Geopriv
Internet-Draft
Expires: December 27, 2006

H. Tschofenig
Siemens
F. Adrangi
Intel
M. Jones
A. Lior
Bridgewater
June 25, 2006

Carrying Location Objects in RADIUS
draft-ietf-geopriv-radius-lo-07.txt

Status of this Memo

Copyright Notice

Abstract

This document describes RADIUS attributes for conveying access network ownership and location information based on a civic and geospatial location format.

The distribution of location information is a privacy sensitive task. Dealing with mechanisms to preserve the user's privacy is important and addressed in this document.

Table of Contents

1. Introduction

Wireless LAN (WLAN) access networks are being deployed in public places such as airports, hotels, shopping malls, and coffee shops by a diverse set of operators such as cellular network operators (GSM and CDMA), Wireless Internet Service Providers (WISPs), and fixed broadband operators.

When a user executes the network access authentication procedure to such a network, information about the location and ownership of this network needs to be conveyed to the user's home network to which the user has a contractual relationship. The main intent of this document is to enable location aware billing (e.g., determine the appropriate tariff and taxation in dependence of the location of the access network/user), location aware subscriber authentication and authorization for roaming environments and to enable other location aware services.

This document describes AAA attributes that are used by a AAA client or a local AAA server in an access network for conveying location-related information to the user's home AAA server.

Although the proposed attributes in this draft are intended for wireless LAN deployments, they can also be used in other types of wireless and wired networks whenever location information is required.

Location information needs to be protected against unauthorized access and distribution to preserve the user's privacy. [10] defines requirements for a protocol-independent model for the access to geographic location information. The model includes a Location Generator (LG) that creates location information, a Location Server (LS) that authorizes access to location information, a Location Recipient (LR) that requests and receives information, and a Rule Maker (RM) that provides authorization policies to the LS which enforces access control policies on requests to location information.

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].

RADIUS specific terminology is borrowed from [2] and [3].

Terminology related to privacy issues, location information and authorization policy rules is taken from [10].

Based on today's protocols we assume that the location information is provided by the access network where the end host is attached. As part of the network attachment authentication to the AAA server location information is sent from the AAA client to the AAA server. The authenticated identity might refer to a user, a device or something else. Although there might often be a user associated with the authentication process (either directly or indirectly; indirectly when a binding between a device and a user exists) there is no assurance that a particular real-world entity (such as a person) triggered this process. Since location based authorization is executed based on the network access authentication of a particular "user" it might be reasonable to talk about user's privacy within this document even though scenarios exist where this might not apply (and device or network privacy might be the correct term). Furthermore, the authors believe that there is a relationship between the NAS (or other nodes in the access network) and the location of the entity that triggered the network access authentication, such as the user. The NAS might in many cases know the location of the end host through various techniques (e.g., wire databases, wireless triangulation). Knowing the location of a network (where the user or end host is attached to) might in many networks also reveal enough information about the location of the user or the end host. A similar assumption is also made with regard to the location information obtained via DHCP (see for example [4]). This information might be used by applications in other protocols (such as SIP [11] with extensions [12]) to indicate the location of a particular user even though the location "only" refers to the location of the network or equipment within the network. This assumption might not hold in all scenarios but seems to be reasonable and practicable.

Please note that the authors use the terms end host and user interchangably with respect to the used identities as part of the network access authentication. The term 'user' is used whenever the privacy of the user could potentially be compromised.

3. Delivery Methods for Location Information

Location Objects, which consist of location information and privacy rules, are transported over the RADIUS protocol from the visited access network to the home AAA server. To embed a Location Object into RADIUS a number of attribute are used, such as Location-Information attribute, Basic-Policy-Rules attribute, Extended-Policy-Rules attribute, Operator-Name attribute. These attributes can be delivered to the RADIUS server during the authentication/ authorization phase described in Section 3.1, or in the mid-session using the dynamic authorization protocol framework described in Section 3.2. This section describes messages flows for both delivery methods.

3.1. Authentication/Authorization Phase Delivery

Figure 1 shows an example message flow for delivering location information during the network access authentication/authorization procedure. Upon a network authentication request from an access network client, the NAS submits a RADIUS Access-Request message which contains location information attributes among other required attributes. The attributes (including location information) are added based on some criteria, such as local policy, business relationship with subscriber's home network provider and in case of location information also considering privacy policies.

```
    +---------+            +---------+                  +---------+
    | Network |            | Network |                  |   AAA   |
    | Access  |            | Access  |                  |  Server |
    | Client  |            | Server  |                  |         |
    +---------+            +---------+                  +---------+
        |                       |                              |
        | Authentication phase  |                              |
        | begin                 |                              |
        |---------------------->|                              |
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Access-Request               |
        |                       | + Location-Information       |
        |                       |----------------------------->|
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Access-Accept                |
        |                       |<-----------------------------|
        | Authentication        |                              |
        | Success               |                              |
        |<----------------------|                              |
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Accounting-Request           |
        |                       | + Location-Information       |
        |                       |----------------------------->|
        |                       |                              |
```

Figure 1: Location Delivery based on out-of-band Agreements

If no location information is provided by the RADIUS client although it is required by the RADIUS server to compute an authorization decision then the RADIUS server challenges the RADIUS client. This exchange is shown in Figure 2. The Access-Challenge thereby provides a hint to the Network Access Server regarding the type of location information attributes that are desired. In the shown message flow these attributes are then provided in the subsequent Access-Request message. When receiving this Access-Request message the authorization procedure at the RADIUS server might be based on a number of criteria, including the newly defined Location-Information and Operator-Name attributes.

```
    +---------+             +---------+                   +---------+
    | Network |             | Network |                   |   AAA   |
    | Access  |             | Access  |                   |  Server |
    | Client  |             | Server  |                   |         |
    +---------+             +---------+                   +---------+
        |                       |                              |
        | Authentication phase  |                              |
        | begin                 |                              |
        |---------------------->|                              |
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Access-Request               |
        |                       | + Challenge-Capable          |
        |                       |----------------------------->|
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Access-Challenge             |
        |                       |  + Rule set Information      |
        |                       |  + Requested-Info            |
        |                       |<-----------------------------|
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Access-Request               |
        |                       | + Location-Information       |
        |                       |----------------------------->|
        |                       |                              |
        :                       :                              :
        :       Multiple Protocol Exchanges to perform         :
        :    Authentication, Key Exchange and Authorization    :
        :                  ...continued...                     :
        :                       :                              :
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Access-Accept                |
        |                       |  + Requested-Info            |
        |                       |<-----------------------------|
        | Authentication        |                              |
        | Success               |                              |
        |<----------------------|                              |
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Accounting-Request           |
        |                       | + Location-Information       |
        |                       |----------------------------->|
        |                       |                              |
```

Figure 2: Location Delivery based on Request

If the AAA server needs to obtain location information also in accounting messages then it needs to include a Requested-Info attribute to the Access-Accept to express that is desired (if privacy policy allow it) and the Network Access Server SHOULD then include location information to the RADIUS accounting messages .

3.2. Mid-session Authorization

The mid-session delivery method uses the Change of Authorization (COA) message as defined in [5]. At anytime during the session the RADIUS server MAY send a COA message containing session identification attributes and a Requested-Info attribute attribute to the AAA client if authorization policies allow it. The COA message MAY instruct the RADIUS client to generate an Authorize-Only Access-Request (Access-Request with Service-Type set to "Authorize-Only") in which case the RADIUS client includes location information in this Access-Request if policies allow it.

Figure 3 shows the approach graphically.

```
 +---------+                                      +---------+
 |   AAA   |                                      |   AAA   |
 |  Client |                                      |  Server |
 |  (NAS)  |                                      |         |
 +---------+                                      +---------+
     |                                                 |
     |  COA  + Service-Type "Authorize Only"           |
     |       + Requested-Info                          |
     |<------------------------------------------------|
     |                                                 |
     |  COA NAK + Service-Type "Authorize Only"        |
     |          + Error-Cause  "Request Initiated"     |
     |------------------------------------------------>|
     |                                                 |
     | Access-Request + Service-Type "Authorize Only"|
     |                + Location-Information           |
     |                + Policy-Rules                   |
     |------------------------------------------------>|
     |                                                 |
     | Access-Accept                                   |
     |<------------------------------------------------|
     |                                                 |
```

Figure 3: Mid-session Authorization

Upon receiving the Access-Request message containing the Service-Type hint attribute with a value of Authorize-Only from the NAS, the

RADIUS server responds with either an Access-Accept or an Access-Reject message.

Since location information can be sent in accounting records (including accounting interim records), RFC 3576 [5] is only needed for authorization changes.

4. Scenarios

In the following subsections we describe two scenarios for use of location information. The location information may refer to the (visited) network or to the end host. How the network obtains the end hosts location information is out of the scope of this document. There are two potential consumers of location information: the AAA server and location-based services. The privacy implications of these scenarios are described in Section 9.

4.1. Scenario 1 - Use of Location Information in AAA

The home network operator requires location information for authorization and billing purposes. The operator may deny service if location information is not available, or it may offer limited service. The NAS delivers location information to the home AAA server.

The location of the AAA client and/or the end host is transferred from the NAS to the RADIUS server (based on a pre-established agreement or if the RADIUS server asks for it under consideration of privacy policies). The NAS and intermediaries (if any) are not allowed to use that information other than to forward it to the home network.

The RADIUS server authenticates and authorizes the user requesting access to the network. If the user's location policies are available to the RADIUS server, the RADIUS server MUST deliver those policies in an Access Accept to the RADIUS client. This information MAY be needed if intermediaries or other elements want to act as Location Servers (see Section 4.2). If the NAS or intermediaries do not receive policies from the RADIUS server (or the end host itself) then they MUST NOT make any use of the location information other than forwarding it to the user's home network.

Location Information may also be reported in accounting messages. Accounting messages are generated when the session starts, stops and periodically. Accounting messages may also be generated when the user roams during handoff. This information may be needed by the billing system to calculate the user's bill. For example, there may be different tariffs or tax rates applied based on the location. Unless otherwise specified by authorization rules, location information in the accounting stream MUST NOT be transmitted to third parties.

The location information in the accounting stream MUST only be sent in the proxy chain to the home network (unless specified otherwise).

4.2. Scenario 2 - Use of Location Information for Other Services

Location Servers are entities that receive the user's location information and transmit it to other entities. In this second scenario, Location Servers comprise also the NAS and the RADIUS server. The RADIUS servers are in the home network, in the visited network, or in broker networks.

Unless explicitly authorized by the user's location policy, location information MUST NOT be transmitted to other parties outside the proxy chain between the NAS and the Home RADIUS server.

Upon authentication and authorization, the home RADIUS server MUST transmit the ruleset (if available) in an Access-Accept. The RADIUS client, intermediate proxies are allowed to share location information if they received ruleset indicates that it is allowed.

5. Attributes

This section defines the Operator-Name, Location-Information, Basic Policy Rules, Extended Policy Rules, and the Capability attribute.

5.1. Operator-Name Attribute

This attribute contains the operator namespace and the operator name. The operator name is combined with the Namespace to uniquely identify the owner of an access network. The value of the Operator-Name is a non-NULL terminated string whose length MUST NOT exceed 253 bytes. The attribute value uniquely identifies the operator name within the scope of the operator namespace

This Namespace field within the Operator-Name attribute provides information about the operator namespace.

This document defines four values for this attribute: GSM, CDMA, REALM and ITU.

Additional namespaces require IANA registration and MUST be associated with an organization responsible for assigning and managing the operator namespace.

GSM (0):

This namespace can be used to indicate operator names based on GSMA TADIG codes. The TADIG Working Group within the GSM Association is the authority responsible for issuing unique Operator-Name values of this type.

CDMA (1):

The CDMA operator namespace can be used to indicate operator names based on the Home Network Identifier (HNI). The HNI is the concatenation of the 3-digit Mobile Country Code (MCC) and 3-digit Mobile Network Code (MNC). The IMSI Oversight Council (IOC) is the authority responsible for issuing unique Operator-Name values for operators of this type.

REALM (2):

The REALM operator namespace can be used to indicate operator names based on any registered domain name. Such names are required to be unique and the rights to use a given realm name are obtained coincident with acquiring the rights to use a particular

Fully Qualified Domain Name (FQDN).

ITU (3):

The ITU operator namespace can be used to indicate operator names based on ITU Carrier codes. The Telecommunication Standardization Bureau (TSB) within the ITU-T is the authority responsible for the repository. Each national regulatory authority is responsible for issuing unique Operator-Name values for operators of this type.

The Operator-Name attribute SHOULD be sent in Access-Request, and Accounting-Request records where the Acc-Status-Type is set to Start, Interim, or Stop.

A summary of the Operator-Name attribute is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Value             ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Value (cont.)                                          ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

To Be Assigned by IANA - Operator-Name

Length:

>= 5

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Namespace   | Operator-Name                                ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Operator-Name                                                ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Namespace:

The value within this field contains the Operator Namespace identifier. The Namespace value is encoded as an 8-bit unsigned integer value.

Example: 2 for REALM

Operator-Name:

The text field of variable length contains an Access Network Operator Name. This field is a RADIUS base data type of Text.

Example: anyisp.com

5.2. Location-Information Attribute

Location-Information attribute SHOULD be sent in Access-Request and in Accounting-Request messages. For the Accounting-Request message the Acc-Status-Type may be set to Start, Interim or Stop.

The Location-Information Attribute provides meta-data about the location information, such as sighting time, time-to-live, mechanism that was used to determine the location information, etc. The format is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Value             ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Value (cont.)                                          ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

  To Be Assigned by IANA - Location-Information

Length:

  >= 21

Value:

  The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. The fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Index                       | Code          |  Entity       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Sighting Time                                                 ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Sighting Time                                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Time-to-Live                                                 ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Time-to-Live                                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Method                                                     ...
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Index (16 bits):

The 16-bit unsigned integer value allows to associate the Location-Information attribute with Location-Info-Civic and Location-Info-Geo attributes.

Code (8 bits):

Describes the location format that is carried in this attribute as an unsigned 8-bit integer value. Two values are defined by this document:

(0) describes civic location information
(1) describes geospatial location information

Entity (8 bits):

This field encodes which location this attribute refers to as an unsigned 8-bit integer value. Two values are defined by this document:

(0) describes the location of the user's client device
(1) describes the location of the AAA client

Sighting Time (64 bits):

NTP timestamp for the 'sighting time' field.

Time-to-Live (64 bits):

NTP timestamp for the 'time-to-live' field.

Method (variable):

Describes the way that the location information was determined. The values are registered with the 'method' Tokens registry by RFC 4119. The data type of this field is a string.

The following two fields need some explanation:

sighting time:

This field indicates when the Location Information was accurate. The data type of this field is a string and the format is a 64 bit

NTP timestamp [13].

time-to-live:

This field gives a hint until when location information should be considered current. Note that the time-to-live field is different than retention-expires, which indicates the time the recipient is no longer permitted to possess the location information and its encapsulating Location Object. The data type of this field is a string and the format is a 64 bit NTP timestamp [13].

The length of the Location-Information Attribute MUST NOT exceed 253 octets.

5.3. Location-Info-Civic Attribute

Civic location is a popular way to describe the location of an entity. For the RADIUS protocol civic location information is an opaque object and the RADIUS server parses the location information based on the encoding format defined in [4]. The data format described in Section 3.1 of [4] is used, with the exception that the first octet (DHCP option code) is not included.

Location-Info-Civic attribute SHOULD be sent in Access-Request and in Accounting-Request messages. For the Accounting-Request message the Acc-Status-Type may be set to Start, Interim or Stop.

The Location-Information attribute provides information about civic location information. The format is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Value             ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Value (cont.)                                          ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

  To Be Assigned by IANA - Location-Info-Civic

Length:

  >= 21

Value:

  The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Index                       |  Civic Location              ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Civic Location                                              ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Index (16 bits):

  The 16-bit unsigned integer value allows to associate the Location-Info-Civic attribute with the Location-Information attributes.

Civic Location (variable):

  The format of the data is described in Section 3.1 of [4] whereby the first 8 bits (i.e., the code for this DHCP option) are not included.

5.4. Location-Info-Geo Attribute

Geospatial location information is encoded as an opaque object whereby the format is reused from [6]. The RFC 3825 Location Configuration Information (LCI) format defined in Section 2 of [6] starting with bit 17 (i.e., the code for the DHCP option and the

length field is not included.).

Location-Info-Geo attribute SHOULD be sent in Access-Request, and Accounting-Request records where the Acc-Status-Type is set to Start, Interim or Stop if available.

The Location-Information attribute provides information about geospatial location information. The format is shown below.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |    Length     |             Value             ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |       Value (cont.)                                           ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

To Be Assigned by IANA - Location-Info-Geo

Length:

>= 21

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Index                       | Geo Location                  ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Geo Location                                                 ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Index (16 bits):

The 16-bit unsigned integer value allows to associate the Location-Info-Geo attribute with the Location-Information attributes.

Geo Location (variable):

The RFC 3825 Location Configuration Information (LCI) format defined in Section 2 of RFC 3825 starting with bit 17 (i.e., the code for the DHCP option and the length field is not included.).

5.5. Basic Policy Rules Attribute

In some environments it is possible for the user to attach information about its privacy preferences available to the network. These preferences allow the visited network, intermediate RADIUS

proxies and the home network to authorize the distribution of the user's location information. The home network will typically possess the user's authorization policies.

Without the user providing authorization information two approaches are possible:

- The user hides its identity information from the access network and from intermediate networks using the appropriate network access authentication mechanism. Section 9 discusses these issues in more details.

- The access network attaches default authorization policies which indicates that intermediate networks and the home network should not distribute the location information to other entities. If the user is able to provide authorization policies to the NAS then these policies will be attached. Additionally, the home network might have authorization policies which control distribution of location information. These policies are sent from the RADIUS server to the RADIUS client. Users can dynamically change their policies using the authroization framework defined in [14] and [15].

With regard to authorization policies this document reuses work done in [16] and encodes it in an non-XML format. Two fields ('sighting time' and 'time-to-live') are additionally included in the Location-Information attribute to conform to the Geopriv Requirements [10], Section 2.7. Two RADIUS attributes are used for this purpose: Basic-Policy-Rule and Extended-Policy-Rule attribute. The latter is defined in Section 5.6. The Basic-Policy-Rule attribute contains a fixed set of privacy relevant fields whereas the Extended-Policy-Rule attribute contains a reference to a more extensive authorization rule set.

The Basic-Policy-Rules attribute MUST be sent in an Access-Accept, an Access-Challenge, an Access-Request, an Access-Reject and an Accounting-Request message if location information is transmitted with this exchange. If authorization policy rules are available to the RADIUS client then the Access-Request MUST carry the Basic-Policy-Rules attribute to to the RADIUS server.

The format of the Basic-Policy-Rules attribute is shown below.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |            Value             ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|       Value (cont.)                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

To Be Assigned by IANA - Basic-Policy-Rules

Length:

>= 12

Value:

The Value field is at least 8 octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Flags                         | Retention Expires            ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Retention Expires                                             ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Retention Expires              | Note Well                    ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Note Well                                                     ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Flag (16 bits):

Only the first bit (R) is defined and corresponds to the retransmission-allowed field. All other bits are reserved and MUST be zero.

```
  0                   1
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |R|o o o o o o o o o o o o o o o|
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

o Reserved Flags

Retention Expires (64 bits):

NTP timestamp for the 'retention-expires' field.

Note Well (variable):

This field contains a URI which points to human readable privacy instructions. The data type of this field is string.

This document reuses fields of the 'usage-rules' element, described in [16]. These fields have the following meaning:

retransmission-allowed:

When the value of this element is '0', then the recipient of this Location Object is not permitted to share the enclosed location information, or the object as a whole, with other parties. The value of '1' allows to share the location information with other parties by considering the extended policy rules.

retention-expires:

This field specifies an absolute date at which time the Recipient is no longer permitted to possess the location information. The data type of this field is a string and the format is a 64 bit NTP timestamp [13].

note-well:

This field contains a URI which points to human readable privacy instructions. This field is useful when location information is distributed to third party entities, which can include humans in a location based service. RADIUS entities are not supposed to process this field.

Whenever a Location Object leaves the AAA system the URI in the note-well attribute MUST be expanded to the human readable text. For example, when the Location Object is transferred to a SIP based environment then the human readable text is placed in the text is put into the 'note-well' attribute inside the 'usage-rules' element inside the PIDF-LO document (see [16]).

5.6. Extended Policy Rules Attribute

The Extended-Policy-Rules attribute SHOULD be sent in an Access-Accept, an Access-Challenge, an Access-Request, an Access-Reject and an Accounting-Request message if location information is transmitted with this exchange. If authorization policy rules are available to the RADIUS client then the Access-Request MUST carry the Basic-Policy-Rules attribute to to the RADIUS server.

Ruleset reference field of this attribute is of variable length. It contains a URI that indicates where a richer ruleset is available. The full ruleset SHOULD be fetched using Transport Layer Security (TLS). As a deviation from [16] this field only contains a reference and does not carry an attached rule set. This modification is motivated by the size limitations imposed by RADIUS.

The format of the Extended-Policy-Rules attribute is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |             Value            ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Value (cont.)                                          ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

To Be Assigned by IANA - Extended-Policy-Rules

Length:

>= 4

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. The fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Ruleset reference                                          ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Ruleset reference:

This field contains a URI that points to policy rules.

5.7. Challenge-Capable Attribute

The Challenge-Capable attribute allows a NAS (or client function of a proxy server) to indicate support for processing general purpose Access-Challenge messages from the RADIUS server, beyond those specified for support of the authentication methods of textual challenge-response, CHAP or EAP. This mechanism allows the RADIUS

server to request additional information from the RADIUS client prior to making an authentication and authorization decision. The Challenge-Capable attribute MUST appear in Access-Request Messages, if the NAS supports this feature, as a hint to the RADIUS Server.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type          | Length        | Value                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

To Be Assigned by IANA - Challenge-Capable Attribute

Length:

4

Value:

The Value field is four octets.
Every bit of the two octets MUST be set to 0.

5.8. Requested-Info Attribute

The Requested-Info attribute allows the RADIUS server to indicate whether it needs civic and/or geospatial location information of the NAS or the end host (i.e., the entities that are indicated in the Entity field of the Location-Information attribute).

If the RADIUS server wants to dynamically decide on a per-request basis to ask for location information from the RADIUS client then the following cases need to be differentiated. If the AAA client and the AAA server have agreed out-of-band to mandate the transfer of location information for every network access authentication request then the issues listed below are not applicable.

- The RADIUS server requires location information for computing the authorization decision. If the RADIUS client does not provide location information with the Access-Request message then the Requested-Info attribute is attached to the Access-Challenge to indicate what is required. Two cases can be differentiated:

  1. If the RADIUS client sends the requested information then the RADIUS server can process the location-based attributes.

2. If the RADIUS server does not receive the requested information in response to the Access-Challenge (including the Requested-Info attribute) then the RADIUS server responds with an Access-Reject with an Error-Cause attribute (including the "Location-Info-Required" error value). Note that an Access-Reject message SHOULD only be sent if the RADIUS server MUST use location information for returning a positive access control decision.

- If the RADIUS server would like location information in the Accounting-Request message but does not require it for computing an authorization decision then an Access-Accept MUST include a Required-Info attribute. This is typically the case when location information is used for inclusion to the user's bill only. The RADIUS client SHOULD attach location information to the Accounting-Request (unless authorization policies dictate something different), if it is available.

If the RADIUS server does not send a Requested-Info attribute then the RADIUS client MUST NOT attach location information to messages to the RADIUS server The user's authorization policies MUST be consulted by the RADIUS server before requesting location information delivery from the RADIUS client.

Figure 11 shows a simple protocol exchange where the RADIUS server indicates the desire to obtain location information, namely civic location information of the user, to grant access. Since the Requested-Info attribute is attached to the Access-Challenge the RADIUS server indicates that location information is required for computing an authorization decision.

```
    +---------+                   +---------+
    | RADIUS  |                   | RADIUS  |
    | Client  |                   | Server  |
    +---------+                   +---------+
         |                              |
         |                              |
         | RADIUS                       |
         | Access-Request               |
         | + Challenge-Capable          |
         |----------------------------->|
         |                              |
         | RADIUS                       |
         | Access-Challenge             |
         | + Requested-Info             |
         |   ('CIVIC_LOCATION',         |
         |    'USERS_LOCATION')         |
         |<-----------------------------|
         |                              |
         | RADIUS                       |
         | Access-Request               |
         | + Location-Information       |
         |   (civic-location)           |
         |----------------------------->|
         |                              |
         |        ....                  |
```

Figure 11: RADIUS server requesting location information

The Requested-Info attribute MUST be sent by the RADIUS server if it wants the RADIUS client to return civic and/or geospatial information. This Requested-Info attribute MAY appear in the Access-Accept or in the Access-Challenge messages.

A summary of the attribute is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Value             ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Value (cont.)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:
  To Be Assigned by IANA - Requested-Info Attribute

Length:
  10

Value:

  The Value field is at least 8 octets in length, and the format is shown below. The data type of the Value field is string. The fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Requested-Info                                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Requested-Info                                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Requested-Info (64 bits):

  This text field contains an integer value that encodes the requested information attributes.
  Each capability value represents a bit position.

This document specifies the following capabilities:

Name:

   CIVIC_LOCATION

Description:

   The RADIUS server uses this attribute to request information from the RADIUS client to be returned. The numerical value representing CIVIC_LOCATION requires the RADIUS client to attach civic location attributes.

Numerical Value:

A numerical value of this attribute is '1'.

Name:

GEO_LOCATION

Description:

The RADIUS server uses this attribute to request information from the RADIUS client to be returned. The numerical value representing GEO_LOCATION requires the RADIUS client to attach geospatial location attributes.

Numerical Value:

A numerical value of this attribute is '2'.

Name:

USERS_LOCATION

Description:

The numerical value representing USERS_LOCATION indicates that the AAA client must sent a Location-Information attribute that contains location information with the Entity attribute expressing the value of zero (0). A value of zero indicates that the location information in the Location-Information attribute refers to the user's client device.

Numerical Value:

A numerical value of this attribute is '4'.

Name:

NAS_LOCATION

Description:

The numberical value representing NAS_LOCATION indicates that the AAA client must sent a Location-Information attribute that contains location information with the Entity attribute expressing the value of one (1). A value of one indicates that the location information in the Location-Information attribute refers to the AAA client.

Numerical Value:

A numerical value of this attribute is '8'.

If neither the NAS_LOCATION nor the USERS_LOCATION bit is set then per-default the location of the user's client device MUST be returned (if authorization policies allow it). If both the NAS_LOCATION and the USERS_LOCATION bits are set then the location information has to be put into separate attributes. If neither the CIVIC_LOCATION nor the GEO_LOCATION bit is set then per-default civic location information MUST be returned (if authorization policies allow it). If both the CIVIC_LOCATION and the GEO_LOCATION bits are set then the location information has to be put into separate attributes. The value of NAS_LOCATION and USERS_LOCATION refers to the location requested via CIVIC_LOCATION and/or via GEO_LOCATION. As an example, if the bits for NAS_LOCATION, USERS_LOCATION and GEO_LOCATION are set then location information of the AAA client and the users' client device are returned in a geospatial location format.

6. Table of Attributes

The following table provides a guide which attributes may be found in which RADIUS messages, and in what quantity.

Request	Accept	Reject	Challenge	Accounting Request	#	Attribute
0-1	0	0	0	0-1	TBD	Operator-Name
0+	0	0	0	0+	TBD	Location-Information
0+	0	0	0	0+	TBD	Location-Info-Civic
0+	0	0	0	0+	TBD	Location-Info-Geo
0-1	0-1	0-1	0-1	0-1	TBD	Basic-Policy-Rules
0-1	0-1	0-1	0-1	0-1	TBD	Extended-Policy-Rules
0	0-1	0	0-1	0	TBD	Requested-Info
0-1	0	0	0	0	TBD	Challenge-Capable

The Location-Information, the Location-Info-Civic and the Location-Info-Geo attribute MAY appear more than once. For example, if the server asks for civic and geospatial location information two Location-Information attributes need to be sent. If multiple Location-Information attributes are sent then they MUST NOT contain the same information.

The next table shows the occurrence of the error-cause attribute.

Request	Accept	Reject	Challenge	Accounting Request	#	Attribute
0	0	0-1	0	0	TBD	Location-Info-Required
0	0	0-1	0	0	101	Error-Cause

7. Diameter RADIUS Interoperability

When used in Diameter, the attributes defined in this specification can be used as Diameter AVPs from the Code space 1-255 (RADIUS attribute compatibility space). No additional Diameter Code values are therefore allocated. The data types and flag rules for the attributes are as follows:

Attribute Name	Value Type	AVP Flag rules MUST	MAY	SHLD NOT	MUST NOT	Encr
Operator-NameID	OctetString	M	P		V	Y
Location-Information	OctetString	M	P		V	Y
Location-Info-Civic	OctetString	M	P		V	Y
Location-Info-Geo	OctetString	M	P		V	Y
Basic-Policy-Rules	OctetString	M	P		V	Y
Extended-Policy-Rules	OctetString	M	P		V	Y
Requested-Info	OctetString	M	P		V	Y
Challenge-Capable	OctetString	M	P		V	Y

The attributes in this specification have no special translation requirements for Diameter to RADIUS or RADIUS to Diameter gateways; they are copied as is, except for changes relating to headers, alignment, and padding. See also Section 4.1 of [7] and Section 9 of [17].

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [17] or Diameter-EAP-Request [18]. What is said about Access-Challenge applies in Diameter to AA-Answer [17] or Diameter-EAP-Answer [18] with Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH. What is said about Access-Accept applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate success. Similarly, what is said about RADIUS Access-Reject packets applies in Diameter to AA- Answer or Diameter-EAP-Answer messages that indicate failure.

What is said about COA-Request applies in Diameter to Re-Auth-Request [17].

What is said about Accounting-Request applies to Diameter Accounting-Request [17] as well.

8. Matching with Geopriv Requirements

This section compares the Geopriv requirements described in [10] and the approach of distributing Location Objects with RADIUS.

The main usage scenario aimed for Location Object transport in RADIUS assumes that the Location Server and the Location Recipient are co-located at a single entity with regard to location based network access authorization, taxation and billing. In Section 8.1 and Section 8.2 we discuss privacy implications when RADIUS is not used according to these usage scenario.

In Section 8.3 Geopriv requirements are matched against these two scenarios.

8.1. Distribution of Location Information at the User's Home Network

This section focuses on location information transport from the local AAA server (acting as the Location Generator) to the home AAA server (acting as the Location Server). To use a more generic scenario we assume that the visited AAA and the home AAA server belong to different administrative domains. The Location Recipient obtains location information about a particular Target via protocols specified outside the scope this document (e.g., SIP, HTTP or an API).

Please note that the main usage scenario defined in this document assumes that the Location Server and the Location Recipient are co-located into a single entity with regard to location based network access authorization, taxation and billing.

The subsequent figure shows the interacting entities graphically.

```
    visited network    |        home network
                       |
                       |        +----------+
                       |        |  Rule    |
                       |        | Holder   |
                       |        |          |
                       |        +----+-----+
                       |             |
                       |         rule|interface
                       |             V
     +----------+      |        +----------+             +----------+
     |Location  |  publication  | Location |  notification |Location  |
     |Generator |<------------->| Server   |<------------->|Recipient |
     |          |  interface    |          |  interface    |          |
     +----------+      |        +----------+             +----------+
                       |
     Local AAA      RADIUS       Home AAA     SIP/HTTP/API/etc.
     Server            |         Server
                       |
```

Figure 16: Location Server at the Home Network

The term 'Rule Holder' in Figure 16 denotes the entity which creates the authorization ruleset.

8.2. Distribution of Location Information at the Visited Network

This section describes a scenario where Location Information is distributed by the visited network.

In order for this scenario to be applicable the following two assumptions must hold:

- The visited network deploys a Location Server and wants to distribute Location Objects of a user

- The visited network is able to learn the user's identity

The visited network provides location information to a Location Recipient (e.g., via SIP or HTTP). During the network access authentication procedure the visited network is able to retrieve the user's authorization policies from the home AAA server. This should ensure that the visited network acts according to the user's policies.

The subsequent figure shows the interacting entities graphically. The transport of the Location Object is not shown in this figure since this aspect is already covered in the previous paragraph.

```
    visited network     |        home network
                        |
     +----------+       |
     |Location  |       |
     |Recipient |       |
     |          |       |
     +----------+       |
          ^             |        +----------+
          |             |        |  Rule    |
          |             |        | Holder   |
      notification      |        |          |
       interface        |        +----+-----+
          |             |             |
          |             |         rule|interface
          v             |             V
     +----------+       |        +----------+
     |Location  | Rule Transport| Home AAA |
     |Generator |<------------->| Server   |
     |& Server  |   RADIUS      |          |
     +----------+       |        +----------+
                        |
```

Figure 17: Location Server at the Visited Network

8.3. Requirements matching

Section 7.1 of [10] details the requirements of a "Location Object".

There are:

Req. 1. (Location Object generalities):

* Regarding requirement 1.1, the Location Object has to be understood by the RADIUS server (and possibly a Diameter server in case of interworking between the two) as defined in this document. Due to the encoding of the Location Object it is possible to convert it to the format used in GMLv3 [19]. The same civic location information format is used in PIDF-LO [16] and this document.

* Regarding requirement 1.2, a number of fields in the civic location information format are optional.

* Regarding requirement 1.3, the inclusion of type of place item (CAtype 29) gives a further classification of the location. This attribute can be seen as an extension.

* Regarding requirement 1.4, the location information is not defined in this document but is extensible.

* Regarding requirement 1.5, the Location Object is useful for both receiving and sending location information as described in this document.

* Regarding requirement 1.6, the Location Object contains both location information and privacy rules. Location information is described in Section 5.2, in Section 5.3 and in Section 5.4. The corresponding privacy rules are detailed in Section 5.5 and in Section 5.6.

* Regarding requirement 1.7, the Location Object is usable in a variety of protocols. The format of the object is reused from other documents as detailed in the respective sections (see Section 5.2, Section 5.3, Section 5.4 Section 5.5 and in Section 5.6).

* Regarding requirement 1.8, the encoding of the Location Object has an emphasis on a lightweight encoding format. As such it is useable on constrained devices.

Req. 2. (Location Object fields):

* Regarding requirement 2.1, the Target Identifier is carried within the network access authentication protocol (e.g., within the EAP-Identity Response when EAP is used and/or within the EAP method itself). As described in Section 9 it has a number of advantages if this identifier is not carried in clear text. This is possible with certain EAP methods whereby the identity in the EAP-Identity Response only contains information relevant for routing the response to the user's home network. The user identity is protected by the authentication and key exchange protocol.

* Regarding requirement 2.2, the Location Recipient is in the main scenario the home AAA server. For a scenario where the Location Recipient is obtaining Location Information from the Location Server via HTTP or SIP the respective mechanisms defined in these protocols are used to identify the recipient. The Location Generator cannot, a priori, know the recipients if they are not defined in this protocol.

* Regarding requirement 2.3, the credentials of the Location Recipient are known to the RADIUS entities based on the security mechanisms defined in the RADIUS protocol itself.

Section 10 describes these security mechanisms offered by the RADIUS protocol. The same is true for requirement 2.4.

* Regarding requirement 2.5, Section 5.2, Section 5.3 and Section 5.4 describe the content of the Location Field. Since the location format itself is not defined in this document motion and direction vectors as listed in requirement 2.6 are not defined.

* Regarding requirement 2.6, this document only describes one Location Data Type for civic and for geospatial location information, respectively. No negotiation needs to take place.

* Regarding requirement 2.7, timing information is provided with 'sighting time' and 'time-to-live' field defined in Section 5.5.

* Regarding requirement 2.8, a reference to an external (more detailed ruleset) is provided with the Section 5.6 attribute.

* Regarding requirement 2.9, security headers and trailers are provided as part of the RADIUS protocol or even as part of IPsec.

* Regarding requirement 2.10, a version number in RADIUS is provided with the IANA registration of the attributes. New attributes are assigned a new IANA number.

Req. 3. (Location Data Types):

* Regarding requirement 3.1, this document reuses civic and geospatial location information as described in Section 5.4 and in Section 5.3.

* With the support of civic and geospatial location information support requirement 3.2 is fulfilled.

* Regarding requirement 3.3, the geospatial location information as defined in this document only refers to absolute coordinates. However, the granularity of the location information can be reduced with the help of the AltRes, LoRes, LaRes fields described in the Location-Information attribute (see Section 5.2).

* Regarding requirement 3.4, further Location Data Types can be added via new coordinate reference systems (CRSs) (see Datum field in the Location-Information attribute of Section 5.4),

extensions to existing fields or via additional attributes.

Section 7.2 of [10] details the requirements of a "Using Protocol". These requirements are listed below:

Req. 4.: The using protocol has to obey the privacy and security instructions coded in the Location Object and in the corresponding Rules regarding the transmission and storage of the LO. This document requires, that RADIUS entities sending or receiving location MUST obey such instructions.

Req. 5.: The using protocol will typically facilitate that the keys associated with the credentials are transported to the respective parties, that is, key establishment is the responsibility of the using protocol. Section 10 specifies how security mechanisms are used in RADIUS and how they can be reused to provide security protection for the Location Object. Additionally, the privacy considerations (see Section 9) are also relevant for this requirement.

Req. 6. (Single Message Transfer): In particular, for tracking of small target devices, the design should allow a single message/ packet transmission of location as a complete transaction. The encoding of the Location Object is specifically tailored towards the inclusion into a single message that even respects the (Path) MTU size. The concept of a transaction is not immediately applicable to RADIUS.

Section 7.3 of [10] details the requirements of a "Rule based Location Data Transfer". These requirements are listed below:

Req. 7. (LS Rules): With the scenario shown in Figure 16 the decision of a Location Server to provide a Location Recipient access to location information is based on Rule Maker-defined Privacy Rules which are stored at the home network or are accessible for the home network. With regard to the scenario shown in Figure 17 the Rule Maker-defined Privacy Rules are sent from the home network to the visited network as part of the Policy-Information attribute (see Section 5.5, Section 5.6 and Section 9 for more details).

Req. 8. (LG Rules): For mid-session delivery it is possible to enforce the user's privacy rules for the transfer of the Location Object. For the initial transmission of a Location Object the user would have to use network access authentication methods which provide user identity confidentiality which would render the Location Object completely useless for the visited network. For the scenario shown in Figure 16 the visited network is already in possession of the users location information prior to the authentication and authorization of the user. A correlation between the location and the user identity might, however, still not be possible for the visited network (as explained in Section 9). The visited network MUST evaluate ruleset provided by the home AAA server as soon as possible.

Req. 9. (Viewer Rules): The Rule Maker might define (via mechanisms outside the scope of this document) which policy rules are disclosed to other entities.

Req. 10. (Full Rule language): Geopriv has defined a rule language capable of expressing a wide range of privacy rules which is applicable in the area of the distribution of Location Objects. A basic ruleset is provided with the Basic-Policy-Rules attribute Section 5.5. A reference to the extended ruleset is carried in Section 5.6. The format of these rules are described in [14] and [15].

Req. 11. (Limited Rule language): A limited (or basic) ruleset is provided by the Policy-Information attribute Section 5.5 (and as introduced with PIDF-LO [16]).

Section 7.4 of [10] details the requirements of a "Location Object Privacy and Security". These requirements are listed below:

Req. 12 (Identity Protection): Support for unlinkable pseudonyms is provided by the usage of a corresponding authentication and key exchange protocol. Such protocols are available, for example, with the support of EAP as network access authentication methods. Some EAP methods support passive user identity confidentiality whereas others even support active user identity confidentiality. This issue is further discussed in Section 10. The importance for user identity confidentiality and identity protection has already been recognized (see for example a document on 'EAP Method Requirements for Wireless LANs' [20]).

Req. 13. (Credential Requirements): As described in Section 10 RADIUS signaling messages can be protected with IPsec. This allows a number of authentication and key exchange protocols to be used as part of IKE, IKEv2 or KINK.

Req. 14. (Security Features): Geopriv defines a few security requirements for the protection of Location Objects such as mutual end-point authentication, data object integrity, data object confidentiality and replay protection. As described in Section 10 these requirements are fulfilled with the usage of IPsec if the mutual authentication refers to the RADIUS entities (acting as various Geopriv entities) which directly communicate with each other.

Req. 15. (Minimal Crypto): A minimum of security mechanisms are mandated by the usage of RADIUS. Communication security for Location Objects between AAA infrastructure elements is provided by the RADIUS protocol (including IPsec and its dynamic key management framework) rather than on relying on object security via S/SIME (which is not available with RADIUS).

9. Privacy Considerations

This section discusses privacy implications for the distribution of location information within RADIUS.

In many cases the location information of the network also reveals the current location of the user with a certain degree of precision depending on the mechanism used, the positioning system, update frequency, where the location was generated, size of the network and other mechanisms (such as movement traces or interpolation).

Two entities might act as Location Servers as shown in Section 4, in Figure 16 and in Figure 17:

9.1. Entity in the visited network

In this scenario it is difficult to obtain authorization policies from the end host (or user) immediately when the user attaches to the network. In this case we have to assume that the visited network does not allow unrestricted distribution of location information to other than the intended recipients (e.g., to third party entities). When the AAA messages traverses one or more broker networks, the broker network is bound by the same guidelines as the visited network with respect to the distribution of location information.

The visited network MUST behave according to the following guidelines:

- o Per default only the home network is allowed to receive location information. The visited network MUST NOT distribute location information to third parties without seeing the user's privacy rule set.

- o If the home network provides the Basic-Policy-Rules attribute either as part of the Access-Accept, the Access-Reject or the Access-Challenge message then the visited network MUST follow the guidance given with these rules.

- o If the home network provides the Extended-Policy-Rules attributes either as part of the Access-Accept, the Access-Reject or the Access-Challenge message then the visited network MUST fetch the full ruleset at the indicated URL and MUST follow the guidance given with these rules.

- o If the RADIUS client in the visited network learns the basic rule set or a reference to the extended rule set by means outside the RADIUS protocol (e.g., provided by the end host) then it MUST include the Basic-Policy-Rules and the Extended-Policy-Rules

attribute in the Access-Request message towards the home AAA server. Furthermore, the visited network MUST evaluate these rules prior to the transmission of location information either to the home network or a third party. The visited network MUST follow the guidance given with these rules.

o If the RADIUS client in the visited network receives the Basic-Policy-Rules attribute with Access-Accept or the Access-Challenge message then the Basic-Policy-Rules MUST be attach in subsequent RADIUS messages which contain the Location-Information attribute (such as interim accounting messages).

o If the RADIUS client in the visited network receives the Extended-Policy-Rules attribute with Access-Accept or the Access-Challenge message then the Basic-Policy-Rules attribute MUST be attach in subsequent RADIUS messages which contain the Location-Information attribute (such as interim accounting messages).

9.2. Entity in the home network

The AAA server in the home network might be an ideal place for storing authorization policies. The user typically has a contractual relationship with his home network and hence the trust relationship between them is stronger. 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). Authorization policy rules described in [15] and in [14] are tailored for this environment. These policies might be useful for limiting further distribution of the user's location to other location based services. The home AAA server (or a similar entity) thereby acts as a location server for access to location services.

The home network MUST behave according to the following guidelines:

o As a default policy the home network MUST NOT distribute the user's location information to third party entities.

o If a user provides basic authorization policies then these rules MUST be returned to the visited network in the Access-Accept, the Access-Reject or the Access-Challenge message.

o If a user provides basic authorization policies then these rules MUST be returned to the visited network in the Access-Accept, the Access-Reject or the Access-Challenge message.

o If a user provides extended authorization policies then they MUST be accessible for the visited networking using a reference to

these rule set. The Extended-Policy-Rules attribute MUST include the reference and they MUST be sent to the visited network in the Access-Accept, the Access-Reject or the Access-Challenge message.

- o The home network MUST follow the user provided rule set for both local storage and for further distribution. With regard to the usage of these rules the home network MUST ensure that the users preferences are taken care of within the given boundaries (such as legal regulations or operational considerations). For example, a user might not want the home network to store information about its location information beyond a indicated time frame. However, a user might on the other hand want to ensure that disputes concerning the billed amount can be resolved. location information might help to resolve the dispute. The user might, for example, be able to show that he has never been at the indicated place.

- o If the policy rules provided by the user indicate that location information must not be distributed at all then the home network MUST provide the Basic-Policy-Rules to the RADIUS entity in the visited network via an Access-Accept, the Access-Reject and the Access-Challenge message. The RADIUS server in the user's home network would set the 'Retention-Expires' and the 'Retransmission-allowed' field to the user indicated value.

For the envisioned usage scenarios, the identity of the user and his device is tightly coupled to the transfer of location information. If the identity can be determined by the visited network or AAA brokers, then it is possible to correlate location information with a particular user. As such, it allows the visited network and brokers to learn movement patterns of users.

The identity of the user can "leak" to the visited network or AAA brokers in a number of ways:

- o The user's device may employ a fixed MAC address, or base its IP address on such an address. This enables the correlation of the particular device to its different locations. Techniques exist to avoid the use of an IP address that is based on MAC address [21]. Some link layers make it possible to avoid MAC addresses or change them dynamically.

- o Network access authentication procedures such as PPP CHAP [22] or EAP [23] may reveal the user's identity as a part of the authentication procedure. Techniques exist to avoid this problem in EAP, for instance by employing private Network Access Identifiers (NAIs) in the EAP Identity Response message [24] and by method-specific private identity exchange in the EAP method (e.g., [24], [25], [26]). Support for identity privacy within

CHAP is not available.

- AAA protocols may return information from the home network to the visited in a manner that makes it possible to either identify the user or at least correlate his session with other sessions, such as the use of static data in a Class attribute [2] or in some accounting attribute usage scenarios [27].

- Mobility mechanisms may reveal some permanent identifier (such as a home address) in cleartext in the packets relating to mobility signaling.

- Application protocols may reveal other permanent identifiers.

Note that to prevent the correlation of identities with location information it is necessary to prevent leakage of identity information from all sources, not just one.

Unfortunately, most users are not educated about the importance of identity confidentiality and there is a lack of support for it in many protocols. This problem is made worse by the fact that the users may be unable to choose particular protocols, as the choice is often dictated by the type of network they wish to access, the kind of equipment they have, or the type of authentication method they are using.

A scenario where the user is attached to the home network is, from a privacy point of view, simpler than a scenario where a user roams into a visited network since the NAS and the home AAA are in the same administrative domain. No direct relationship between the visited and the home network operator may be available and some AAA brokers need to be consulted. With subscription-based network access as used today the user has a contractual relationship with the home network provider which could allow higher privacy considerations to be applied (including policy rules stored at the home network itself for the purpose of restricting further distribution).

In many cases it is necessary to secure the transport of location information along the RADIUS infrastructure. Mechanisms to achieve this functionality are discussed in Section 10.

10. Security Considerations

Requirements for the protection of a Location Object are defined in [10]: Mutual end-point authentication, data object integrity, data object confidentiality and replay protection. The distribution of location information can be restricted with the help of authorization policies. Basic authorization policies are attached to the location information itself, in the same fashion as described in [16]. It is possible that the user was already able to transfer some authorization policies to the access network to restrict the distribution of location information. This is, however, rather unlikely in case of roaming users. Hence, it will be primarily the NAS creating the Location Object which also sets the authorization policies. If no authorization information is provided by the user then the visited network MUST set the authorization policies to only allow the home AAA server to use the provided location information. Other entities, such as the visited network and possibly AAA brokers MUST NOT use the location information for a purpose other than described in this document. More extensible authorization policies can be stored at the user's home network. These policies are useful when location information is distributed to other entities in a location-based service. This scenario is, however, outside the scope of this document.

It is necessary to use authorization policies to limit the unauthorized distribution of location information. The security requirements which are created based on [10] are inline with threats which appear in the relationship with disclosure of location information as described in [28]. PIDF-LO [16] proposes S/MIME to protect the Location Object against modifications. S/SIME relies on public key cryptography which raises performance, deployment and size considerations. Encryption would require that the local AAA server or the NAS knows the recipient's public key (e.g., the public key of the home AAA server). Knowing the final recipient of the location information is in many cases difficult for RADIUS entities. Some sort of public key infrastructure would be required to obtain the public key 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, computationally expensive.

If no authentication, integrity and replay protection between the participating RADIUS entities is provided then an adversaries can spoof and modify transmitted attributes. Two security mechanisms are proposed for RADIUS:

- o [2] proposes the usage of a static key which might raise some concerns about the lack dynamic key management.

o RADIUS over IPsec [29] allows to run standard key management mechanisms, such as KINK, IKE and IKEv2 [30], 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 from being successful. This is another requirement raised in the area of key transport with RADIUS and does not represent a deployment obstacle. The performance advantages 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 (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 [29]. Where an untrusted AAA intermediary is present, the Location Object MUST NOT be provided to the intermediary.

In case that IPsec protection is not available for some reason and RADIUS specific security mechanisms have to be used then the following considerations apply. The Access-Request message is not integrity protected. This would allow an adversary to change the contents of the Location Object or to insert and modify attributes and fields or to delete attributes. To address these problems the Message-Authenticator (80) can be used to integrity protect the entire Access-Request packet. The Message-Authenticator (80) is also required when EAP is used and hence is supported by many modern RADIUS servers.

Access-Request packets including Location attribute(s) without a Message-Authenticator(80) attribute SHOULD be silently discarded by the RADIUS server. A RADIUS server supporting the Location attributes MUST calculate the correct value of the Message-Authenticator(80) and MUST silently discard the packet if it does not match the value sent.

Access-Accept, including Location attribute(s) without a Message-Authenticator(80) attribute SHOULD be silently discarded by the NAS. A NAS supporting the Location attribute MUST calculate the correct value of a received Message-Authenticator(80) and MUST silently discard the packet if it does not match the value sent.

RADIUS and Diameter make some assumptions about the trust between traversed AAA entities in sense that object level security is not

provided by neither RADIUS nor Diameter. Hence, some trust has to be placed on the AAA entities to behave according to the defined rules. Furthermore, the AAA protocols do not involve the user in their protocol interaction except for tunneling authentication information (such as EAP messages) through their infrastructure. RADIUS and Diameter have even become a de-facto protocol for key distribution. Hence, in the past there were some concerns about the trust placed into the infrastructure particularly from the security area when it comes to keying. The EAP keying infrastructure is described in [23].

11. IANA Considerations

The authors request that the Attribute Types, and Attribute Values defined in this document be registered by the Internet Assigned Numbers Authority (IANA) from the RADIUS name spaces as described in the "IANA Considerations" section of RFC 3575 [8], in accordance with BCP 26 [9]. Additionally, the Attribute Type should be registered in the Diameter name space.

This document defines the following attributes:

Operator-Name
Location-Information
Basic-Policy-Rules
Extended-Policy-Rules
Challenge-Capable
Requested-Info

Please refer to Section 6 for the registered list of numbers.

This document also instructs IANA to assign a new value for the Error-Cause attribute [5], of "Location-Info-Required" TBA.

Additionally, IANA is requested to create the following new registries:

11.1. New Registry: Operator Type

This document also defines an operator namespace registry (used in the Namespace field of the Operator-Name attribute). IANA is requested to add the following values to this registry using their identifier and operator-namespace / associated registry owners for the operator namespace pairs:

Identifier	Operator-Namespace / Registry Owner
0	GSM - GSM Association/TADIG WG
1	CDMA - IMSI Oversight Council
2	REALM - IANA or delegate
3	ITU - ITU-T/TSB

Following the policies outline in [9] new values to the Operator-Namespaces will be assigned after Expert Review by the Geopriv working group or its designated successor. Updates can be provided based on expert approval only. No mechanism to mark entries as "deprecated" is envisioned. Based on expert approval it is possible

to delete entries from the registry.

11.2. New Registry: Requested-Info attribute

This document creates a new IANA registry for the Requested-Info attribute. IANA is requested to add the following four values to this registry:

Value	Capability Token
1	CIVIC_LOCATION
2	GEO_LOCATION
4	USERS_LOCATION
8	NAS_LOCATION

The semantic of these values is defined in Section 5.8.

Following the policies outline in [8] new Value/Capability Tokens with a description about their sematnic for usage with the Requested-Info attribute will be assigned after Expert Review by the RADEXT working group or its designated successor. Updates can be provided based on expert approval only. A designated expert will be appointed by the O&M Area Directors. No mechanism to mark entries as "deprecated is envisioned. Based on expert approval it is possible to delete entries from the registry.

Each registration must include:

Name:

Capability Token (i.e., an identifier of the capability)

Description:

Brief description indicating the meaning of the info element.

Numerical Value:

A numerical value that is placed into the Capability attribute representing a bit in the bit-string of the Requested-Info attribute.

12. Acknowledgments

The authors would like to thank the following people for their help with a previous version of this draft and for their input:

Chuck Black

Paul Congdon

Jouni Korhonen

Sami Ala-luukko

Farooq Bari

Ed Van Horne

Mark Grayson

Jukka Tuomi

Jorge Cuellar

Christian Guenther

Henning Schulzrinne provided the civic location information content found in this draft. The geospatial location information format is based on work done by J. Polk, J. Schnizlein and M. Linsner. The authorization policy format is based on the work done by Jon Peterson.

The authors would like to thank Victor Lortz, Jose Puthenkulam, Bernrad Aboba, Jari Arkko, Parviz Yegani, Serge Manning, Kuntal Chowdury, Pasi Eronen, Blair Bullock and Eugene Chang for their feedback to an initial version of this draft. We would like to thank Jari Arkko for his text contributions. Lionel Morand provided detailed feedback on numerous issues. His comments helped to improve the quality of this document. Jouni Korhonen and John Loughney helped us with the Diameter RADIUS interoperability. Andreas Pashalidis reviewed the final document and provided a number of comments. Bernard Aboba, Alan DeKok, Lionel Morand, Jouni Korhonen, David Nelson and Emile van Bergen provided guidance on the Requested-Info attribute and participated in the capability exchange discussions.

This document is based on the discussions within the IETF GEOPRIV working group. Therefore, the authors thank Henning Schulzrinne, James Polk, John Morris, Allison Mankin, Randall Gellens, Andrew

Newton, Ted Hardie, Jon Peterson for their time to discuss a number of issues with us. We thank Stephen Hayes for aligning this work with 3GPP activities.

The RADEXT working group chairs, David Nelson and Bernard Aboba, provided several draft reviews and we would like to thank them for the help and their patience.

13. References

13.1. Normative References

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

[2] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[3] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[4] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", draft-ietf-geopriv-dhcp-civil-09 (work in progress), January 2006.

[5] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[6] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

[7] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[8] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.

[9] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

13.2. Informative References

[10] Cuellar, J., Morris, J., Mulligan, D., Peterson, D., and D. Polk, "Geopriv Requirements", RFC 3693, February 2004.

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

[12] Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance", draft-ietf-sip-location-conveyance-02 (work in progress), March 2006.

[13] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[14] Schulzrinne, H., "Common Policy: An XML Document Format for Expressing Privacy Preferences", draft-ietf-geopriv-common-policy-10 (work in progress), May 2006.

[15] Schulzrinne, H., "A Document Format for Expressing Privacy Preferences for Location Information", draft-ietf-geopriv-policy-08 (work in progress), February 2006.

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

[17] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[18] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[19] "Open Geography Markup Language (GML) Implementation Specification", OGC 02-023r4, http://www.opengis.org/techno/implementation.htm", , January 2003.

[20] Stanley, D., Walker, J., and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", RFC 4017, March 2005.

[21] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[22] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[23] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[24] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

[25] Josefsson, S., Palekar, A., Simon, D., and G. Zorn, "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-10 (work in progress), October 2004.

[26] Tschofenig, H., "EAP IKEv2 Method", draft-tschofenig-eap-ikev2-11 (work in progress), June 2006.

[27] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

[28] Danley, M., "Threat Analysis of the Geopriv Protocol", RFC 3694, September 2003.

[29] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[30] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

Authors' Addresses

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

Email: Hannes.Tschofenig@siemens.com

Farid Adrangi
Intel Corporatation
2111 N.E. 25th Avenue
Hillsboro OR
USA

Email: farid.adrangi@intel.com

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

Email: mark.jones@bridgewatersystems.com

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
CANADA

Email: avi@bridgewatersystems.com

Acknowledgment

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