Geopriv H. Tschofenig
Internet-Draft Siemens
Expires: April 21, 2005 F. Adrangi
Intel
A. Lior
M. Jones
Bridgewater
October 21, 2004

Carrying Location Objects in RADIUS
draft-ietf-geopriv-radius-lo-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes RADIUS attributes for conveying the Access Network's operational ownership and location information based on a civil and geospatial location format.

The distribution of location information is privacy sensitive. 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 (AN) are being deployed in public places such as airports, hotels, shopping malls, and coffee shops by a diverse set of operators such as cellular carriers (GSM and CDMA), Wireless Internet Service Providers (WISP), and fixed broadband operators.

When a user executes the network access authentication procedure to such a network, information about the location and operational ownership of this network needs to be conveyed to the user's home network to which the user has a contractal 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 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. This document defines attributes for RADIUS [1].

Although the proposed attributes in this draft are intended for wireless LAN deployments, they can also be used in other wireless and wired networks where location-aware services are required.

Location information needs to be protected against unauthorized access and distribution to preserve the user's privacy with regard to location information. With [8] requirements for a protocol-independent model for the access to geographic location information was defined. 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 of a target.

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 [2].

RADIUS specific terminology is reused from [1] and [3].

Terminology related to privacy issues, location information and authorization policy rules are taken from [8].

3. Delivery Methods for Location Information

Location Objects, which consist of location information and privacy rules, are transported over the RADIUS protocol from visited access network to the home AAA server. To embedd a Location Object into RADIUS a number of AVPs are used, such as Location-Information AVP, Basic-Policy-Rules AVP, Extended-Policy-Rules AVP, Location-Type AVP and Operator-Name AVP. These AVPs 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 flow 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 authentication and/or authorization procedure is completed based on a number of criteria, including the newly defined Location-Information, Operator-Name, Location-Type, Policy-Information attributes. A RADIUS Accounting Request message is also allowed to carry location specific attributes.

```
    +---------+            +---------+                  +---------+
    | Access  |            | Network |                  |   AAA   |
    | Network |            | Access  |                  |  Server |
    | Client  |            | Server  |                  |         |
    +---------+            +---------+                  +---------+
        |                       |                              |
        | Authentication phase  |                              |
        | begin                 |                              |
        |---------------------->|                              |
        |                       |                              |
        |                       |                              |
        |                       | RADIUS                       |
        |                       | Access-Request               |
        |                       | + Location-Information       |
        |                       |   attributes                 |
        |                       |----------------------------->|
        |                       |                              |
        :                       :                              :
        :       Multiple Protocol Exchanges to perform         :
        :    Authentication, Key Exchange and Authorization    :
        :                  ...continued...                     :
```

```
        :                        :                              :
        |                        | RADIUS                       |
        |                        | Access-Accept                |
        |                        |  + Rule set Information      |
        |                        |<-----------------------------|
        | Authentication         |                              |
        | Accept                 |                              |
        |<-----------------------|                              |
        |                        |                              |
        |                        | RADIUS                       |
        |                        | Accounting Request           |
        |                        | + Location-Information       |
        |                        |   attributes                 |
        |                        |----------------------------->|
        |                        |                              |
```

Figure 1: Message Flow: Authentication/Authorization Phase Delivery

3.2 Mid-session Delivery

Mid-session delivery method uses the Change of Authorization (COA) message as defined in [4]. At anytime during the session the AAA server may send the access network a COA message containing session identification attributes. The COA message may instruct the access network to generate an Authorize-Only Access-Request (Access-Request with Service-Type set to "Authorize-Only") in which case it is instructing the access network to send the location information attributes.

Figure 2 shows the approach graphically.

```
            Access network                                    AAA server
                 |                                                |
                 |  COA  + Service-Type "Authorize Only"          |
                 |<-----------------------------------------------|
                 |                                                |
                 |  COA NAK + Service-Type "Authorize Only"       |
                 |          + Error-Cause  "Request Initiated"    |
                 |----------------------------------------------->|
                 |                                                |
                 | Access-Request + Service-Type "Authorize Only"|
                 |              + Location Information attributes |
                 |              + Location Information policy     |
                 |----------------------------------------------->|
                 |                                                |
                 | Access-Accept                                  |
                 |<-----------------------------------------------|
                 |                                                |
```

Figure 2: Message Flow: Mid-session Delivery

Upon receiving the Authorize-Only message from the access network, the AAA server MUST respond with either an Access-Accept message or an Access-Reject message.

4. Scenarios

In the following subsections we describe two scenarios for use of location information. The location infomration may refer to network or user location information which in some cases may be identical. How the network obtains the user's location information is out of scope of this document. There are two consumers of the location information: the AAA servers and other location-based services. The privacy implications of these scenarios are described in Section 14.

4.1 Scenario 1 - Use of Location Information in AAA

The home network operator requires location informaion 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 user's location is transferred from the NAS to the RADIUS server. The NAS and intermediaries (if any) are not allowed to use that information other then to forward it to the home network.

The RADIUS server authenticates and authorizes the session. 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). In the absence of receiving the policies intermediaries MUST NOT divulge the location information.

Location Information may also be reported in accouning 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 a rates applied based on the location and there may be different tax rates applied based on the location. Unless otherwise specified by authorization rules, location information in the accounting stream may 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 RADIUS server

roles. The RADIUS servers are in the home network, in the visited network, or in broker networks.

The Location Server MUST NOT transmit location information to parties other than members of the proxy chain from the NAS to 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.

Note that the NAS is the source of all location information that is disseminated by RADIUS, the NAS could tag the location information with the policy rules or a reference for the policy rules received in an Access-Accept. All location information in the accounting stream will now be tagged.

5. Overview

Location information and ownership of the access network is conveyed in the following RADIUS attributes: Operator-Name, Location-Information and Location-Type. Furthermore, the Basic-Policy-Rules and the Extended-Policy-Rules attributes are attached to the Location-Information attribute turning location information into a Location Object as defined in [8].

5.1 Operator-Name Attribute

This attribute contains an operator name which uniquely identifies the ownership of an access network. The attribute value is a non-NULL terminated string whose Length MUST NOT exceed 253 bytes. The attribute value is comprised of a prefix and an identity, separated by a colon. The prefix identifies the operator type; example: GSM, CDMA, and REALM. The identity uniquely identifies the operator name within the scope of the operator type.

As an example consider the string 'GSM:TADIG' where GSM is a prefix indicating an operator type and TADIC is a unique globally known GSM operator ID.

This document defines three operator type prefixes which are: GSM, CDMA, and REALM. The GSM prefix can be used to indicate operator names based on GSMA TADIG codes. REALM can be used by any domain name acquired from IANA. Possible forthcoming operator types MUST be associated with an organization responsible for assigning/managing operator names.

5.2 Location-Information Attribute

This document describes two formats for conveying location information: civil and geospatial location information. Section 5.2.1 defines the civil location information format. Section 5.2.2 defines the geospatial location information format.

Additionally, the following fields provide more details about the transmitted location information.

The 'Precision' field provides information of the accuracy about the provided location information. Location information can refer to the Access Point, the user, the or the RADIUS server or the network itself. With large networks the location information of each of these entities might be different. The 'Precision' field allows to give a hint about the precision of the provided location information.

The 'Method' field describes the way that the location information was derived or discovered. Possible values for this field

include, as an example GPS or manual configuration. The inclusion of this field should help the user's home network deduce further information about the accuracy and to provide an easier translation into a Location Object for transmission to third party entities (e.g., using SIP). Note that the values for this field are reused from [9].

5.2.1 Civil Location Information

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.

For this document, we reuse the civil location format defined in [5].

The civil location format includes a number of fields, including the country (expressed as a two-letter ISO 3166 code) and the administrative units A1 through A6 of [5] . This designation offers street-level precision.

For completeness we include more detailed information from [5] with regard to the defined civil location elements:

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

A5	neighborhood, block	Morningside Heights
A6	street	Broadway
PRD	Leading street 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

More description of these civil location elements can be found in Section 3.4 of [5]. These elements can be used to express further information about the location, language specific settings via the 'language' item and encoding information via the 'script' item. Section 13 shows usage examples of this attribute.

All attributes are optional and can appear in any order. The values are encoded using UTF-8 [6].

5.2.2 Geospatial Location Information

This document reuses geospatial location information from [7] which defines latitude, longitude, and altitude, with resolution indicators

for each. The value in the Altitude field either indicates meters or floors (via the Altitude Type field). As a coordinate reference system Section 2.1 of [7] defines (via extensible mechanism using IANA registration) three values in the Datum field: WGS 84, NAD 83 (with the associated vertical datum for the North American Vertical Datum of 1988), NAD 83 (with the associated vertical datum for the Mean Lower Low Water (MLLW). WGS 84 is used by the GPS system.

During a protocol run it is possible to return Location-Information attributes which provide both location information elements. If only one location information element is provided then civil location MUST be included in the request. Additionally, geospatial location MAY be provided.

6. Basic- and Extended-Policy-Rule Attributes

In some environments it is possible for the user to attach information about its privacy preferences. These preferences allow the visited network, intermediate RADIUS proxies and the home network to authorize the distribution of the user's location information.

Without the user providing authorization information two approaches are possible:

- o The user hides its location information from the access network and from intermediate networks using the appropriate network access authentication mechanism. Section 14 discusses these issues in more details.
- o The access network attaches default authorization policies which prevents intermediate networks and the home network to distribute the location information to other entities. Additionally, the home network might have authorization policies which control distribution of location information. Users can dynamically change their policies using the authroization framework defined in [10] and [11].

With regard to authorization policies this document reuses work done in [9] 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 [8], Section 2.7. Two RADIUS attributes are used for this purpose: Basic-Policy-Rule and Extended-Policy-Rule attribute. 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.

7. Location-Type Attribute

This document defines a separate attribute for the type of the location. Instead of the values of the 'type-of-place' attribute defined in Section 4.6 of [12] which is reused by [5] we define our own list of values for the Location-Type attribute. The reason for this is given by the size constraints of the attribute, dependence to other documents and to the location names required for the RADIUS context. Consequently, CA type '25' which equals the placetype is not used in the Location-Information attribute as described in Section 5.2.

```
     0 Reserved
     1 Coffee Shop
     2 Hotel
     3 Airport
     4 Mall
     5 Restaurant
     6 Bus
     7 Library
     8 Convention Center
     9 School
    10 Office
    11 Airplane
    12 Train
    13 Ship
    14 Educational Institute
    15 Public Place
    16 Other
```

Using these attribute types it is possible to describe the area in more detail.

8. Diameter RADIUS Interoperability

In deployments where RADIUS clients talk with DIAMETER servers or DIAMETER clients talk with RADIUS servers then a translation agent will be deployed and operate in accordance to the NASREQ specification [13].

9. Attributes

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

9.1 Operator-Name Attribute

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        | Operator-Name                ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:
  To Be Assigned by IANA - Operator-Name

Length:
  >= 3 Bytes

Operator-Name:
  The text field contains an Access Network Operator Name in prefix-based format.
  Example: REALM:anyisp.com

9.2 Location-Information Attribute

Location-Information 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 has two variations depending on civil or 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       | Code          |  Precision    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Sighting Time                                                 ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Sighting Time                                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Time-to-Live                                                  ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Time-to-Live                                                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Method      |    Location-Info                               ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type (8 bits):
  To Be Assigned by IANA - Location-Information

Length (8 bits):
  >= 3 Bytes

Code (8 bits):
  Describes which location format is carried in this attribute:
  (0) describes civil location information
  (1) describes geospatial location information
  All other bites of the Code field is reserved
  and required for alignment.

Precision (8 bits):
  Describes which location this attribute refers to:
  (0) describes the location of the NAS
  (1) describes the location of the AAA server
  (2) describes the location of the end host (user)
  (3) describes the location of the network

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 (8 bits):
  Describes the way that the location information was
  derived or discovered. The following values are currently
  defined:
  (0) Global Positioning System (GPS)

(1) GPS with assistance (A-GPS)
(2) Manual configured information
(3) Provided by DHCP
(4) Triangulation: triangulated from time-of-arrival, signal strength or similar measurements
(5) Cell: location of the cellular radio antenna
(6) IEEE 802.11 WLAN access point

Location-Info (variable):
Contains either civic or geospatial location information attributes.

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 [14].
time-to-live: This field gives a hint until when it should be considered current. Note that the time-to-live field is different than the 'retention-expires' rule. The data type of this field is a string and the format is a 64 bit NTP timestamp [14].

For civil location information the Location-Info field in the above structure is defined as followed:

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Countrycode          |  Civic address elements      ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Countrycode (16 bits):
Two-letter ISO 3166 country code in capital ASCII letters.

Civic address elements (variable):
The text field contains location information element.

The format of the civic address elements is described in Section 3.3 of [5] with a TLV pair (whereby the Type and Length fields are one-octet long). An example is given in Section 13.

For geospatial location information the Location-Info field is defined as follows:

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

```
|   LaRes   |     Latitude                                        +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Latitude      |    LoRes  |  Longitude                          +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Longitude                |  AT   |  AltRes   | Altitude  +
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Altitude                  |    Datum      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

LaRes (6 bits):
  Latitude resolution

Latitude (34 bits)

LoRes (6 bits):
  Longitude resolution.

Longitude (34 bits)

Altitude (30 bits)

AltRes (6 bits):
  Altitude resolution

AT (4 bits):
  Altitude Type for altitude. The following codes are defined:

  (1) Meters
  (2) Floors

Datum (8 bits):
  Coordinate reference system
  The following codes for the this field are defined:

  (1) WGS 84
  (2) NAD 83 (with the associated vertical datum for
             the North American Vertical Datum of 1988)
  (3) NAD 83 (with the associated vertical datum for
             the Mean Lower Low Water (MLLW))

The length of the Location-Information Attribute MUST NOT exceed 253 octets. The length of the geospatial location information format is fixed with 16 bytes plus a four byte header.

The Datum field contains an identifier for the coordinate system used to interpret the values of Latitude, Longitude and Altitude. The field with value (2) and the value (3) both represent the NAD 83 coordinate reference system but they differ from each other with

regard to their vertical datum representation as briefly noted in Section 5.2.2 and described in more detail in [7].

9.3 Basic Policy Rules Attribute

The Basic-Policy-Rules attribute MUST be sent in Access-Accept, Access-Challenge, Access-and Access-Reject messages 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.

A summary 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        |R|  Flags                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Retention Expires                                            ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Retention Expires                                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Note Well                                                    ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type :
  To Be Assigned by IANA - Basic-Policy-Rules

Length:
  > 3 Bytes

Flag (16 bits):
  Only the first bit (R) is defined an corresponds to the retransmission-allowed field. All other bits are reserved.

Retention Expires (64 bits):
  NTP timestamp for the 'retention-expires' field.

Note Well (variable):
  This field contains a URI with human readable privacy instructions.

This document reuses fields of the 'usage-rules' element, described in [9]. 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 [14].

note-well: This field contains a URI with 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.

9.4 Extended Policy Rules Attribute

The Extended-Policy-Rules attribute SHOULD be sent in Access-Accept, Access-Challenge, Access-and Access-Reject messages 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 [9] 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.

A summary 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        | Ruleset reference           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Type :
  To Be Assigned by IANA  - Extended-Policy-Rules

Length:
  > 3 Bytes

Ruleset reference:
  The text field contains a reference to the policy rules.
```

9.5 Location-Type Attribute

Location-Type 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.

A summary of the Location-Type 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        | Loc-Type                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type (8 bits):
  To Be Assigned by IANA - Location-Name

Length (8 bits):
  4 Bytes

Loc-Type (16 bits):
  The content of this field corresponds to the integer codes for access network location type.

These integer codes for the location type can be found in Section 7.

10. 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
0-1	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
0-1	0	0	0	0-1	TBD	Location-Type

The Location-Information attribute may appear more than once. This is useful if the size of one Location-Information attribute exceeds the maximum size of an AVP. This might happen in case of civil location information which has a variable number of fields. The fields used for the civil location information format of the Location-Information AVP (see Section 5.2.1 MUST NOT appear more than once.

11. IANA Considerations

This document requires the assignment of four new RADIUS attribute numbers for the following attributes:

Operator-Name
Location-Information
Basic-Policy-Rules
Extended-Policy-Rules
Location-Name

Please refer to Section 10 for the registered list of numbers.

12. Matching with Geopriv Requirements

This section compares the Geopriv requirements described in [8] 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 12.1 and Section 12.2 we discuss privacy implications when RADIUS is not used according to these usage scenario.

In Section 12.3 Geopriv requirements are matched against these two scenarios.

12.1 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 14: Location Server at the Home Network

The term 'Rule Holder' in Figure 14 denotes the entity which creates the authorization ruleset.

12.2 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 a few assumptions must hold:

- o The visited network deploys a Location Server and wants to distribute Location Objects of a user
- o The visited network is able to learn the user identity of the user

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 authorization policies of the user via RADIUS from the home AAA server.

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 15: Location Server at the Visited Network

12.3 Requirements matching

Section 7.1 of [8] 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. The same civil location information format is used in PIDF-LO and this document.
* Regarding requirement 1.2, some fields of the Location Object defined in this document are optional. See Section 5.2.1 as an example.
* Regarding requirement 1.3, the inclusion of the Location-Type attribute which gives a further classification of the location. This attribute can be seen as an extension.
* Regarding requirement 1.4, the Location Object is extensible in the same fashion as RADIUS 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 and the corresponding privacy rules are detailed in Section 9.3 and in Section 9.4.
* 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 9.3 and in Section 9.4).
* 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 14 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 users home network. The true user identity is protected by the authentication and key exchange protocol.
* Regarding requirement 2.2, the Location Recipient Identity is, in the main scenario the home AAA server. This entity is located using the structure of the Network Access Identifier. 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 15 describes these security mechanisms offered by the RADIUS protocol. The same is true for requirement 2.4.
* Regarding requirement 2.5, Section 5.2 describes the content of the Location Field. Motion and direction vectors as listed in requirement 2.6 are not provided as attributes. It is, however, possible to deduce the motion and direction of an entity via the Mid-session Delivery mechanism as shown in Figure 2.
* Regarding requirement 2.6, this document only describes one Location Data Type for civil 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 9.3.
* Regarding requirement 2.8, a reference to an external (more detailed ruleset) is provided with the Section 9.4 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 defines two Location Data Types as described in Section 5.2.
* With the support of civil and geospatial location information support requirement 3.2 is fulfilled.
* Regarding requirement 3.3, geospatial location information only supports absolute coordinates rather than a delta. 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 9.2).
* 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 5.2), extensions to existing fields (e.g., new location types as shown in Section 7) or via additional attributes.

Section 7.2 of [8] details the requirements of a "Using Protocol".

There are:

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 15 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 14) are also applicable for this discussion.

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 [8] details the requirements of a "Rule based Location Data Transfer".

There are:

Req. 7. (LS Rules): With the scenario shown in Figure 14 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 15 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 9.3, Section 9.4 and Section 14 for more details).

Req. 8. (LG Rules): It is possible for the non-initial transmission (i.e., mid-session delivery) of a Location Object to enforce the users privacy rules. 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 14 the visited network is already in possession of the users location information prior to the authentication and authorization of the user (which might require several roundtrips). A correlation between the location and the user identity might, however, still not be possible for the visited network (as explained in Section 14). 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 this area concerning the distribution of Location Objects. A basic ruleset is provided with the Basic-Policy-Rules attribute Section 9.3. A reference to the extended ruleset is carried in Section 9.4. The format of these rules are described

in [10] and [11].

Req. 11. (Limited Rule language): A limited (or basic) ruleset is provided by the Policy-Information attribute Section 9.3 (and as introduced with PIDF-LO [9]).

Section 7.4 of [8] details the requirements of a "Location Object Privacy and Security".

There are:

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 15. 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' [15]).

Req. 13. (Credential Requirements): As described in Section 15 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 15 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. Security for Location Objects 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). The handling of emergency calls is not specified as part of the RADIUS protocol and subject for an architectural investigation. As such it might not even be applicable to RADIUS itself.

13. Example

This section provides an example for a civil location information format within the Location-Information attribute. The size of the geo-spatial location information object is fixed and well-described examples can be found in the Appendix of [7].

Due to the size limitations of the RADIUS attributes we give a more detailed example borrowed from Section 4 of [5].

Type	Length	Value
Type	8 bits	TBD
Length	8 bits	43
Code	16 bits	1
Precision	8 bits	2
Countrycode	16 bits	DE
CAtype	8 bits	1
CAlength	8 bits	7
CAvalue	7 bytes	Bavaria
CAtype	8 bits	3
CAlength	8 bits	6
CAvalue	6 byte	Munich
CAtype	8 bits	6
CAlength	8 bits	11
CAvalue	11 bytes	Marienplatz
CAtype	8 bits	19
CAlength	8 bits	1
CAvalue	1 byte	8
CAtype	8 bits	24
CAlength	8 bits	5
CAvalue	5 bytes	80331

The Length element provides the length of the entire payload minus the length of the initial 'Type', the 'Length' and the 'Code' attribute. The Precision field has a value of '2' which refers to the location of the end host (user). The CountryCode is set to 'DE'. Note that the subsequent attributes are in Type-Length-Value format. Type '1' indicates the region of 'Bavaria', '3' refers to the city 'Munich', '6' to the street 'Marienplatz', the house number '8' is indicated by the type '19' and the zip code of '80331' is of type '24'.

The total sum of these attributes is 46 bytes.

14. 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, Figure 14 or in Figure 15:

14.1 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 other than the intended recipients (e.g., to third party entities) immediately.

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 se.
- 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).

14.2 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 to his home network and hence the trust relationship between them are higher. 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 [11] and in [10] are tailored for this environment. These policies might be useful for preventing 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.

- 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 or 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 network access authentication procedure is tightly coupled to the transfer of location information. If the authentication mechanism allows the visited network or AAA brokers to learn the user's identity 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.

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. Mechanism to achieve this functionality are discussed in Section 15.

One way to ensure that the visited network and intermediate networks are incapable to learn the user identity is to use EAP methods that hide the user's identity either actively or passively. Some EAP methods (such as [16]) protect the user's identity against passive adversaries by utilizing temporal identities. In some cases the visited network is still able to retrieve the plaintext identity of the user and user identity confidentiality is only provided against eavesdroppers at the wireless link. Depending on the movement patters of the user, the network topology and available roaming agreements it is possible that a AAA broker is able to see both the plaintext user identity and subsequent temporal identities. Associating location information and the user identity is possible in

these cases.

It is assumed that the true username is not carried within the initial EAP-Identity Request/Response message exchange. Support for username privacy is supported with [17].

For stronger security and privacy protection active user identity confidentiality is highly suggested. EAP methods such as [18] or [19] provide such a protection.

Unfortunately, most users are not educated about the importance of user identity confidentiality and many EAP methods do not provide active user identity confidentiality. User identity confidentiality is often treated as an exotic feature which mainly aims to prevent eavesdroppers on the wireless link to learn the user identity of the attached users. Awareness for this threat type does often not exist. In many cases it is even not possible for users to freely select their favorite authentication and key exchange protocol (based on their security requirements). Instead the choice is often predetermined by a given architecture.

It was noted that different granularity of location information can be provided to the home network. From a privacy point of view lower granularity is preferable. The user, however, has no control over the granularity and cannot lie about its location.

15. Security Considerations

Requirements for the security protection of a Location Object is defined in [8]: 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 [9]. 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 prevent the unauthorized distribution of location information. The security requirements which are created based on [8] are inline with threats which appear in the relationship with disclosure of location information as described in [20]. [9] 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 guarantee of freshness is necessary (for example, based on timestamps).

The security of S/SIME is based on public key cryptography which raises performance, deployment and size considerations. Encryption requires 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 fact impossible 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 AVPs. Two security mechanisms are proposed for RADIUS:

- [1] proposes the usage of a static key which might raise some concerns about the lack dynamic key management.
- RADIUS over IPsec [21] allows to run standard key management mechanisms, such as KINK [22], IKE and IKEv2 [23], 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 RAIDUS already no additional considerations need to be addressed beyond those described in [21]. 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. [24] documents this keying infrastructure and the security implications. The uniqueness of the AAA infrastructure therefore raises some concerns about the interpretation of the retention and redistribution restrictions. The privacy guidelines listed in Section 14 are applicable in this context.

16. 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
Jukkat Tuomi
Jorge Cuellar
Christian Guenther

Henning Schulzrinne provided the civil 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.

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 think Stephen Hayes for aligning this work with 3GPP activities.

17. References

17.1 Normative References

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

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

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

[4] 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.

[5] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", draft-ietf-geopriv-dhcp-civil-04 (work in progress), October 2004.

[6] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

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

17.2 Informative References

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

[9] Peterson, J., "A Presence-based GEOPRIV Location Object Format", draft-ietf-geopriv-pidf-lo-03 (work in progress), September 2004.

[10] Schulzrinne, H., "A Document Format for Expressing Privacy Preferences", draft-ietf-geopriv-common-policy-02 (work in progress), October 2004.

[11] Schulzrinne, H., "A Document Format for Expressing Privacy Preferences for Location Information", draft-ietf-geopriv-policy-03 (work in progress), October 2004.

[12] Schulzrinne, H., Gurbani, V., Kyzivat, P. and J. Rosenberg, "RPID: Rich Presence: Extensions to the Presence Information

Data Format (PIDF)", draft-ietf-simple-rpid-03 (work in progress), March 2004.

[13] Calhoun, P., Zorn, G., Spence, D. and D. Mitton, "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-17 (work in progress), July 2004.

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

[15] Stanley, D., Walker, J. and B. Aboba, "EAP Method Requirements for Wireless LANs", draft-walker-ieee802-req-04 (work in progress), August 2004.

[16] Arkko, J. and H. Haverinen, "EAP AKA Authentication", draft-arkko-pppext-eap-aka-12 (work in progress), April 2004.

[17] Aboba, B., "The Network Access Identifier", draft-arkko-roamops-rfc2486bis-02 (work in progress), July 2004.

[18] Josefsson, S., Palekar, A., Simon, D. and G. Zorn, "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-09 (work in progress), October 2004.

[19] Tschofenig, H. and D. Kroeselberg, "EAP IKEv2 Method (EAP-IKEv2)", draft-tschofenig-eap-ikev2-04 (work in progress), July 2004.

[20] Danley, M., "Threat Analysis of the Geopriv Protocol", RFC 3694, September 2003, <reference.RFC3694.xml>.

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

[22] Thomas, M. and J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)", draft-ietf-kink-kink-06 (work in progress), July 2004.

[23] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

[24] Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-03 (work in progress), July 2004.

[25] Adrangi, F., "Access Network Bandwidth Capability", draft-adrangi-radius-bandwidth-capability-01 (work in progress), July 2004.

Authors' Addresses

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

EMail: Hannes.Tschofenig@siemens.com

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

EMail: farid.adrangi@intel.com

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

EMail: avi@bridgewatersystems.com

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

EMail: mark.jones@bridgewatersystems.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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