

GEOPRIV WG
Internet-Draft
Expires: July 12, 2004

J. Peterson
NeuStar
January 12, 2004

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

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/lid-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 July 12, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document describes an 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 which has similar properties.

Internet-Draft

GEOPRIV Location Obj

January 2004

Table of Contents

1.	Introduction	3
2.	Location Object Format	4
2.1	Baseline PIDF Usage	4
2.2	Extensions to PIDF for Location and Usage Rules	5
2.2.1	'location-info' element	5
2.2.2	'usage-rules' element	7
2.2.3	Schema definitions	9
2.3	Example Location Objects	11
3.	Carrying PIDF in a Using Protocol	13
4.	Securing PIDF	13
5.	Security Considerations	15
6.	IANA Considerations	15
6.1	URN Sub-Namespace Registration for urn:ietf:params:xml:ns:pidf:geopriv10	15
	Author's Address	18
A.	To Do	18
	Normative References	16
	Informative References	16
B.	Acknowledgments	18
	Full Copyright Statement	19

Internet-Draft

GEOPRIV Location Obj

January 2004

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, event 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 [[12](#)] has observed that this problem bears some resemblance to the general problem of communicating and securing presence information on the Internet. Presence (which is defined in [[11](#)]) provides a real-time communications disposition for a user, and thus has 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 existing formats based on civil location, geographic 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 [9]. It is considered an advantage of this proposal that existing presence protocols (such as [14]) 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, the usage of this location object format is not limited to presence using protocols - any protocol that can carry XML

or MIME types can carry PIDF.

Some of the requirements in [9] and [10] concern data collection and usage policies associated with location objects. This document provides only the minimum markup necessary for a user to express the necessary privacy preferences as specified by the geopriv requirements (the three basic elements in [10]). However, this document does not demonstrate how a full XML-based ruleset accommodating the needs of Location Servers could be embedded in PIDF - it is assumed that other protocols (such as HTTP) will be used to move rules between Rule Holders and Location Servers, and that full rulesets will be defined in a separate document.

[2.](#) Location Object Format

[2.1](#) Baseline PIDF Usage

The GEOPRIV requirements [9] (or REQ for short) 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 an "entity" attribute of the 'presence' element that signifies the URI of the entity whose presence the document describes. Consequently, 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 'presentity'). The URI in the "entity" attribute generally uses the "pres" URI scheme defined in [3]. Such URIs can

serve as unlinkable pseudonyms (per REQ 12).

PIDF optionally contains a 'contact' element that provides 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 document 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' umbrella element, which holds an "id" element 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). 'timestamp', 'status', and 'contact' are composed under 'tuple'.

[2.2](#) Extensions to PIDF for Location and Usage Rules

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. By composing this two subelements under 'geopriv', the usage rules are clearly and explicitly associated with the location information.

For extensibility (see REQ 1.4), the schema allows any other

subelements to appear under the 'geopriv' element. No such subelements are currently envisioned by this document.

[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 directives indicating the XML Schema(s) that will be used for geographic location 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). Since it satisfies REQ 2.5.1, this document works from the assumption that GML 3.0 [\[15\]](#) shall be this mandatory format (a 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 object types, topologies, metadata, coordinate reference systems and units of measurement. The simplest package for GML supporting location information is the 'feature.xsd' schema. Various format descriptions (including latitude/longitude based location information) are supported by Feature (see section 7.4.1.4 of [\[15\]](#) for examples),

which resides here:

urn:opengis:specification:gml:schema-xsd:feature:v3.0

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 baseline interoperability has defined by this document, only support for the 'feature.xsd' GML schema is REQUIRED.

Implementations MAY support the civil location format (civilLoc) defined in [Section 2.2.3](#). civilLoc provides the following elements:

Label	Description	Example
country	The country is identified by the two-letter ISO 3166 code.	US
A1	national subdivisions (state, region, province, prefecture)	New York
A2	county, parish, gun (JP), district (IN)	King's County
A3	city, township, shi (JP)	New York
A4	city division, borough, city district, ward, chou (JP)	Manhattan
A5	neighborhood, block	Morningside Heights
A6	street	Broadway
PRD	Leading street	N, W

	direction	
POD	Trailing street suffix	SW
STS	Street suffix	Avenue, Platz, Street

HNO	House number, numeric part only.	123
HNS	House number suffix	A, 1/2
LMK	Landmark or vanity address	Low Library
LOC	Additional location information	Room 543
FLR	Floor	5
NAM	Name (residence, business or office occupant)	Joe's Barbershop
PC	Postal code	10027-0401

Either the GML 3.0 geographical information format element, or the location format element ('civilLoc') defined in this document, MAY appear in in a 'location-info' element. Both MAY also be used in the same 'location-info' element. In summary, the feature.xsd schema of GML 3.0 MUST be support by implementations compliant with this specification, and the civilLoc format MAY be supported by implementations compliant with this specification.

[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 [[10](#)] document. Each 'geopriv' element SHOULD contain one 'usage-rules' element - Location Generators MAY opt not to include this element if the Rule Maker has requested that all sub-elements given below have their default values.

Following the policy requirements 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 limits retransmission, one that limits 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', distributing this Location is permitted (barring an existing out-of-band 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 also not present, then twenty-four hours from the time at which the Location Object is received by the Location Recipient. 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 that indicates where a fuller ruleset of policies related to this object can be found. This URI SHOULD use the HTTPS URI scheme, and if it does, 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. The URI MAY alternatively use the CID URI scheme [7], in which case it MUST denote a MIME body carried with the Location Object by the using protocol. Rulesets carried as MIME bodies SHOULD be encrypted and signed by the Rule Maker; unsigned rulesets SHOULD NOT be honored by Location Servers or Location Recipients. Note that in order to avoid network lookups that result in an authorization failure, creators of Location Objects MAY put HTTPS-based ruleset-references into an encrypted external MIME body referenced by a CID; in this way, recipients of the Location Object that are unable to decrypt the external MIME body will not learn the HTTPS

Internet-Draft

GEOPRIV Location Obj

January 2004

URI unless they are able to decrypt the MIME body.

'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 definitions

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:import namespace="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy">

  <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:schema>
```

The 'geopriv10' schema imports, for the 'usage-rules' element, the following policy schema. This schema has been broken out from the basic geolocation object in order to allow for its reuse. The semantics associated with these elements described in [Section 2.2.2](#) apply only to the use of these elements to define policy for

geolocation objects; any other use of 'usage-rules' must characterize its own semantics for all 'usage-rules' subelements.

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

  <xs:complexType name="locPolicyType">
    <xs:sequence>
      <xs:element name="retransmission-allowed" type="xs:boolean"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="retention-expiry" type="xs:dateTime"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="external-ruleset" 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:complexType name="notewell">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute ref="xml:lang"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

</xs:schema>
```

The following schema is a trivial representation of civil location that MAY be implemented by entities compliant with this specification.

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

```
<xs:complexType name="civilAddress">
  <xs:sequence>
    <xs:element name="country" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="A1" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="A2" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="A3" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="A4" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="A5" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="A6" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="PRD" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="POD" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="STS" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="HNO" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="HNS" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="LMK" type="xs:string"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="LOC" type="xs:string"
```

```

        minOccurs="0" maxOccurs="1"/>
        <xs:element name="FLR" type="xs:string"
            minOccurs="0" maxOccurs="1"/>
        <xs:element name="NAM" type="xs:string"
            minOccurs="0" maxOccurs="1"/>
        <xs:element name="PC" type="xs:string"
            minOccurs="0" maxOccurs="1"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0"
            maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

</xs:schema>

```

[2.3](#) Example Location Objects

Note that these examples show PIDF documents without any MIME headers or security applied to them (see [Section 4](#) below).

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>

```

The following XML instance document is an example of the use of the civilLoc object 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:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civilLoc"
  entity="pres:geotarget@example.com">
  <tuple id="sg89ae">
    <timestamp>2003-06-22T20:57:29Z</timestamp>
    <status>
      <gp:geopriv>
        <gp:location-info>
          <cl:civilAddress>
            <cl:country>US</cl:country>
            <cl:A1>New York</cl:A1>
            <cl:A3>New York</cl:A3>
            <cl:A6>Broadway</cl:A6>
          </cl:civilAddress>
        </gp:location-info>
      </gp:geopriv>
    </status>
  </tuple>
</presence>

```

```
<cl:HNO>123</cl:HNO>
<cl:LOC>Suite 75</cl:LOC>
<cl:PC>10027-0401</cl:PC>
</cl:civilAddress>
</gp:location-info>
<gp:usage-rules>
  <gp:retransmission-allowed>yes</gp:retransmission-allowed>
  <gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
</gp:usage-rules>
</gp:geopriv>
</status>
</tuple>
</presence>
```

[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 [\[9\]](#) 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 compliant applications MUST implement the AES encryption algorithm for S/MIME, as specified in [8] (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 [17] 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. Implementations of this specification SHOULD support X.509 certificates for S/MIME, and MUST support password-based CMS encryption (see [18]). Any symmetric keying systems SHOULD derive high-entropy content encoding keys (CEKs). When X.509 certificates are used to sign PIDF Location Objects, the subjectAltName of the certificate SHOULD use the "pres" URI scheme.

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 a key that can be decrypted by the Location Server (the digital 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 re-sign 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 [\[16\]](#). The requirements that were identified in that analysis of the threat model were incorporated into [\[9\]](#), 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 (as opposed to the using protocol).

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:geopriv10.

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-imp-pcim-pidf-07](#) (work in progress), August 2001.
- [3] Peterson, J., "Common Profile for Presence (CPP)", [draft-ietf-imp-pres-04](#) (work in progress), October 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] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", [RFC 2392](#), August 1998.
- [8] Schaad, J., "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)", [RFC 3565](#), July 2003.

- [9] Cuellar, J., Morris, J., Mulligan, D., Peterson, J. and J. Polk, "Geopriv requirements", [draft-ietf-geopriv-reqs-03](#) (work in progress), February 2003.
- [10] Morris, J., Mulligan, D. and J. Cuellar, "Core Privacy Protections for Geopriv Location Object", [draft-morris-geopriv-core-02](#) (work in progress), June 2003.
- [11] Day, M., Rosenberg, J. and H. Sugano, "A Model for Presence and Instant Messaging", [RFC 2778](#), February 2000.
- [12] Peterson, J., "A Presence Architecture for the Distribution of Geopriv Location Objects", [draft-peterson-geopriv-pres-00](#) (work in progress), February 2003.
- [13] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", [RFC 2396](#), August 1998.
- [14] 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.
- [15] OpenGIS, "", OGC 02-023r4, January 2003, <[http:// http://www.opengis.org/techno/implementation.htm](http://www.opengis.org/techno/implementation.htm)>.
- [16] 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.
- [17] ITU-T, "Recommendation X.509 - Open Systems Interconnection - The Directory: Authentication", ITU-T X.509, June 1997, <[http:// http://www.itu.int](http://www.itu.int)>.
- [18] Gutmann, P., "Password-based Encryption for CMS", [RFC 3211](#), December 2001.

Internet-Draft

GEOPRIV Location Obj

January 2004

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

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. Special thanks to Carl Reed of OpenGIS for a close read of the document.

The civil location format described in this document was proposed by Henning Schulzrinne for communicating location information in DHCP, and has been appropriated in its entirety for this document.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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