIDF: 'application/cpim-pidf+xml'. PIDF may therefore be carried as a MIME body in protocols that use MIME (such as SMTP, HTTP, or SIP) with an encapsulating set of MIME headers, including a Content-Type of 'application/cpim-pidf+xml".

Further specification of the behavior of using protocols (including subscribing to or requesting presence information) is outside the scope of this document.

4. Securing PIDF

There are a number of ways in which XML documents can be secured. XML itself supports several ways of partially securing documents, including element-level encryption and digital signature properties.

For the purposes of this document, only the securing of a PIDF

document as a whole, rather than element-by-element security, is considered. None of the requirements [8] suggest that only part of the information in a location object might need to be protected while other parts are unprotected - virtually any such configuration would introduce potentials for privacy leakage. Consequently, the use of MIME-level security is appropriate.

S/MIME [5] allows security properties (including confidentiality, integrity and authentication properties) to be applied to the contents of a MIME body. Therefore, all PIDF implementations that support the XML Schema extensions for location information described in this document MUST support S/MIME, and in particular must support the CMS [6] EnvelopedData and SignedData messages, which are used for encryption and digital signatures respectively. It is believed that this mechanism meets REQs 2.10, 13, 14.1, 14.2, 14.3, 14.4.

Additionally, all implementations MUST implement the AES encryption algorithm for S/MIME, as specified in [7] (and per REQ 15.1). Of course, implementations MUST also support the baseline encryption and digital signature algorithms described in the S/MIME specification.

S/MIME generally entails the use of X.509 [16] certificates. In order to encrypt a request for a particular destination end-to-end (i.e. to a Location Recipient), the Location Generator must possess credentials (typically an X.509 certificate) that have been issued to the Location Recipient.

S/MIME was designed for end-to-end security between email peers that communicate through multiple servers (i.e mail transfer agents) that do not modify message bodies. There is, however, at least one instance in which Location Servers modify Location Objects - namely when Location Servers enforce policies on behalf of the Rule Maker. For example, a Rule Maker may specify that Location Information should be coarsened (made less specific) before it is transmitted to particular recipients. If the Location Server were unable to modify a Location Object, because it was encrypted, signed, or both, it would be unable to accomplish this function. Consequently, when a Location Generator wants to allow a Location Server to modify such messages, they MAY encrypt such messages with keys issued to the Location Server (the signature, of course, can still be created with keying material from the Location Generator's certificate). After modifying the Location Object, the Location Server can resign the Object with its own credentials (encrypting it with any keys issued to the Location Recipient, if they are known to the Server).

Note that policies for data collection and usage of location information, in so far as they are carried within a location object, are discussed in Section 2.2.2.

5. Security Considerations

The threats to which an Internet service carrying geolocation might be subjected are detailed in [15]. The requirements that were identified in that analysis of the threat model were incorporated into [8], in particular within Section 7.4. This document aims to be compliant with the security requirements derived from those two undertakings in so far as they apply to the location object itself.

Security of the location object defined in this document, including normative requirements for implementations, is discussed in Section 4. This security focuses on end-to-end integrity and confidentiality properties that are applied to a location object for its lifetime via S/MIME.

Security requirements associated with using protocols (including authentication of subscribers to geographical information, and so on) are outside the scope of this document.

6. IANA Considerations

6.1 URN Sub-Namespace Registration for urn:ietf:params:xml:ns:pidf:geopriv10

This section registers a new XML namespace, as per the guidelines in [4].

URI: The URI for this namespace is urn:ietf:params:xml:ns:pidf:geopr.

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), Jon Peterson (jon.peterson@neustar.biz).

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
          "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
     content="text/html;charset=iso-8859-1"/>
  <title>GEOPRIV PIDF Extensions</title>
</head>
<body>
  <h1>PIDF Extensions of Geographical Information and Privacy</
h1>
  <h2>urn:ietf:params:xml:ns:pidf:geopriv10</h2>
  <p>See <a href="[[[URL of published RFC]]]">RFCXXXX</a>.</p>
</body>
</html>
END
```

Normative References

[1] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.

[2] Sugano, H., Fujimoto, S., Klyne, G., Bateman, A., Carr, W. and J. Peterson, "CPIM Presence Information Data Format", draft-ietf-impp-cpim-pidf-07 (work in progress), August 2001.

[3] Peterson, J., "Common Profile for Presence (CPP)", draft-ietf-impp-pres-03 (work in progress), May 2003.

[4] Mealling, M., "The IETF XML Registry", draft-mealling-iana-xmlns-registry-05 (work in progress), June 2003.

[5] Ramsdell, B., "S/MIME Version 3 Message Specification", draft-ietf-smime-rfc2633bis-03 (work in progress), January 2003.

[6] Housley, R., "Cryptographic Message Syntax", RFC 3369, August 2002.

[7] Schaad, J. and R. Housley, "Use of the AES Encryption Algorithm and RSA-OAEP Key Transport in CMS", draft-ietf-smime-aes-alg-06 (work in progress), January 2003.

Informative References

[8] Cuellar, J., Morris, J., Mulligan, D., Peterson, J. and J. Polk, "Geopriv requirements", draft-ietf-geopriv-reqs-03 (work in progress), February 2003.

[9] Morris, J., Mulligan, D. and J. Cuellar, "Core Privacy Protections for Geopriv Location Object", draft-morris-geopriv-core-01 (work in progress), March 2003.

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

[11] Peterson, J., "A Presence Architecture for the Distribution of Geopriv Location Objects", draft-peterson-geopriv-pres-00 (work in progress), February 20003.

[12] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

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

[14] OpenGIS, "", OGC 02-023r4, January 2003, <http:// http://www.opengis.org/techno/implementation.htm>.

[15] Danley, M., Morris, J., Mulligan, D. and J. Peterson, "Threat Analysis of the geopriv Protocol", draft-ietf-geopriv-threats-00 (work in progress), February 2003.

[16] ITU-T, "Recommendation X.509 - Open Systems Interconnection - The Directory: Authentication", ITU-T X.509, June 1997, <http:// http://www.itu.int>.

[17] Gutmann, P., "Password-based Encryption for CMS", RFC 3211, December 2001.

Author's Address

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
US

Phone: +1 925/363-8720
EMail: jon.peterson@neustar.biz
URI: http://www.neustar.biz/

Appendix A. To Do and Unmet requirements

Today, this document makes a very half-hearted recommendation for GML3.0 as the mandatory-to-implement geolocation format for Location Objects. Much more discussion is needed of the merits and flaws of this approach. We also need to identify an appropriate worldwide postal address format (surely there are existing XML standards for this that we can reuse).

Below are various GEOPRIV requirements [8] that currently are not met by this document. These requirements may be met in future versions of the document.

REQ 1.5: Requesting location information is deferred to the using protocol in this paradigm of GEOPRIV. The Location Object contains no support for this feature either way.

REQ 1.8: The S/MIME mechanism in this document, in so far as it uses X.509, may be too heavyweight to accommodate constrained devices with little memory or processing power. There are variants of S/MIME that do not use certificates for various security function, but instead use symmetric keys (see [17]), and which would consequently be a better fit for constrained devices.

REQ 2.2: The identity of the Location Recipient should not have to be known to the Location Generator - it is possible that the Generator publishes its location information to a Location Server that enforces policies relevant to various Recipients without informing the Generator that location information has been requested. Carrying the identity of the recipient is deferred to the using protocol in this paradigm of GEOPRIV.

REQ 2.3 & 2.4: These requirements would need to be further specified before it would be possible for a solution document to satisfy them. It is not clear what these credentials are, nor why the Location Generator would possess them and place them inside Location Objects.

XML Schemas and examples have not been validated.

Appendix B. Acknowledgments

This document was produced with the assistance of many members of the GEOPRIV IETF working group.

Full Copyright Statement

Acknowledgement

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