

Radius EXT
Internet-Draft
Expires: July 2, 2003

M. Jones
Bridgewater Systems Corporation
H. Tschofenig
J. Cuellar
Siemens
January 2003

GEOPRIV support for RADIUS
draft-jones-radius-geopriv-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 2, 2003.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

Network access servers are increasingly capable of providing user and device location information to AAA servers. This enables the AAA server to make additional authorization decisions based on the location of the user or access device. The home or visited network may also use the location information for other purposes (e.g., acting as a location server). This document provides guidelines for the encoding and transport of location information using the RADIUS protocol which are compliant with the Geopriv requirements for security and privacy.

Internet-Draft

GEOPRIV support for RADIUS

January 2003

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Framework and Scenarios	5
3.1	Location information about a network	7
3.2	Location information about an end user	7
3.3	Visited and Home network as a Location Server	8
3.4	Default privacy-sensitive policy	9
4.	RADIUS Usage Scenarios	10
4.1	Home Network Access	10
4.2	Visited Network Access	11
4.3	Visited Network Access via Broker	12
5.	Location Information	15
5.1	Civil Location	15
5.2	Geospatial Location	16
6.	Example	19
7.	Packet Formats	21
8.	Security Considerations	23
9.	Open Issues	25
	Normative References	26
	Informative References	27
	Authors' Addresses	27
A.	Contributors	28
B.	Acknowledgments	29
	Intellectual Property and Copyright Statements	30

1. Introduction

Location information needs to be protected against unauthorized access to preserve privacy of the owner of the location information. The GEOPRIV working group has defined a protocol-independent model for access to geographic information. The model includes a location generator (LG) that produces location information, a location server (LS) that authorizes access to location information, a location recipient (LR) that requests and receives information, and a rulemaker (RM) that provides policy rules to the LS which enforce access control policies on access to a target.

The GEOPRIV working group provided mainly two results. [\[6\]](#) provides the building blocks for the Location Object (LO) itself which contains location information and authorization policies. Two policy rule namespaces have been defined. The first basic rule set, which can be found in [\[6\]](#), can restrict how long the receiver can retain location information and it can prohibit any further distribution. More sophisticated authorization policy rules can be attached to the LO itself (by value or by reference). Location server evaluate these rules to restrict access to location information. GEOPRIV does not reinvent a new location information format. Instead, a subset of GMLv3 is used to provide a rich and flexible mechanisms for representing location information. [Section 5](#) and [\[6\]](#) provide more details on location information encoding using XML in GMLv3. [\[7\]](#) gives details on authorization policies.

Network access servers are increasingly capable of providing user and device location information to AAA servers. This enables the AAA server to make additional authorization decisions based on the location of the user or access device. The home or visited network may also use the location information for other purposes (e.g. acting as a location server). The privacy issues discussed in GEOPRIV are especially applicable to the transport of Location Objects between administrative domains using the RADIUS protocol [\[5\]](#) . This document

describes the types of location information available to RADIUS clients and servers. It also analyses the various RADIUS usage scenarios with a view to providing security and privacy recommendations for the transport of location information. Finally, the document provides recommendations for the encoding of location and rule set information in the RADIUS protocol. The GEOPRIV requirements [3] will be the guiding document for these recommendations.

[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 [1].

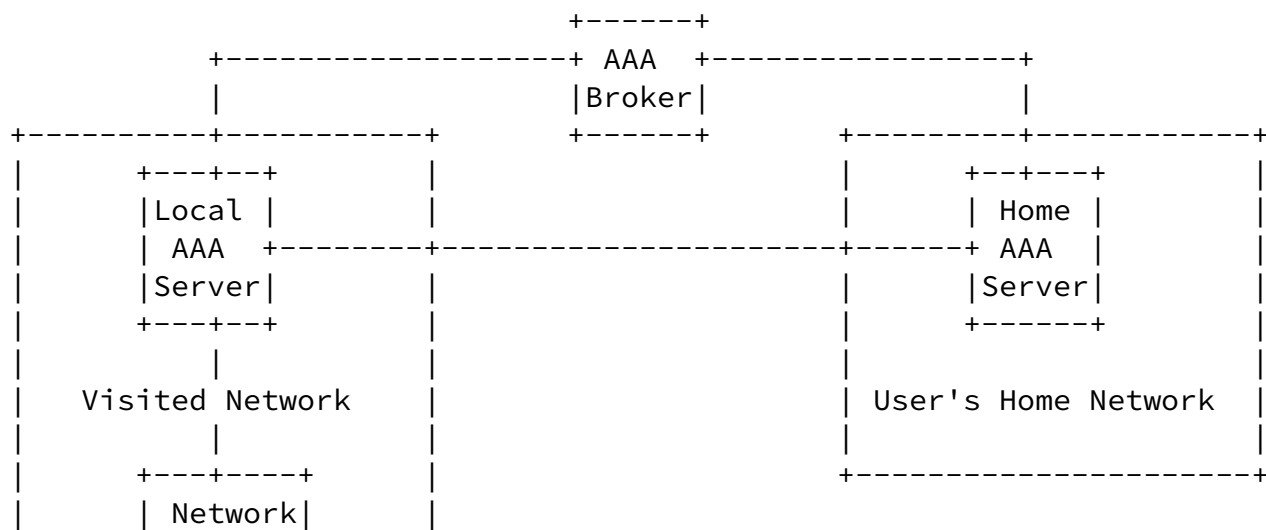
This document reuses the terminology of [3] for Geopriv specific terms such as location server (LS), location recipient (LR), target, using protocol, rule maker (RM) and location object (LO).

[3.](#) Framework and Scenarios

This section describes different models on how location information is retrieved and for which entity location information is requested. Requesting and using location information of a user certainly has privacy implications. In many cases the location information of the network might also reveal the current location of the user with a certain degree of precision depending on the mechanism used, to determine the location, update frequency, where the location was generated, size of the network and other mechanism (such as movement traces or interpolation).

We distinguish the case where location information of the visited network is desired whereas the location information of the end host is requested. The latter case can be distinguished from the former by considering the usage of this information. If location information is used for a purpose related to a user then we think it is inappropriate to ignore privacy aspects. In some usage scenarios the network access authentication procedure can be tightly coupled with the transfer of location information. This easily allows to correlate the authenticated user identity and its location

information.



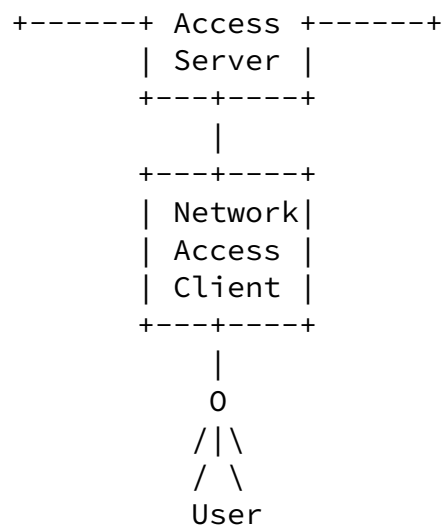


Figure 1: Framework

Figure 1 shows the different entities participating the various scenarios and note that they might have multiple roles in the Geopriv architecture. For example, the location generator might be the network access client, the user, the local AAA server or another entity in the network. The location server at the local network might be co-located with the AAA server but might also be a physically separated entity.

A future version of this document will include a discussion of a more fine-grain differentiation for location requests. The home AAA server is able to request the location object for a particular user or of the visited network.

Two variants can be considered. First, the Location Object is requested implicitly, i.e., the Location Object is attached during the network authentication exchange. Second, the home AAA server requests the LO explicitly. This has implications on how a query has

to be constructed (i.e., how does the home AAA server request the location object for a particular user).

Currently, we assume that the Location Object is sent from the visited AAA server to the home AAA server during or after a successful the network access authentication procedure.

Both RADIUS and DIAMETER have the ability to provide interim updates on network usage. Hence, this functionality can be used to periodically transmit upto date location information. The interval of these updates is typically dictated by the home network when the session is authorized.

[3.1](#) Location information about a network

The home AAA server requests location information about the visited network itself. In some cases (with a large visited network) it might be difficult to imply the location of a particular user (at least with a certain granularity). GMLv3 provides mechanisms describe the irregular shape of a network.

This scenario is useful particularly in cases where the network is non-stationary (such as trains, ships, busses) or where a relationship between the home network and the visited network is dynamically established and the visited network is, to some extent, not known to the home network.

If a user is authenticated/authorized only once by the Home AAA server for the use of the entire visited network, the Home AAA server may want to know the extent of the visited network prior to authorizing the usage. It may even return an authorized shape such that re-authorization is required if the user moves outside the specified shape.

From a privacy point of view this scenario is certainly simpler since the network is able to control disclosure of its own location information and is able to restrict its distribution (and its granularity). Still GEOPRIV is useful since both the location information format and mechanisms for authorization policy handling can be used. If location information is bundled with a particular user (or used in the context of a particular user) then the authors argue that privacy concerns are applicable. This leads us to the second usage scenario.

[3.2](#) Location information about an end user

The home AAA server requests (or automatically receives) the location object of a particular user. This assumes that the location of the

user is known to the visited network with a certain precision. The exchange might be combined with the initial network access authentication request or even with a later service request. In the latter case it is possible that the target (i.e., user) was already able to transfer some authorization policies to the access network to prevent unlimited distribution of location information. In the former case it is difficult for the end host to provide some rules to the visited network.

Additionally, it might even be possible that the end host itself provides location information to the local network. From a protocol point of view this message exchange might be outside of scope of this document. However, the consequence of such an exchange is that the network is able to retrieve highly accurate information and also policy rules which might allow disclosure of location information in many ways. Note that the end host might also provide incorrect information (i.e., lie about its current location) to the visited network which can only be prevented to a certain extent. Rules can be included per-value or per-reference. In case that rules are provided per-reference then the local network **MUST** resolve the reference before responding to redistributing it. For the purpose of providing location information to the home network the end host acts as location generator (LG) and most likely as rule maker (RM) and the local network acts as a location recipient (LR) with regard to location information relevant for the local network itself. However, to provide location information to the home network the local network itself acts as a location server (LS).

[3.3](#) Visited and Home network as a Location Server

Although not immediately applicable to Radius as a using protocol for Geopriv, the authors think that this issue deserves a short discussion. Both the visited and the home network might not be the final consumer of the location information itself. Once the infrastructure is deployed and useful applications are available there might be a strong desire to use location information for other purposes as well (such as location aware applications). Geopriv authorization rules are tailored for this environment as well.

As described in previous sections no ideal protocol is available for communication between the end host and the visited network to obtain location information of the end host. If the location itself is known then the user would have to communicate policies for disclosure of location information. Geopriv does not mandate a particular mechanism for carrying policies other than with the Location Object itself (per value and per reference). Many different protocols might be used to create, update or delete policies at a LS in the visited network. PANA [\[8\]](#) might be a protocol for carrying location objects between

Internet-Draft

GEOPRIV support for RADIUS

January 2003

the end host and the visited network or even for providing a URL to policies (the policies might be stored at the home network, for example). Since PANA does not provide confidentiality protection it is necessary to protect the Location Object with S/MIME which might lead to IP fragmentation. If authorization policies itself should be delivered to the network then XCAP [[10](#)] could be used.

The scenario for having the location server at the home network is much simpler since a strong trust relationship between the user and the home network is available. With the subscription of the user default policies can be configured.

[3.4](#) Default privacy-sensitive policy

This section talks about the default configuration for distributing location objects.

Two types of entities act as location servers in the configuration shown in Figure 1:

Entity in the visited network (e.g., visited AAA server): In this scenario it might be difficult to have policies retrieved from the end host (or user). In this case we have to assume that the visited network does not allow unrestricted distribution of location information. Hence, as a simplification we can assume that per default only the home network is allowed to receive location information.

Entity in the home network (e.g., home AAA server): An entity in the home network serves two purposes: First, it might be an ideal place for storing authorization policies and additionally it could store the user's location information for further distribution. In the latter case the home AAA server (or a similar entity) acts as a location server to respond to queries from location recipients. If the end host provides a location object then it might not always want to transport policies along with them. Instead it might be desirable to provide a reference to those objects stored at the home location server. As a default policy we specify that the home network MUST NOT distribute the user's location information for other. Per default MUST NOT distribute location information of a user to networks other than the user's home network.

[4.](#) RADIUS Usage Scenarios

[4.1](#) Home Network Access

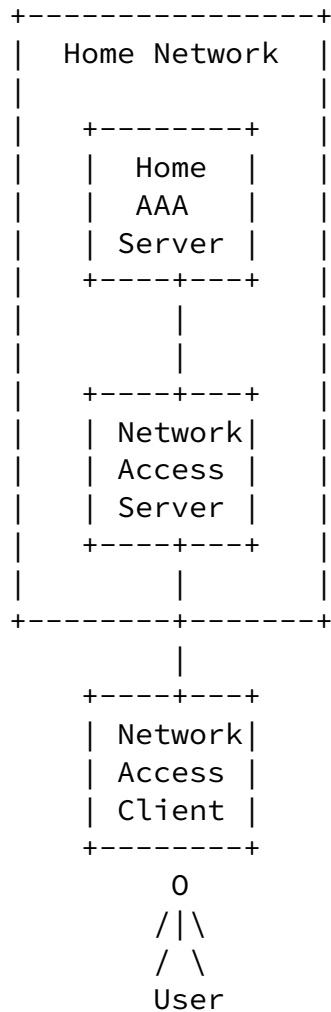


Figure 2: Home Network Access

In Figure 2, the user is requesting access to his or her home network. The RADIUS protocol is used to communicate the user's

identity and credentials from the NAS to the Home AAA Server. The NAS may also be in possession of location information at the time of authentication and this location information MAY be provided to the Home AAA Server in the Access-Request packet. If the NAS also determines the ruleset (or ruleset reference) which applies to the location information, it MUST forward it to the Home AAA server along with the location information.

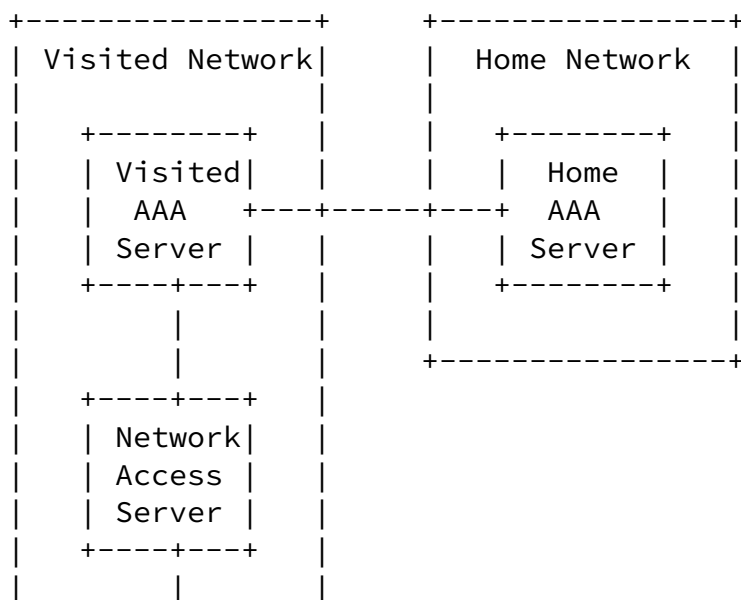
In this scenario, the NAS is considered to operate in the role of a Location Generator and NOT a Location Server. Consequently, RADIUS is NOT considered a 'Using Protocol' and the transport of the location and/or ruleset between NAS and Home AAA Server are not subject to the

GEOPRIV security and privacy requirements.

Note that Home AAA MAY also be capable of functioning as a Location Server but the protocol between such a Location Server and the Location Recipient is out of the scope of this draft.

Even though RADIUS does not serve as a Geopriv using protocol it is still useful to reuse results of the Geopriv working group with regard to the location information format. Using GMLv3 prevents to reinvent a new location format.

[4.2](#) Visited Network Access



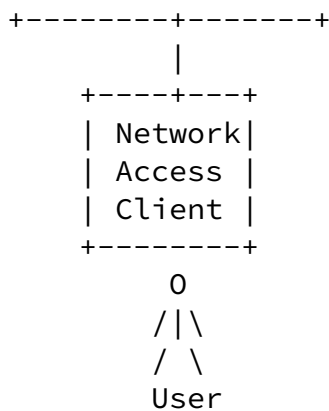


Figure 3: Visited Network Access

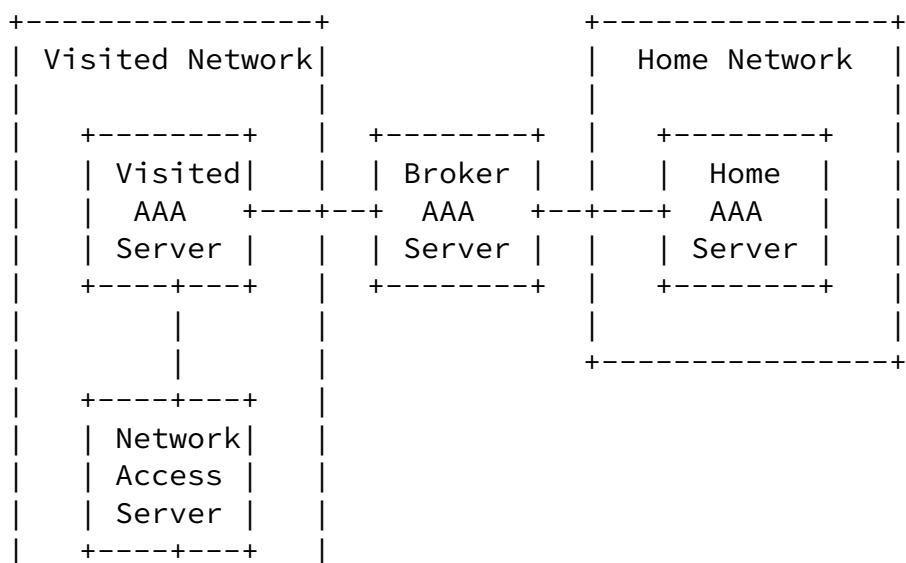
In Figure 3, the user is attempting to access a partner network. The RADIUS protocol is used to communicate the user's identity and credentials from the NAS to the Visited AAA Server and subsequently onto the Home AAA Server. In this scenario, the Visited AAA Server can be considered as acting in the role of Location Server whether or

not the location information is explicitly requested by the Home AAA Server. The Home AAA server is acting in the role of Location Recipient.

If the Visited AAA Server has determined both the location and applicable ruleset, it MUST evaluate the ruleset prior to communicating the location information to the Home AAA. If the rules allow forwarding, the Visited AAA Server MUST forward the ruleset along with the location information to the Home AAA Server.

If, however, the Visited AAA Server is unable to determine the applicable ruleset, it MUST advertise availability of the location information to the Home AAA Server and request the appropriate ruleset. If the Home AAA Server does not return the requested ruleset, the Visited AAA server MUST discard the location information.

[4.3](#) Visited Network Access via Broker



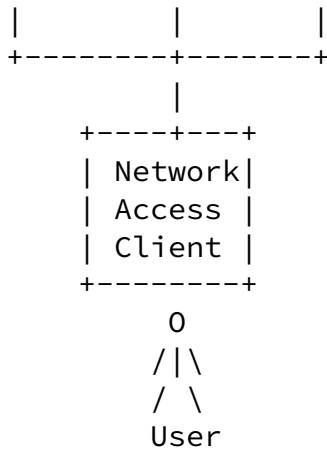


Figure 4: Visited Network Access via Broker

In Figure 4, the Visited and Home Network do not have a direct roaming agreement and so roaming is facilitated by an intermediary called a broker. The Broker AAA Server is responsible for routing AAA requests to the appropriate Home AAA Server and returning the results to the Visited AAA Server. The RADIUS protocol is used to communicate the user's identity and credentials from the NAS to Visited AAA Server to Broker AAA Server and finally onto the Home AAA Server. As in the previous section, the Visited AAA Server MUST NOT provide location information to the Broker AAA Server without first evaluating the rule set governing the usage of the information.

If the Visited AAA Server has determined both the location and applicable ruleset, it MUST evaluate the ruleset prior to communicating the location information to the Broker AAA Server. If the rules allow forwarding, the Visited AAA Server MUST forward the ruleset along with the location information to the Broker AAA Server. In turn, the Broker AAA Server MUST also evaluate the ruleset prior to communicating the location information and ruleset to the Home AAA

Server.

If the Visited AAA Server is unable to determine the ruleset, it MUST advertise availability of the location information to the Broker AAA Server and request the appropriate ruleset. If the Broker AAA Server is able to determine the ruleset, it MUST return the ruleset to the Visited AAA Server on request. If the Broker AAA Server is unable to determine the ruleset, the Broker AAA Server MUST forward the

advertisement of the availability of the location information to the Home AAA Server and request the appropriate ruleset. The Broker AAA server MUST NOT modify the ruleset returned by the Home AAA server prior to returning it to the Visited AAA server.

On receipt of the ruleset, the Visited AAA Server MUST evaluate it and only forward the location information to the Broker AAA server if permitted by the ruleset. In turn, the Broker AAA Server MUST also evaluate the ruleset prior to forwarding the location information and ruleset to the Home AAA Server. The ruleset MUST always accompany the forwarded location information and MUST NOT be modified in transit.

Geopriv defines both civil and geo-spatial location information which is useful in this context. Since GMLv3 does not provide civil location information the civil location format of [6] is used.

5.1 Civil Location

Civil location is a popular way to describe the location of an entity. Using an unstructured (as a text string) or a custom format for civil location format is dangerous since the automatic processing capabilities are limited.

The civil location format includes a number of fields, including the timezone, the country (expressed as a two-letter ISO 3166 code), and the administrative units of [11] A1 through A6. This designation offers street-level precision.

The description below is only included for completeness. A more detailed description can be found in [6].

The following civil location elements are defined:

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 direction	N, W
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

Table 1

An example of a civil location XML fragment is shown below:

```
<country>US</country>
<a1>NJ</a1>
<a2>Bergen</a2>
<a3>Leonida</a3>
<a6>Westview</a6>
```

[5.2](#) Geospatial Location

Geospatial location information is purely based on the capabilities

The Geography Markup Language (GML) as defined by OASIS provides powerful capabilities and is a flexible system for modelling topologies and for describing the location of an object. GML makes use of XML and [6] uses the 'feature.xsd' schema.

Location information based on GML is only one information element within PIDF-LO (defined in [6]). Location information is, as a 'location-info' element, encapsulated within the XML-based Presence Information Data Format (PIDF) (see [9]) which provides additional information such as a 'timestamp' element which shows the creation time of the PIDF document or the 'presence' element pointing to the URI of the entity whose location information the PIDF object describes.

Subsequently we provide some examples for location information. These examples are meant to illustrate the capability of GMLv3 'feature.xsd'.

The first example of a geospatial location XML fragment with the 'gml:Envelope' element. The Envelope element allows to define pairs of positions with opposite corners in arbitrary dimensions.

```
<gml:location>
  <gml:Envelope>
    <gml:pos>140. -35.</gml:pos>
    <gml:pos>1. 33.</gml:pos>
  </gml:Envelope>
</gml:location>
```

The second example shows the 'gml:EnvelopeWithTimePeriod' element which is an Envelope element that includes also a temporal extent. Including a time period is useful to indicate the duration in which the indicated location is valid.

```
<gml:EnvelopeWithTimePeriod>
  <gml:coord>
    <gml:X>12</gml:X>
  </gml:coord>
  <gml:coord>
```

```

        <gml:X>22</gml:X>
    </gml:coord>
    <gml:timePosition indeterminatePosition="after">
        2002-11-25T13:20:20</gml:timePosition>
    <gml:timePosition indeterminatePosition="before">
        2002-11-25T13:25:20</gml:timePosition>
</gml:EnvelopeWithTimePeriod>

```

The next few examples show more sophisticated structures such as the

'gml:Polygon' or the 'gml:LinearRing' element. A LinearRing is defined by four or more coordinate tuples, with linear interpolation between them; the first and last coordinates must be coincident. A Polygon is a special surface that is defined by a single surface patch. The boundary of this patch is coplanar and the polygon uses planar interpolation in its interior. It is backwards compatible with the Polygon of GML 2, GM_Polygon of ISO 19107 is implemented by PolygonPatch.

```

<gml:LinearRing>
  <gml:pos>1 1</gml:pos>
  <gml:pos>2 2</gml:pos>
  <gml:pos>3 3</gml:pos>
  <gml:pointRep>
    <gml:Point gml:id="p9876">
      <gml:pos>4 7</gml:pos>
    </gml:Point>
  </gml:pointRep>
</gml:LinearRing>

<gml:Polygon>
  <gml:exterior>
    <gml:LinearRing>
      <gml:coordinates>10,10 20,10 30,
        10 30,20 10,20 10,10</gml:coordinates>
    </gml:LinearRing>
  </gml:exterior>
</gml:Polygon>

```

Please note that the geographic position might be indicated using different coordinate reference systems. GMLv3 defines a number of

commonly used ones but allows the system to be extended to support other reference systems.

Encoding of location information within the 'gml:LocationString' element, which is a member of the locator attribute in the 'gml:Location' element, MUST NOT be used within Geopriv. Encoding of unstructured location information as a opaque string prevents interoperability and makes automatic processing difficult. If this type of location information is desired then civil location information should be used instead (see [Section 5.1](#)).

[6](#). Example

This section provides a complete example of location information based on PIDF [[9](#)] and PIDF-LO [[6](#)] including a basic ruleset (defined in PIDF-LO). Please note that the namespaces currently not yet registered and therefore we point to local files. An example with the more flexible authorization rules as defined with [[7](#)] will be provided in a future version of this 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"

  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:ietf:params:xml:ns:pidf
    ./pidfSchema.xsd
    urn:ietf:params:xml:ns:pidf:geopriv10:civilLoc
    ./pidf-lo-00-geopriv10-civilLoc.xsd
    urn:ietf:params:xml:ns:pidf:geopriv10
    ./pidf-lo-00-geopriv10.xsd"
  entity="pres:geotarget@example.com">

  <tuple id="sg89ae">
```

```

<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: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>2004-06-23T04:57:29Z</gp:retention-expiry>
    </gp:usage-rules>
  </gp:geopriv>
</status>
<timestamp>2003-06-22T20:57:29Z</timestamp>
</tuple>
</presence>

```

The "entity" XML element which is part of every PIDF document signifies the URI of the entity whose presence the document describes. This value of this attributes indicates the target of that location information. The "tuple id" element uniquely identify the PIDF segment which allow easy tracking over time. The "timestamp" element designates the time at which the PIDF document was created and it corresponds to the sighting time as stated in requirement 2.7a of [3].

Based on the description in [Section 5](#) it can be seen that civil location is embedded within the PIDF-LO and PIDF document. PIDF provides elements (such as timestamp) and also contains XML elements offered by PIDF-LO (for example the basic authorization rules 'retention-expiry' and 'retransmission-allowed'). PIDF-LO offers support for civil and gespatial location information.

[7](#). Packet Formats

In a previous section, it was stated that the Visited AAA MUST NOT forward the location information to the Broker or Home AAA prior to evaluating the governing rule set. This is accomplished by the Visited AAA including a RuleSetRequest attribute in the RADIUS Access-Request packet. The value of this attribute can be used to indicate whether the originator is capable of processing a RuleSet and/or RuleSet reference. A LocationOriginatorRealm attribute is also included in the RADIUS Access-Request in order to identify who is requesting the RuleSet.

The RuleSet or RuleSet reference is returned to the Visited AAA in either an Access-Accept or Access-Reject. It is returned in an Access-Accept if the location is NOT required by the Home AAA in order to complete the authorization for the session. It is returned in an Access-Reject if the location is required by the Home AAA in order to complete the authorization for the session. In the later case, the Visited AAA MUST resubmit the Access-Request after evaluating the RuleSet.

Attribute Name	Type	Request	Accept	Reject
LocationOriginatorRealm	text	0-1	0	0
RulesetRequest	integer	0-1	0	0
LocationObject	text	0-1	0	0
RuleSet	text	0-1	0-1	0-1

Table 2

- o 0 This attribute MUST NOT be present in packet.
- o 0+ Zero or more instances of this attribute MAY be present in packet.
- o 0-1 Zero or one instance of this attribute MAY be present in packet.
- o 1 Exactly one instance of this attribute MUST be present in packet.

TBD: Add packet size considerations.

TBD: Add attribute descriptions, encodings and types.

TBD: Need IANA considerations section for new attribute types.

8. Security Considerations

The Geopriv requirements draft [3] addresses the minimal security protection required for the Location Object: Mutual end-point authentication, data object integrity, data object confidentiality and replay protection. These security properties are implemented via S/MIME and between elements. Protection for the LO includes any attached authorization rules.

To capture the different scenarios we need to address them individually:

If location information of the visited network is requested by the home network then the visited network acts as a location server (LS) and as a location generator (LG). As such the visited network is able to restrict the distribution of location information.

If location information of the user is requested by the home network then the extensions to RADIUS defined in this draft suggest to use it as a using protocol. The protocol capabilities make RADIUS a non-classic using protocol since the initial network access authentication procedure might serve the purpose of attaching location information to the exchange. Additionally, RADIUS can be used to request location information periodically to keep the Location Server at the home network uptodate with the current location of the end user and its movement patterns.

If location information (either of the user, visited network or home network) is requested then the results of Geopriv are applicable. Although this communication exchange is not directly applicable for Radius itself it is useful to consider it in the larger context of privacy considerations.

Protection needs to be protected in two fashions. First, it is necessary to use authorization policies to prevent the unauthorized distribution of location information. Second, it is necessary to fulfill the security requirements of the Geopriv requirements draft. These requirements are inline with the Geopriv threats draft (see [2]). [6] proposes S/MIME to protect the Location Object against modifications and against eavesdropping. To provide mutual authentication confidentiality protection and a digital signature is necessary. Furthermore, to offer replay protection a gurantee of freshness is necessary (for example, based on timestamps).

The security of S/SIME is based on public key cryptography which raises some performance and deployment questions. Encryption requires that the local AAA server knows the recipients (i.e., home AAA

servers) public key. Some sort of public key infrastructure is

therefore required to obtain the public key (at the visited network) and to verify the digital signature (at the home network). Providing per-object cryptographic protection is, both at the home and at the visited network, quite expensive.

To overcome this limitation an alternative approach is suggested. Two security mechanisms are proposed for RADIUS:

- o [5] proposes the usage of a static key which is not appropriate for protection of location information due to the missing dynamic key management and absent confidentiality protection. If no authentication, integrity and replay protection between the participating entities are provided then an adversaries can spoof and modify transmitted AVPs.
- o RADIUS over IPsec [4] allows to run standard key management mechanisms, such as KINK, IKE and IKEv2, to establish IPsec security associations. Confidentiality protection MUST be used to prevent eavesdropper gaining access to location information. Confidentiality protection is not only a property required by this document, it is also required for the transport of keying material in the context of EAP authentication and authorization. Hence, this requirement is, in many environments, already fulfilled. Mutual authentication must be provided between the local AAA server and the home AAA server to prevent man-in-the-middle attacks. This is another requirement raised in the area of key transport with RADIUS and does not represent a deployment obstacle. The performance advantages a superior compared to the usage of S/MIME and object security since the expensive authentication and key exchange protocol run needs to be provided only once (at for a long time). Symmetric channel security with IPsec is highly efficient. Since IPsec protection is suggested as a mechanism to protect RADIUS already no additional considerations need to be addressed beyond those described in [4].

IPsec protection therefore seems to be adequate.

Where an untrusted AAA intermediary is present, the Location Object MUST NOT be provided to the intermediary. This can be avoided by use of re-directs or by using S/MIME encryption.

[9.](#) Open Issues

This section lists some open issues which have been identified while working on this approach:

- o The size of the Location Object might be large when encoded in XML. A discussion of possible approaches for 'compressing' the location object needs to be provided in a future version of this document.
- o Tentative open issue: Packet formats
- o DIAMETER is also a good (or even a better) candidate to carry Location Object as described in this document. The authors decided to start with RADIUS but there are not reasons why the same mechanism should not be supported by DIAMETER.

Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.
- [2] Danley, M., "Threat Analysis of the geopriv Protocol", [draft-ietf-geopriv-threat-analysis-01](#) (work in progress), September 2003, <reference.I-D.ietf-geopriv-threat-analysis.xml>.
- [3] Cuellar, J., Morris, J., Mulligan, D., Peterson, D. and D. Polk, "Geopriv requirements", [draft-ietf-geopriv-reqs-04](#) (work in progress), October 2003, <reference.I-D.ietf-geopriv-reqs.xml>.
- [4] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", [RFC 3579](#), September 2003.
- [5] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.
- [6] Peterson, J., "A Presence-based GEOPRIV Location Object Format", [draft-ietf-geopriv-pidf-lo-00](#) (work in progress), January 2004, <reference.I-D.ietf-geopriv-pidf-lo.xml>.

- [7] Tschofenig, H., Morris, J., Cuellar, J., Polk, J. and H. Schulzrinne, "Policy Rules for Disclosure and Modification of Geographic Information", [draft-ietf-geopriv-policy-00](#) (work in progress), November 2003, <reference.I-D.ietf-geopriv-policy.xml>.

Informative References

- [8] Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", [draft-ietf-pana-pana-02](#) (work in progress), October 2003, <reference.I-D.ietf-pana-pana.xml>.
- [9] Sugano, H. and S. Fujimoto, "Presence Information Data Format (PIDF)", [draft-ietf-imp-pim-pidf-08](#) (work in progress), May 2003, <reference.I-D.ietf-imp-pim-pidf.xml>.
- [10] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", [draft-ietf-simple-xcap-01](#) (work in progress), October 2003, <reference.I-D.ietf-simple-xcap.xml>.
- [11] Schulzrinne, H., "DHCP Option for Civil Location", [draft-ietf-geopriv-dhcp-civil-00](#) (work in progress), July 2003, <reference.I-D.ietf-geopriv-dhcp-civil.xml>.

Authors' Addresses

Mark Jones
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
CANADA

E-Mail: mark.jones@bridgewatersystems.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

E-Mail: Hannes.Tschofenig@siemens.com

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

E-Mail: Jorge.Cuellar@siemens.com

Jones, et al.

Expires July 2, 2003

[Page 27]

Internet-Draft

GEOPRIV support for RADIUS

January 2003

[Appendix A](#). Contributors

Add your name here.

[Appendix B](#). Acknowledgments

This document is partially based on the discussions within the IETF GEOPRIV working group.

Some parts of this document are based on other Geopriv documents (for obvious reasons). For editorial reasons some paragraphs are included in this draft but might be replaced by a reference in a future version. The authors thank Henning Schulzrinne, James Polk and John Morris for their work they have done in the Geopriv working group. Henning additionally provided the civil location content found in this draft.

Furthermore, we also have 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 time discussing a number of details with us. It was fun to work with them.

Finally, we would like to thank Hongkun Jiang <jiang@in.tum.de> for this assistance with GMLv3.

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). 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 assignees.

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

Internet-Draft

GEOPRIV support for RADIUS

January 2003

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

Acknowledgment

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

Jones, et al.

Expires July 2, 2003

[Page 31]