GEOPRIV
Internet-Draft
Intended status: Standards Track
Expires: November 8, 2009

H. Tschofenig, Ed.
Nokia Siemens Networks
F. Adrangi
Intel
M. Jones
A. Lior
Bridgewater
B. Aboba
Microsoft Corporation

May 7, 2009

# Carrying Location Objects in RADIUS and Diameter
## draft-ietf-geopriv-radius-lo-24.txt

Abstract

This document describes procedures for conveying access network ownership and location information based on a civic and geospatial location format in Remote Authentication Dial In User Service (RADIUS) and Diameter.

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

This document defines attributes within RADIUS and Diameter that can be used to convey location-related information within authentication and accounting exchanges.

Location information may be useful in a number of scenarios. Wireless networks (including wireless LAN) 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, Wireless Internet Service Providers (WISPs), and fixed broadband operators. In these situations, the home network may need to know the location of the user, in order to enable location-aware billing, location-aware authorization, or other location-aware services. Location information can also prove useful in other situations (such as wired networks) where operator network ownership and location information may be needed by the home network.

In order to preserve user privacy, location information needs to be protected against unauthorized access and distribution. Requirements for access to location information are defined in [RFC3693]. 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. In Appendix A the requirements for a GEOPRIV Using Protocol are compared to the functionality provided by this document.

## 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 [RFC2119].

RADIUS specific terminology is borrowed from [RFC2865] and [RFC2866].

Terminology related to privacy issues, location information and authorization policy rules is taken from [RFC3693].

## 3. Delivery Methods for Location Information

The following exchanges show how location information is conveyed in RADIUS. In describing the usage scenarios, we assume that privacy policies allow location to be conveyed in RADIUS; however, as noted in Section 6 similar exchanges can also take place within Diameter. Privacy issues are discussed in Section 7.2.

### 3.1. Location Delivery based on Out-of-Band Agreements

Figure 1 shows an example message flow for delivering location information during the network access authentication and authorization procedure. Upon a network authentication request from an access network client, the Network Access Server (NAS) submits a RADIUS Access-Request message that contains location information attributes among other required attributes. In this scenario location information is attached to the Access-Request message without an explicit request from the RADIUS server. Note that such an approach with a prior agreement between the RADIUS client and the RADIUS server is only applicable in certain environments, such as in situations where the RADIUS client and server are within the same administrative domain. The Basic-Location-Policy-Rules Attribute is populated based on the defaults described in Section 4.4, unless it has been explicitly configured otherwise.

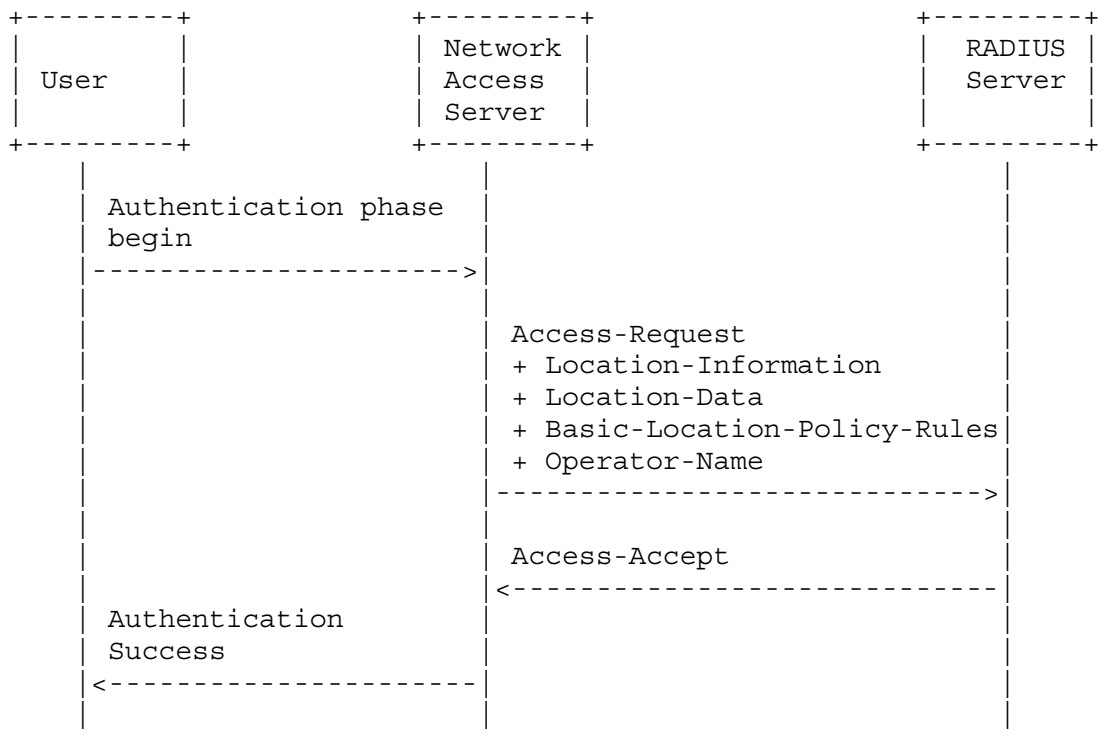



Figure 1: Location Delivery based on out-of-band Agreements

## 3.2. Location Delivery based on Initial Request

If the RADIUS client provides a Location-Capable Attribute in the Access-Request, then the RADIUS server MAY request the RADIUS client for location information if it requires that information for authorization, and location information was not provided in Access-Request. This exchange is shown in Figure 2. The inclusion of the Location-Capable Attribute in an Access-Request message indicates that the NAS is capable of providing location data in response to an Access-Challenge. The subsequent Access-Challenge message sent from the RADIUS server to the NAS provides a hint regarding the type of desired location information attributes. The NAS treats the Basic-Location-Policy-Rules and Extended-Location-Policy-Rules Attributes as opaque data (e.g., it echoes these rules provided by the server within the Access-Challenge back in the Access-Request). In the shown message flow the location attributes are then provided in the subsequent Access-Request message. When evaluating this Access-Request message the authorization procedure at the RADIUS server might be based on a number of criteria, including the newly defined attributes listed in Section 4.

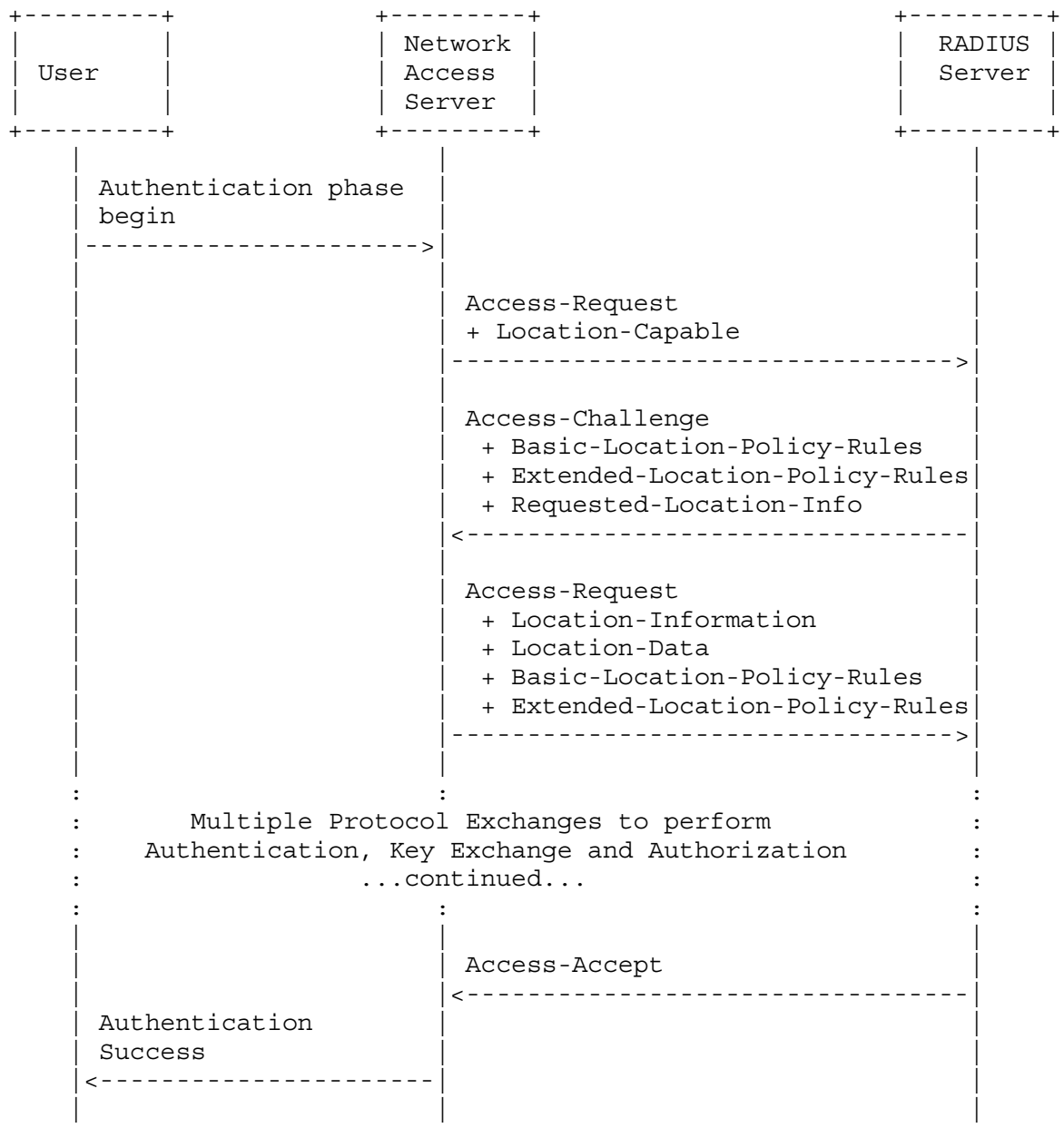



Figure 2: Location Delivery based on Initial Request

## 3.3. Location Delivery based on Mid-Session Request

The on-demand mid-session location delivery method utilizes the Change of Authorization Request (CoA-Request) message and the CoA-NAK, defined in [RFC5176]. At any time during the session the Dynamic Authorization Client MAY send a CoA-Request containing

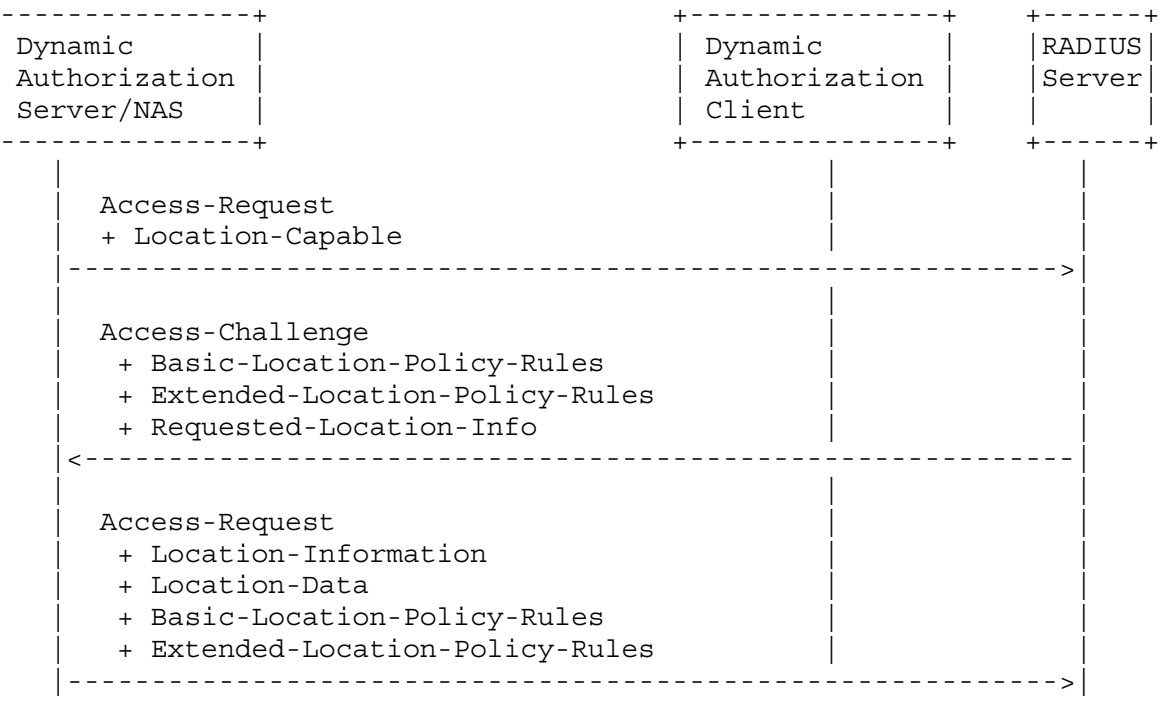
session identification attributes to the NAS (i.e., Dynamic Authorization Server).

In order to enable the on-demand mid-session location delivery method, the RADIUS server MUST return an instance of the Requested-Location-Info Attribute with the 'FUTURE_REQUESTS' flag set and instances of the Basic-Location-Policy-Rules and Extended-Location-Policy-Rules Attributes in the Access-Accept message for the session. Upon receipt of a CoA-Request message containing a Service-Type Attribute with value "Authorize Only" for the same session, the NAS MUST include location information and echo the previously received Basic-Location-Policy-Rules and Extended-Location-Policy-Rules Attributes in the subsequent Access-Request message.

Upon receiving the Access-Request message containing the Service-Type Attribute with a value of Authorize-Only from the NAS, the RADIUS server responds with either an Access-Accept or an Access-Reject message.

The use of dynamic authorization [RFC5176] is necessary when location information is needed on-demand and cannot be obtained from accounting information in a timely fashion.

Figure 3 shows the above-described approach graphically.



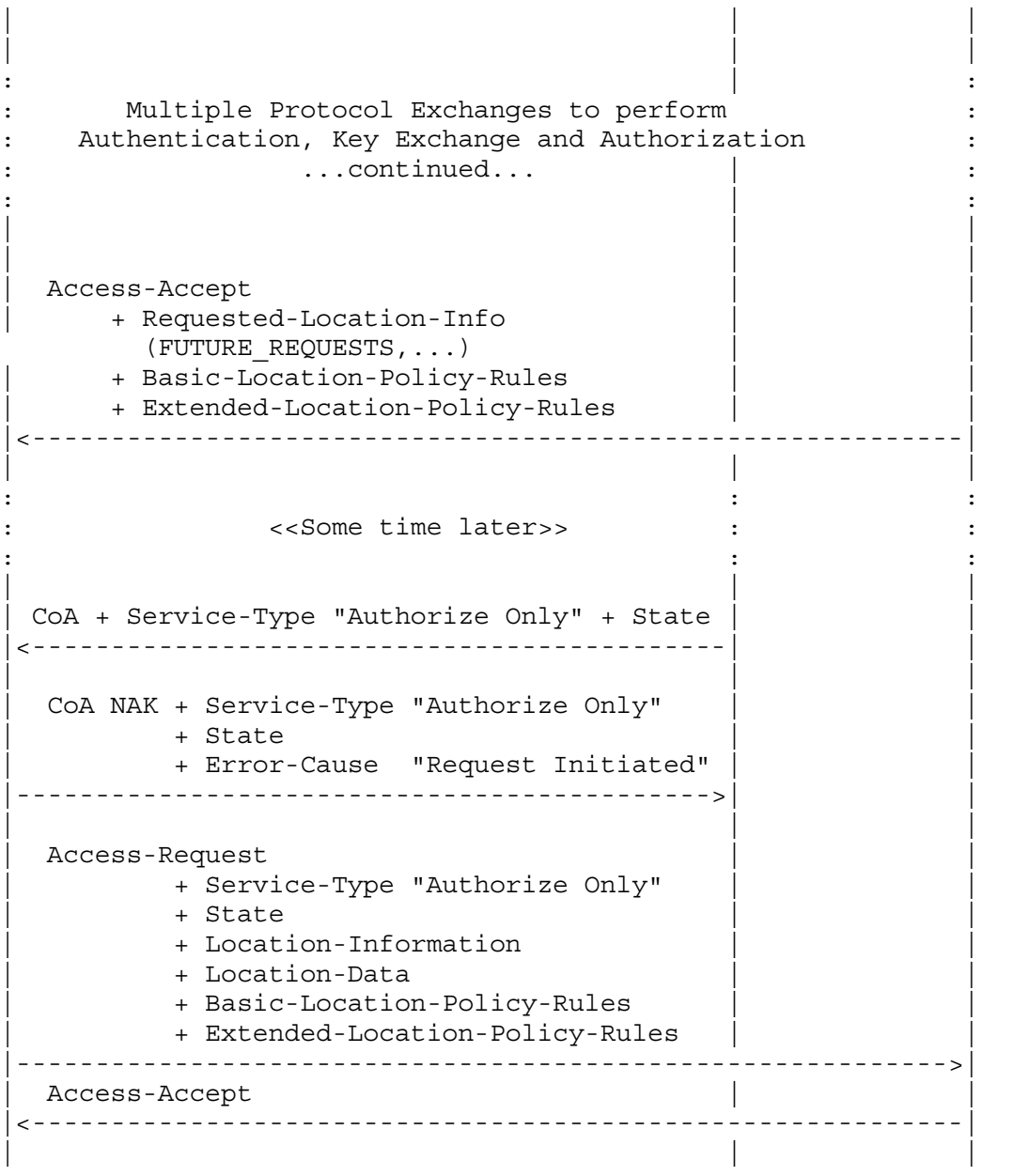
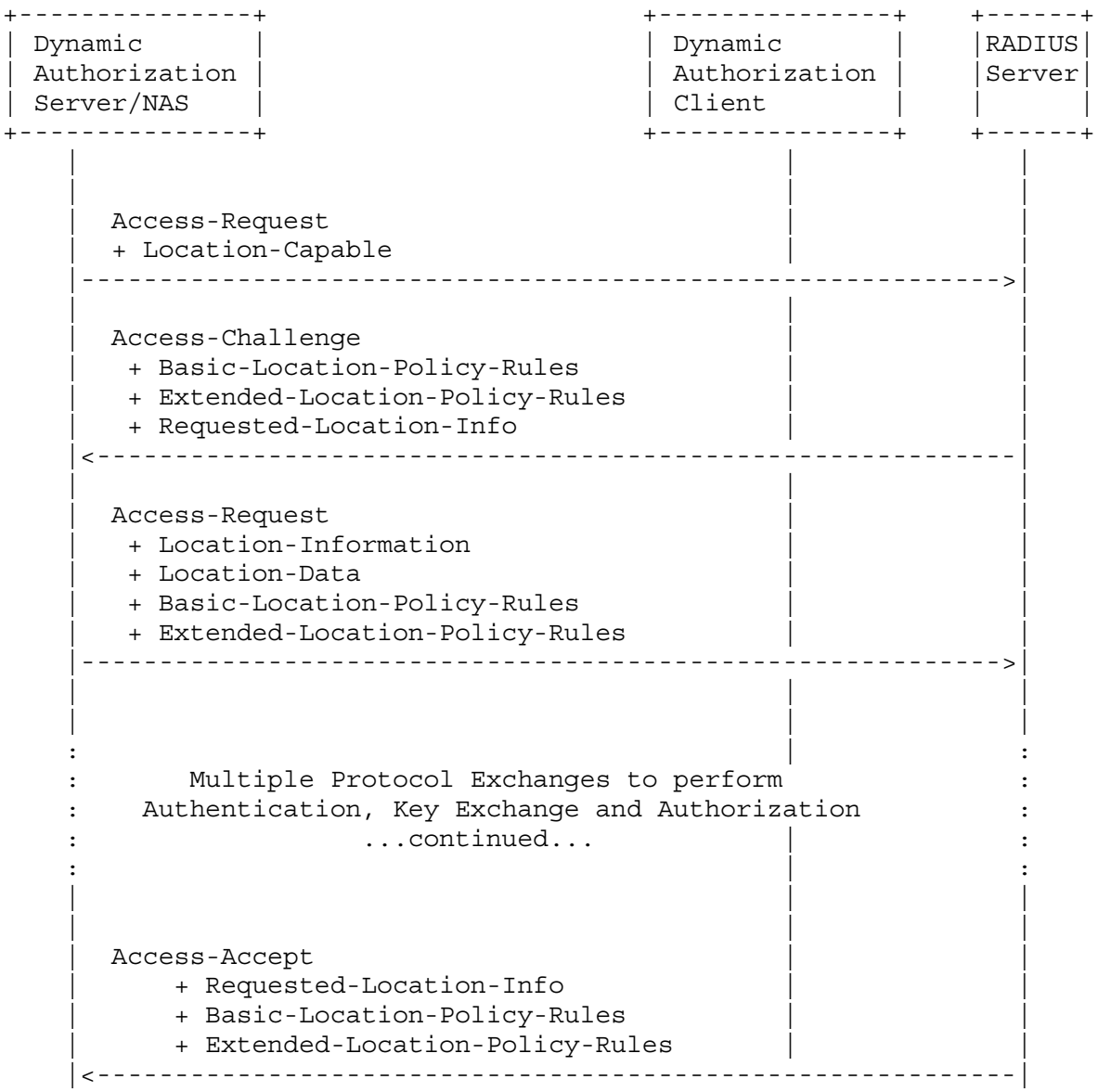



Figure 3: Location Delivery based on CoA with Service-Type 'Authorize Only'

When the Dynamic Authorization Client wants to change the values of the requested location information, or set the values of the requested location information for the first time, it may do so without triggering a reauthorization. Assuming that the NAS had previously sent an Access-Request containing a Location-Capable

Attribute, the DAC can send a CoA-Request to the NAS without a Service-Type Attribute, but including the NAS Identifiers and Session identifiers as per [RFC5176] and the Requested-Location-Info, Basic-Location-Policy-Rules and Extended-Location-Policy-Rules Attributes. The Requested-Location-Info, Basic-Location-Policy-Rules and Extended-Location-Policy-Rules Attributes MUST NOT be used for session identification.

Figure 4 shows this approach graphically.



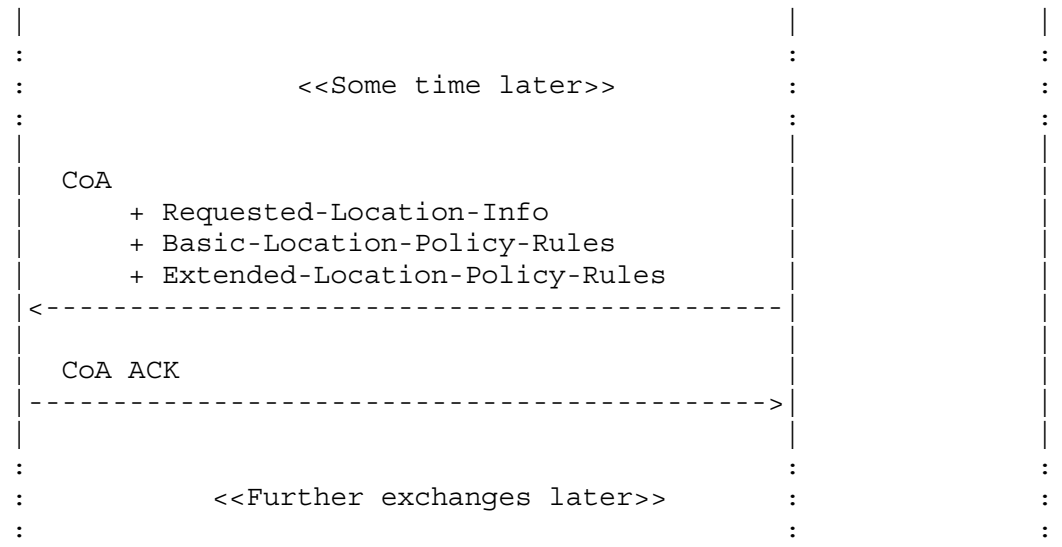



Figure 4: Location Delivery based on CoA

## 3.4. Location Delivery in Accounting Messages

Location Information may also be reported in accounting messages. Accounting messages are generated when the session starts, when the session stops and periodically during the lifetime of the session. Accounting messages may also be generated when the user roams during handoff.

Accounting 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.

If the RADIUS server needs to obtain location information in accounting messages then it needs to include a Requested-Location-Info Attribute to the Access-Accept message. The Basic-Location-Policy-Rules and the Extended-Location-Policy-Rules Attributes are to be echoed in the Accounting-Request if indicated in the Access-Accept.

Figure 5 shows the message exchange.

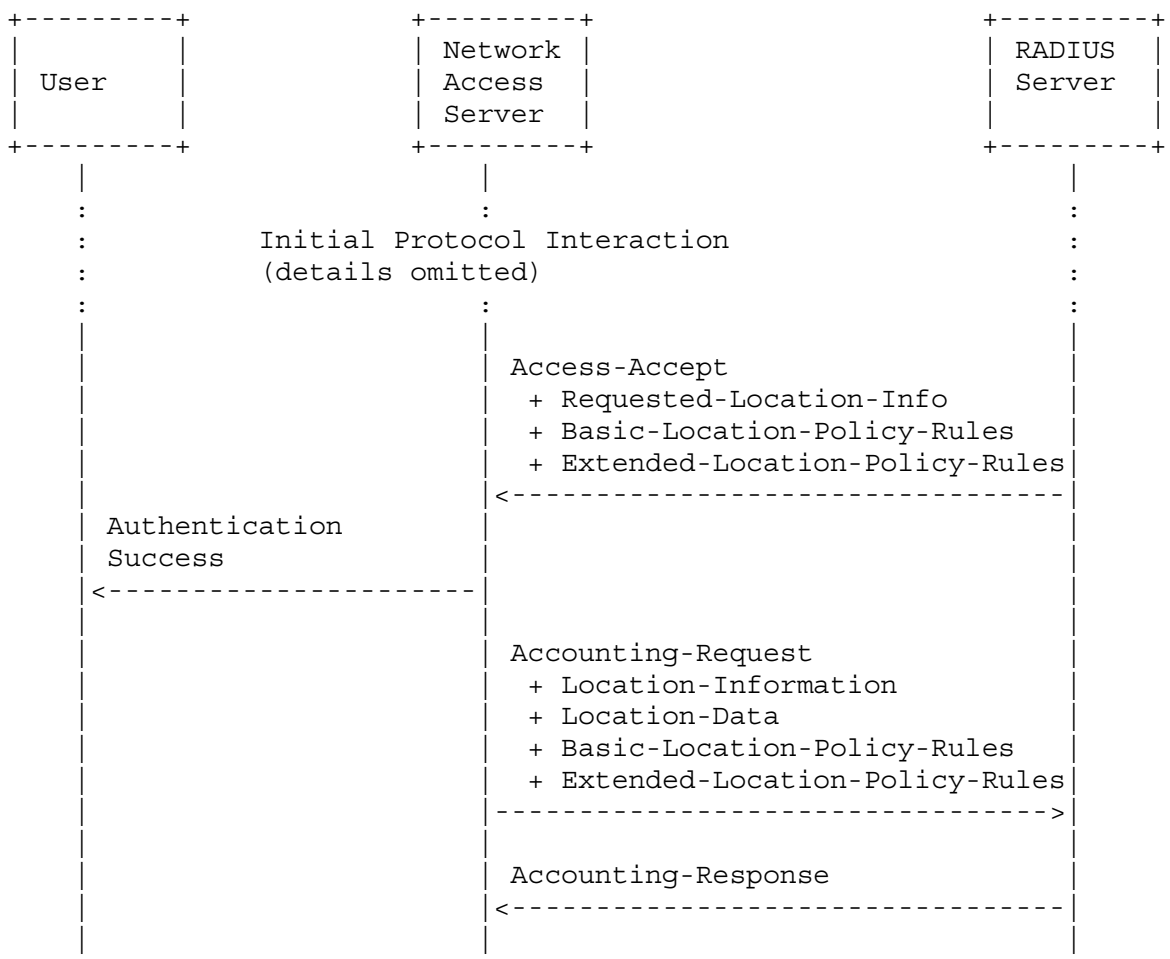



Figure 5: Location Delivery in Accounting Messages

# 4. Attributes

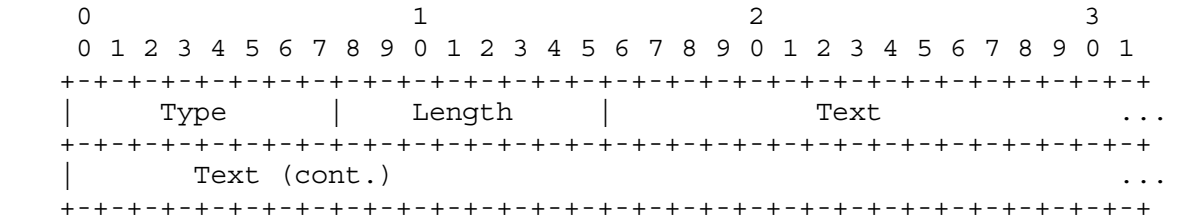
It is important to note that the location specific parts of the attributes defined below are not meant to be processed by the RADIUS server. Instead, a location server specific component used in combination with the RADIUS server is responsible for receiving, processing and further distributing location information (in combination with proper access control and privacy protection). As such, from a RADIUS server point of view location information is treated as opaque data.

## 4.1. Operator-Name Attribute

This attribute carries the operator namespace identifier and the operator name. The operator name is combined with the namespace identifier 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 Operator-Name Attribute SHOULD be sent in Access-Request, and Accounting-Request messages where the Acc-Status-Type is set to Start, Interim, or Stop.

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




Type:

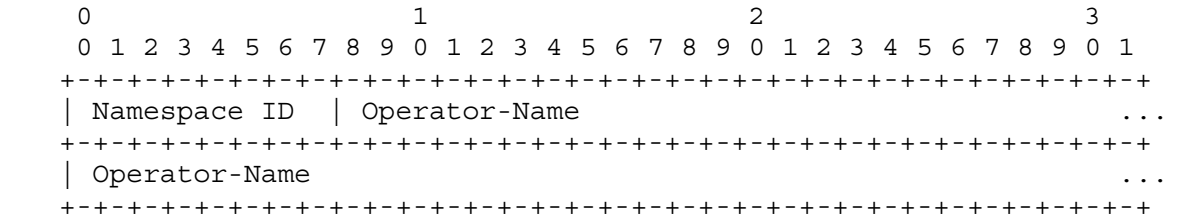
To Be Assigned by IANA - Operator-Name

Length:

>= 4

Text:

The format is shown below. The data type of this field is string. All fields are transmitted from left to right:




Namespace ID:

The value within this field contains the operator namespace identifier. The Namespace ID value is encoded in ASCII.

Example: '1' (0x31) 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.

The Namespace ID field provides information about the operator namespace. This document defines four values for this attribute that are listed below. Additional namespace identifiers must be registered with IANA (see Section 8.1) and must be associated with an organization responsible for managing the namespace.

TADIG ('0' (0x30)):

This namespace can be used to indicate operator names based on Transferred Account Data Interchange Group (TADIG) codes, as defined in [GSM]. TADIG codes are assigned by the TADIG Working Group within the GSM Association. The TADIG Code consists of two fields, with a total length of five ASCII characters consisting of a three-character country code and a two-character alphanumeric operator (or company) ID.

REALM ('1' (0x31)):

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). Since this operator is limited to ASCII, any registered domain name which contains non-ASCII characters must be converted to ASCII. The Punycode encoding [RFC3492] is used for this purpose.

E212 ('2' (0x32)):

The E212 namespace can be used to indicate operator names based on the Mobile Country Code (MCC) and Mobile Network Code (MNC) defined in [ITU212]. The MCC/MCC values are assigned by the Telecommunications Standardization Bureau (TSB) within the ITU-T and designated administrators in different countries. The E212 value consists of three ASCII digits containing the MCC, followed by two or three ASCII digits containing the MNC.

ICC ('3' (0x33)):

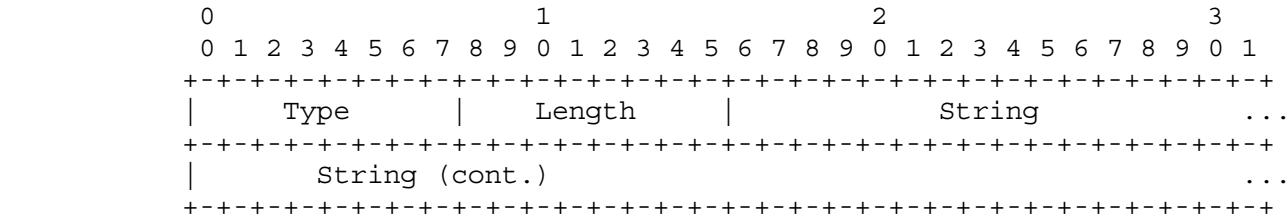
The ICC namespace can be used to indicate operator names based on International Telecommunication Union (ITU) Carrier Codes (ICC) defined in [ITU1400]. ICC values are assigned by national regulatory authorities and are coordinated by the Telecommunication Standardization Bureau (TSB) within the ITU Telecommunication Standardization Sector (ITU-T). When using the ICC namespace, the attribute consists of three uppercase ASCII characters containing a three-letter alphabetic country code, as defined in [ISO], followed by one to six uppercase alphanumeric ASCII characters containing the ICC itself.

### 4.2. Location-Information Attribute

The Location-Information Attribute MAY 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, location determination method, etc.

The format is shown below.




Type:

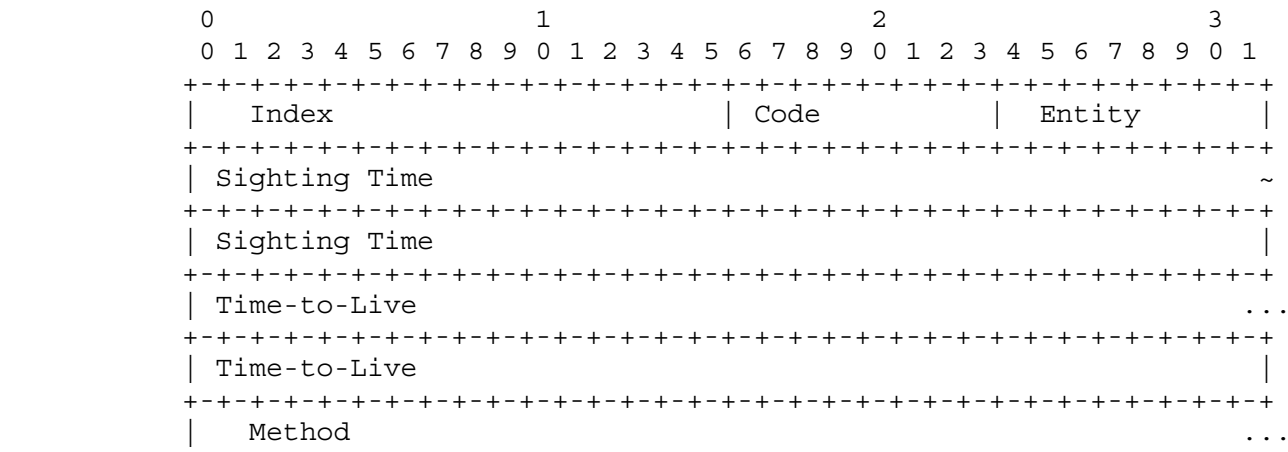
To Be Assigned by IANA - Location-Information

Length:

>= 23

String:

The format is shown below. The data type of this field is string. All fields are transmitted from left to right:



Index (16 bits):

The 16-bit unsigned integer value allows this attribute to provide information relating to the information included in the Location-Data Attribute to which it refers (via the Index).

Code (8 bits):

This field indicates the content of the location profile carried in the Location-Data Attribute. Two profiles are defined in this document, namely one civic location profile (see Section 4.3.1) that uses value (0) and a geospatial location profile (see Section 4.3.2) that uses the value (1).

Entity (8 bits):

This field encodes which location this attribute refers to as an unsigned 8-bit integer value. Location information can refer to different entities. This document registers two entity values, namely:

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

Value (1) describes the location of the RADIUS client

The registry used for these values is established by this document, see Section 8.4.

Sighting Time (64 bits)

This field indicates when the Location Information was accurate. The data type of this field is a string and and the content is expressed in the 64 bit Network Time Protocol (NTP) timestamp format [RFC1305].

Time-to-Live (64 bits):

This field gives a hint until when location information should be considered current. The data type of this field is a string and the content is expressed in the 64 bit Network Time Protocol (NTP) timestamp format [RFC1305]. Note that the time-to-live field is different than Retention Expires field used in the Basic-Location-Policy-Rules Attribute, see Section 4.4. Retention expires

indicates the time the recipient is no longer permitted to possess the location information.

Method (variable):

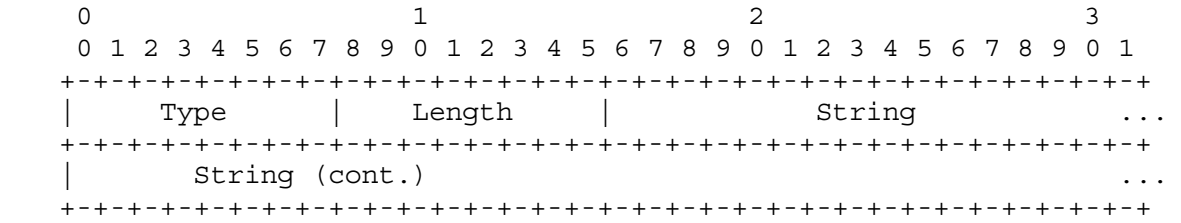
Describes the way that the location information was determined. This field MUST contain the value of exactly one IANA-registered 'method' token [RFC4119].

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

### 4.3. Location-Data Attribute

The Location-Data Attribute MAY 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 format is shown below.




Type:

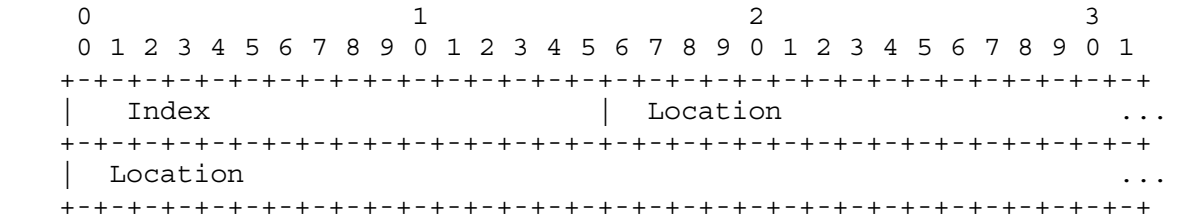
To Be Assigned by IANA - Location-Data

Length:

>= 5

String:

The format is shown below. The data type of this field is string. All fields are transmitted from left to right:




Index (16 bits):

The 16-bit unsigned integer value allows to associate the Location-Data Attribute with the Location-Information Attributes.

Location (variable):

The format of the location data depends on the location profile. This document defines two location profiles. Details of the location profiles is described below.

### 4.3.1. Civic Location Profile

Civic location is a popular way to describe the location of an entity. This section defines the civic location information profile corresponding to the value (0) indicated in the Code field of the Location-Information Attribute. The location format is based on the encoding format defined in Section 3.1 of [RFC4776] whereby the first

3 octets (i.e., the code for this DHCP option, the length of the DHCP option, and the 'what' element are not included) are not put into the Location field of the above-described RADIUS Location-Data Attribute.

#### 4.3.2. Geospatial Location Profile

This section defines the geospatial location information profile corresponding to the value (1) indicated in the Code field of the Location-Information Attribute. Geospatial location information is encoded as an opaque object whereby the format is reused from the Section 2 of RFC 3825 Location Configuration Information (LCI) format [RFC3825] starting with the third octet (i.e., the code for the DHCP option and the length field is not included).

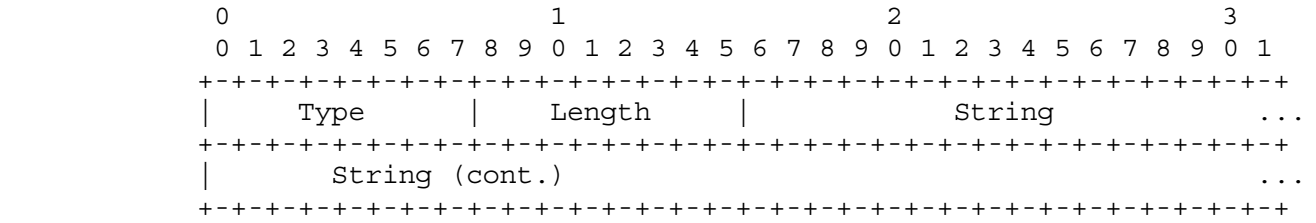
### 4.4. Basic-Location-Policy-Rules Attribute

The Basic-Location-Policy-Rules Attribute MAY be sent in an Access-Request, Access-Accept, an Access-Challenge, a Change-of-Authorization and in an Accounting-Request message.

Policy rules control the distribution of location information. The obligation with respect to understanding and processing of the Basic-Location-Policy-Rules Attribute for RADIUS clients is to utilize a default value of Basic-Location-Policy-Rules unless explicitly configured otherwise, and also for clients to echo the Basic-Location-Policy-Rules Attribute that they receive from a server. As a default, the note-well field does not carry a pointer to human readable privacy policies, the retransmission-allowed is set to zero (0), i.e., further distribution is not allowed, and the retention-expires field is set to 24 hours.

With regard to authorization policies this document reuses work done in [RFC4119] and encodes them in a 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 [RFC3693], Section 2.7.

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




Type:

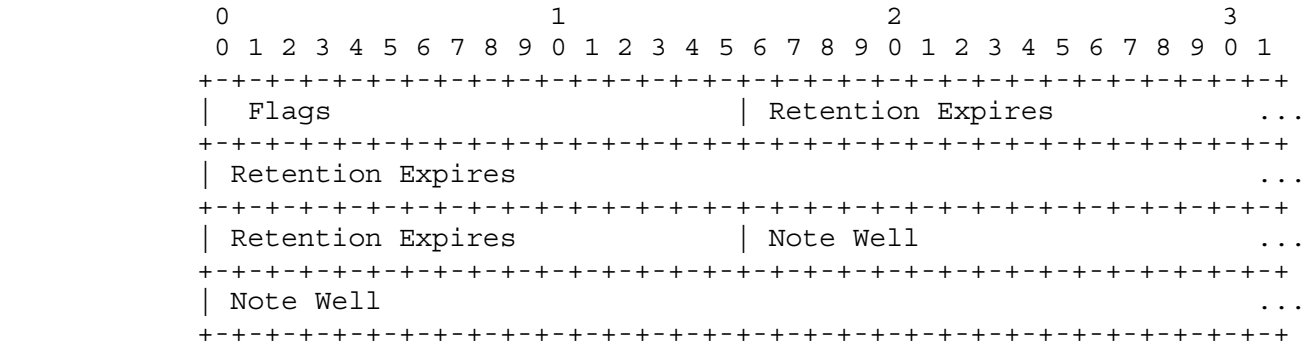
To Be Assigned by IANA - Basic-Location-Policy-Rules

Length:

>= 12

String:

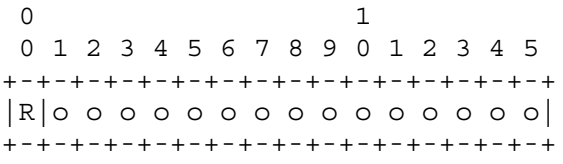
The format is shown below. The data type of this field is string. All fields are transmitted from left to right:




This document reuses fields of the RFC 4119 [RFC4119] 'usage-rules' element. These fields have the following meaning:

Flags (16 bits):

The Flags field is a bit mask and only the first bit (R) is defined in this document and corresponds to the retransmission-allowed field:




R = retransmission-allowed
o = reserved.

All reserved bits MUST be zero. When the value of this field the retransmission-allowed field is set to zero (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 (64 bits):

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 [RFC1305].

Note Well (variable):

This field contains a URI that points to human readable privacy instructions. The data type of this field is string. 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 RADIUS eco-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 into the 'note-well' element of the 'usage-rules' element contained in the PIDF-LO document (see [RFC4119]). The note-well field may be empty.

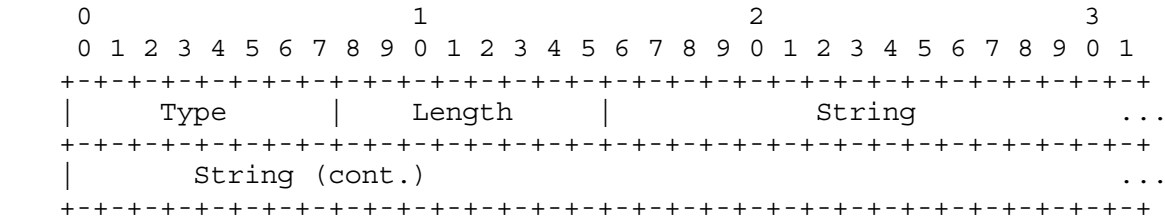
## 4.5. Extended-Location-Policy-Rules Attribute

The Extended-Location-Policy-Rules Attribute MAY be sent in an Access-Request, an Access-Accept, an Access-Challenge, an Access-Reject, an Change-of-Authorization and in an Accounting-Request message.

The ruleset reference field of this attribute is of variable length. It contains a URI that indicates where the richer ruleset can be found. This URI SHOULD use the HTTPS URI scheme. As a deviation from [RFC4119] this field only contains a reference and does not carry an attached extended rule set. This modification is motivated by the size limitations imposed by RADIUS.

Policy rules control the distribution of location information and, as with the Basic Policy Rules Attribute the obligation with respect to understanding and processing of the Extended-Location-Policy-Rules Attribute for RADIUS clients is when they are explicitly configured to attach the URI, and also for clients to echo the Extended-Location-Policy-Rules Attribute that they receive from a server. There is no expectation that RADIUS clients will need to retrieve data at the URL specified in the attribute and to parse the XML policies.

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




Type:

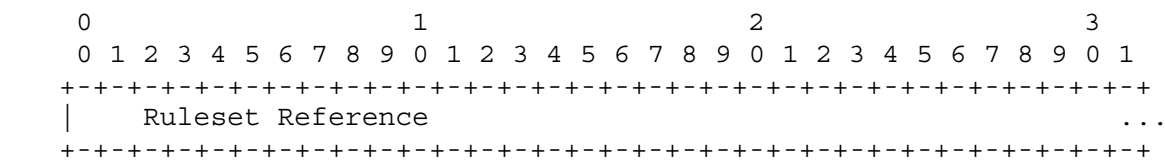
To Be Assigned by IANA - Extended-Location-Policy-Rules

Length:

>= 3

String:

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

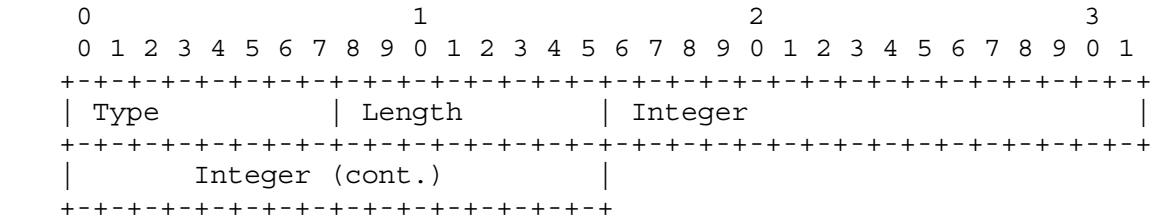



Ruleset Reference:

This field contains a URI that points to the policy rules.

## 4.6. Location-Capable Attribute

The Location-Capable Attribute allows a NAS (or client function of a proxy server) to indicate support for the functionality specified in this document. The Location-Capable Attribute with the value for 'Location Capable' MUST be sent with the Access-Request messages, if the NAS supports the functionality described in this document and is capable of sending location information. A RADIUS server MUST NOT challenge for location information unless the Location-Capable Attribute has been sent to it.




Type:

To Be Assigned by IANA - Location-Capable Attribute

Length:

6

Integer:

The content of the Integer field encodes the requested capabilities.
Each capability value represents a bit position.

This document specifies the following capabilities:

Name:

CIVIC_LOCATION

Description:

The RADIUS client uses the CIVIC_LOCATION to indicate that it is able to return civic location based on the location profile defined in Section 4.3.1.

Numerical Value:

A numerical value of this token is '1'.

Name:

GEO_LOCATION

Description:

The RADIUS client uses the GEO_LOCATION to indicate that it is able to return geodetic location based on the location profile defined in Section 4.3.2.

Numerical Value:

A numerical value of this token is '2'.

Name:

USERS_LOCATION

Description:

The numerical value representing USERS_LOCATION indicates that the RADIUS client is able to provide a Location-Information attribute with the Entity attribute expressing the value of zero (0), i.e., the RADIUS client is capable of returning location information of the user's client device.

Numerical Value:

A numerical value of this token is '4'.

Name:

NAS_LOCATION

Description:

The numerical value representing NAS_LOCATION indicates that the RADIUS client is able to provide a Location-Information attribute that contains location information with the Entity attribute expressing the value of one (1), i.e., the RADIUS client is capable of returning location information of the NAS.

Numerical Value:

A numerical value of this token is '8'.

### 4.7. Requested-Location-Info Attribute

The Requested-Location-Info Attribute allows the RADIUS server to indicate what location information about which entity it wants to receive. The latter aspect refers to the entities that are indicated in the Entity field of the Location-Information Attribute.

The Requested-Location-Info Attribute MAY be sent in an Access-Accept, in an Access-Challenge, or a Change of Authorization packet.

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 RADIUS client and the RADIUS server have agreed out-of-band to mandate the transfer of location information for every network access authentication request then the processing listed below is not applicable.

- If the RADIUS server requires location information for computing the authorization decision and the RADIUS client does not provide it with the Access-Request message then the Requested-Location-Info Attribute is attached to the Access-Challenge with a hint about what is required.

- If the RADIUS server does not receive the requested information in response to the Access-Challenge (including the Requested-Location-Info Attribute) then the RADIUS server may respond with an Access-Reject message with an Error-Cause Attribute (including the "Location-Info-Required" value).

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

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

Figure 6 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-Location-Info Attribute is attached to the Access-Challenge the RADIUS server indicates that location information is required for computing an authorization decision.

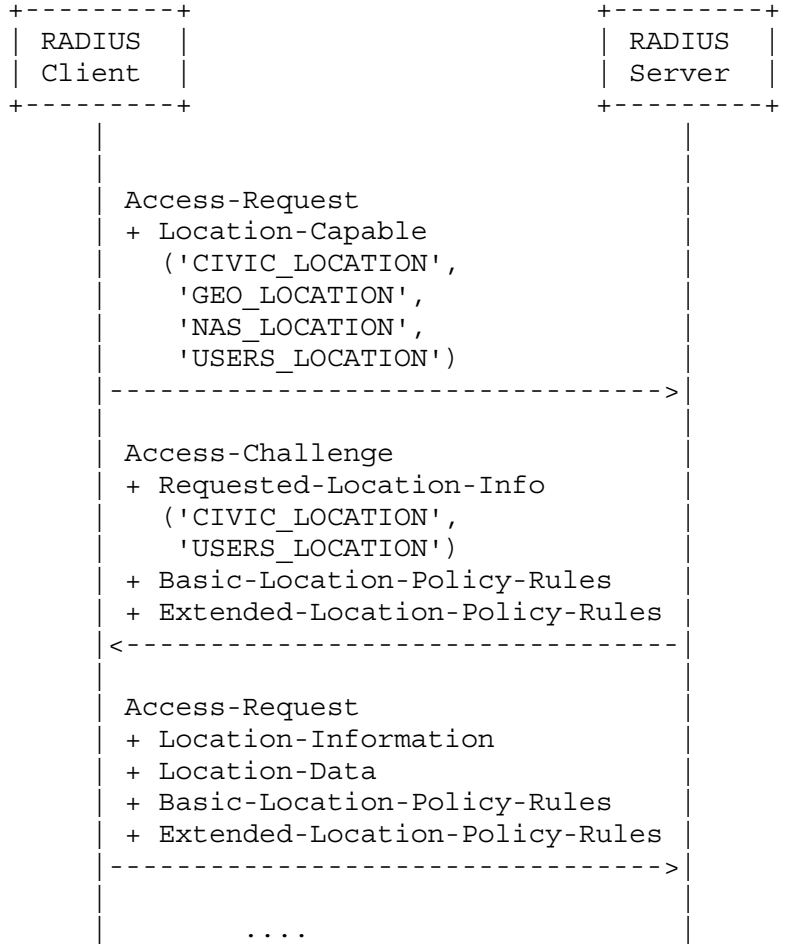
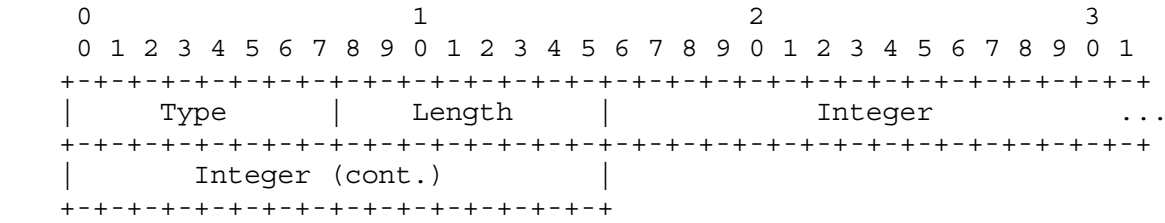



Figure 6: RADIUS server requesting location information

The Requested-Location-Info Attribute MUST be sent by the RADIUS server, in the absence of an out-of-band agreement, if it wants the RADIUS client to return location information and if authorization policies permit it. This Requested-Location-Info Attribute MAY appear in the Access-Accept or in the Access-Challenge message.

A summary of the attribute is shown below.




Type:

To Be Assigned by IANA - Requested-Location-Info Attribute

Length:

6

Integer:

The content of the Integer field 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 the Requested-Location-Info Attribute with the value set to CIVIC_LOCATION to request specific location information from the RADIUS client. The numerical value representing CIVIC_LOCATION requires the RADIUS client to attach civic location attributes. CIVIC_LOCATION refers to the location profile defined in Section 4.3.1.

Numerical Value:

A numerical value of this token is '1'.

Name:

GEO_LOCATION

Description:

The RADIUS server uses the Requested-Location-Info Attribute with the value set to GEO_LOCATION to request specific location information from the RADIUS client. The numerical value representing GEO_LOCATION requires the RADIUS client to attach geospatial location attributes. GEO_LOCATION refers to the location profile described in Section 4.3.2.

Numerical Value:

A numerical value of this token is '2'.

Name:

USERS_LOCATION

Description:

The numerical value representing USERS_LOCATION indicates that the RADIUS client MUST sent a Location-Information attribute with the Entity attribute expressing the value of zero (0). Hence, there is a one-to-one relationship between USERS_LOCATION token and the value of zero (0) of the Entity attribute inside the Location-Information attribute. 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 token is '4'.

Name:

NAS_LOCATION

Description:

The numerical value representing NAS_LOCATION indicates that the RADIUS client MUST sent a Location-Information attribute that contains location information with the Entity attribute expressing the value of one (1). Hence, there is a one-to-one relationship between NAS_LOCATION token and the value of one (1) of the Entity attribute inside the Location-Information attribute. A value of one indicates that the location information in the Location-Information attribute refers to the RADIUS client.

Numerical Value:

A numerical value of this token is '8'.

Name:

FUTURE_REQUESTS

Description:

The numerical value representing FUTURE_REQUESTS indicates that the RADIUS client MUST provide future Access-Requests for the same session with the same type of information as returned in the initial Access-Request message.

Numerical Value:

A numerical value of this token is '16'.

Name:

NONE

Description:

The RADIUS server uses this token to request that the RADIUS client stops sending location information.

Numerical Value:

A numerical value of this token is '32'.

If neither the NAS_LOCATION nor the USERS_LOCATION bit is set then per-default the location of the user's client device is returned (if authorization policies allow it). If both the NAS_LOCATION and the USERS_LOCATION bits are set then the returned location information has to be put into separate attributes. If neither the CIVIC_LOCATION nor the GEO_LOCATION bit is set in the Requested-Location-Info Attribute then no location information is returned. 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 information requested via CIVIC_LOCATION and via GEO_LOCATION.

As an example, if the bits for NAS_LOCATION, USERS_LOCATION and GEO_LOCATION are set then location information of the RADIUS client and the users' client device are returned in a geospatial location format.

## 5. 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 | 0-1 | 0 | 0 | 0+ | TBD | Operator-Name |
| 0+ | 0 | 0 | 0 | 0+ | TBD | Location-Information |
| 0+ | 0 | 0 | 0 | 0+ | TBD | Location-Data |
| 0-1 | 0-1 | 0-1 | 0-1 | 0-1 | TBD | Basic-Location-Policy-Rules |
| 0-1 | 0-1 | 0-1 | 0-1 | 0-1 | TBD | Extended-Location-Policy-Rules |
| 0 | 0-1 | 0 | 0-1 | 0 | TBD | Requested-Location-Info |
| 0-1 | 0 | 0 | 0 | 0 | TBD | Location-Capable |
| 0 | 0 | 0-1 | 0 | 0 | 101 | Error-Cause [note1] |

[note1] The Error-Cause attribute contains the value for the 'Location-Info-Required' error.

Change-of-Authorization Messages

| Request | ACK | NAK | # | Attribute |
|---|---|---|---|---|
| 0-1 | 0 | 0 | TBD | Basic-Location-Policy-Rules |
| 0-1 | 0 | 0 | TBD | Extended-Location-Policy-Rules |
| 0-1 | 0 | 0 | TBD | Requested-Location-Info |

Legend:

| | |
|---|---|
| 0 | This attribute MUST NOT be present. |
| 0+ | Zero or more instances of this attribute MAY be present. |
| 0-1 | Zero or one instance of this attribute MAY be present. |
| 1 | Exactly one instance of this attribute MUST be present. |
| 1+ | One or more of these attributes MUST be present. |

Figure 7: Table of Attributes

The Error-Cause Attribute is defined in [RFC5176].

The Location-Information and the Location-Data 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.

The attributes defined in this document are not used in any messages

other than the ones listed in Figure 7.

This document requests IANA to allocate a new value from the Error-Cause registry with the semantic of 'Location-Info-Required'.

## 6. 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, as defined in [RFC3588], for the Diameter AVPs are as follows:

| | | AVP Flag rules | | | | |
|---|---|---|---|---|---|---|
| Attribute Name | Value Type | MUST | MAY | SHOULD NOT | MUST NOT | Encr |
| Operator-Name | OctetString | | P | | V,M | Y |
| Location-Information | OctetString | | P | | V,M | Y |
| Location-Data | OctetString | | P | | V,M | Y |
| Basic-Location-Policy-Rules | OctetString | | P | | V,M | Y |
| Extended-Location-Policy-Rules | OctetString | | P | | V,M | Y |
| Requested-Location-Info | OctetString | | P | | V,M | Y |
| Location-Capable | OctetString | | P | | V,M | Y |

The RADIUS 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 [RFC3588] and Section 9 of [RFC4005].

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [RFC4005] or Diameter-EAP-Request [RFC4072]. What is said about Access-Challenge applies in Diameter to AA-Answer [RFC4005] or Diameter-EAP-Answer [RFC4072] 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 [RFC4005].

What is said about Accounting-Request applies to Diameter Accounting-

Request [RFC4005] as well.

Note that these AVPs may be used by Diameter applications other than RFC 4005 [RFC4005] and RFC 4072 [RFC4072]. The above-mentioned applications are, however, likely to be relevant in the context of this document.

# 7. Security Considerations

A number of security aspects are relevant for the distribution of location information via RADIUS. These aspects are discussed in separate sub-sections.

## 7.1. Communication Security

Requirements for the protection of a Location Object are defined in [RFC3693], namely mutual end-point authentication, data object integrity, data object confidentiality and replay protection.

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

- [RFC2865] proposes the usage of a static key that raised concerns regarding the lack dynamic key management. At the time of writing, work is ongoing to address some shortcomings of [RFC2865] attribute security protection.

- RADIUS over IPsec [RFC3579] enables the use of standard key management mechanisms, such as KINK, IKE and IKEv2 [RFC4306], to establish IPsec security associations. Confidentiality protection MUST be used to prevent eavesdropper gaining access to location information. Confidentiality protection already present for other reasons in many environments, such as 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 neighboring RADIUS entities to prevent man-in-the-middle attacks. Since mutual authentication is already required for key transport within RADIUS messages it does not represent a deployment obstacle. Since IPsec protection is suggested as a mechanism to protect RADIUS already no additional considerations need to be addressed beyond those described in [RFC3579].

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, modify and delete attributes or individual fields. 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 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 location attributes 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 RADIUS entities in the sense that object level security is not provided by neither RADIUS nor Diameter. Hence, some trust has to be placed on the RADIUS entities to behave according to the defined rules. Furthermore, the RADIUS protocol does 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 for network access authentication applications. 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 [RFC4282].

## 7.2. Privacy Considerations

This section discusses privacy implications for the distribution of location information within RADIUS. Note also that it is possible for the RADIUS server to obtain some amount of location information from the NAS identifier. This document, however, describes procedures to convey more accurate location information about the end host and/or the network. In a number of deployment environments location information about the network also reveals the current location of the user with a certain degree of precision depending on the location determination mechanism used, update frequency, the size of the network and other factors, such as movement traces.

Three types of use cases have to be differentiated:

- RADIUS server does not want to receive location information from the RADIUS client.

- In case there is an out-of-band agreement between the entity responsible for the NAS and the entity operating the RADIUS server then location information may be sent without an explicit request from the RADIUS server.

- The RADIUS server dynamically requests location information from the NAS.

#### 7.2.1. RADIUS Client

The RADIUS client MUST behave according to the following guidelines:

- If neither an out-of-band agreement exists nor location information is requested by the RADIUS server then location information is not disclosed by the RADIUS client.

- The RADIUS client MUST pass location information to other entities (e.g., when information is written to a local database or to the log files) only together with the policy rules. The entity receiving the location information (together with the policies) MUST follow the guidance given with these rules.

- A RADIUS client MUST include Basic-Location-Policy-Rules and Extended-Location-Policy-Rules Attributes that are configured within an Access-Request packet.

- NAS implementations supporting this specification, which are configured to provide location information, MUST echo Basic-Location-Policy-Rules and Extended-Location-Policy-Rules Attributes unmodified within a subsequent Access-Request packet. In addition, an Access-Request packet sent with a Service-Type value of "Authorize Only" MUST include Basic-Location-Policy-Rules or Extended-Location-Policy-Rules Attributes received in a previous Access-Accept if the FUTURE_REQUESTS flag was set in the Requested-Location-Info Attribute.

#### 7.2.2. RADIUS Server

The RADIUS server is a natural place for storing authorization policies since the user typically has some sort of trust relationship with the entity operating the RADIUS server. Once the infrastructure is deployed and location aware applications are available then there might be a strong desire to use location information for other purposes as well.

The Common Policy framework [RFC4745] that was extended for geolocation privacy [I-D.ietf-geopriv-policy] are tailored for this purpose. The Extensible Markup Language (XML) Configuration Access Protocol (XCAP) [RFC4825] gives users the ability to change their privacy policies using a standardized protocol. These policies are an important tool for limiting further distribution of the user's location to other location based services.

The RADIUS server MUST behave according to the following guidelines:

- The RADIUS server MUST attach available rules to the Access-Accept, the Access-Reject or the Access-Challenge message when the RADIUS client is supposed to provide location information.

- When location information is made available to other entities (e.g., writing to stable storage for latter billing processing) then the RADIUS server MUST attach the privacy rules to location information.

#### 7.2.3. RADIUS Proxy

A RADIUS proxy, behaving as a combined RADIUS client and RADIUS server, MUST follow the rules described in Section 7.2.1 and Section 7.2.2.

### 7.3. Identity Information and Location Information

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 RADIUS 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 user's identity can be "leaked" to the visited network or RADIUS brokers in a number of ways:

- 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 [RFC3041]. Some link layers make it possible to avoid MAC addresses or change them dynamically.

- Network access authentication procedures, such as PPP CHAP [RFC1994] or EAP [RFC4282], may reveal the user's identity as a part of the authentication procedure. Techniques exist to avoid this problem in EAP methods, for instance by employing private Network Access Identifiers (NAIs) in the EAP Identity Response message [RFC4187] and by method-specific private identity exchange in the EAP method (e.g., [RFC4187], [RFC5281] [I-D.josefsson-pppext-eap-tls-eap], [RFC5106]). Support for identity privacy within CHAP is not available.

- RADIUS 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 [RFC2865] or in some accounting attribute usage scenarios [RFC4372].

- Mobility protocols may reveal some long-term identifier, such as a home address.
- Application layer protocols may reveal other permanent identifiers.

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 some protocols lack support for identity privacy mechanisms. This problem is made worse by the fact that users may be unable to choose particular protocols, as the choice is often dictated by the type of network operator they use, 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 RADIUS server are in the same administrative domain. No direct relationship between the visited and the home network operator may be available and some RADIUS brokers need to be consulted. With subscription-based network access as used today the user has a contractual relationship with the home network provider that could (theoretically) 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 7.1.

## 8. 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 [RFC3575], in accordance with BCP 26 [RFC2434]. Additionally, the Attribute Type should be registered in the Diameter name space. For RADIUS attributes and registries created by this document IANA is requested to place them at http://www.iana.org/assignments/radius-types.

This document defines the following attributes:

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

Please refer to Section 5 for the registered list of numbers.

This document also instructs IANA to assign a new value for the Error-Cause Attribute [RFC5176], of "Location-Info-Required".

Additionally, IANA is requested to create the following new registries listed in the subsections below.

### 8.1. New Registry: Operator Namespace Identifier

This document also defines an operator namespace identifier registry (used in the Namespace ID field of the Operator-Name Attribute). Note that this document requests IANA only to maintain a registry of existing namespaces for use in this identifier field, and not to establish any namespaces nor to place any values within namespaces.

IANA is requested to add the following values to the operator namespace identifier registry using a numerical identifier (allocated in sequence), a token for the operator namespace and a contact person for the registry.

| Identifier | Operator Namespace Token | Contact Person |
|---|---|---|
| 0x30 | TADIG | TD.13 Coordinator (td13@gsm.org) |
| 0x31 | REALM | IETF O&M Area Directors (ops-ads@ietf.org) |
| 0x32 | E212 | ITU Director (tsbdir@itu.int) |
| 0x33 | ICC | ITU Director (tsbdir@itu.int) |

Note that the above identifier values represent the ASCII value '0' (decimal 48 or hex 0x30), '1' (decimal 49, or hex 0x31), '2' (decimal 50, or hex 0x32) and '3' (decimal 51, or hex 0x33). This encoding was chosen to simplify parsing.

Requests to IANA for a new value for a Namespace ID, i.e., values from 0x34 to 0xFE, will be approved by Expert Review. A designated expert will be appointed by the IESG.

The Expert Reviewer should ensure that a new entry is indeed required or could fit within an existing database, e.g., whether there is a real requirement to provide a token for an Namespace ID because one is already up and running, or whether the REALM identifier plus the name should recommended to the requester. In addition, the Expert Reviewer should ascertain to some reasonable degree of diligence that a new entry is a correct reference to an Operator Namespace, when a new one is registered.

### 8.2. New Registry: Location Profiles

Section 4.2 defines the Location-Information Attribute and a Code field that contains 8 bit integer value. Two values, zero and one, are defined in this document, namely:

Value (0): Civic location profile described in Section 4.3.1

Value (1): Geospatial location profile described in Section 4.3.2

The remaining values are reserved for future use.

Following the policies outline in [RFC3575] the available bits with a description of their semantic will be assigned after the expert review process. Updates can be provided based on expert approval only. Based on expert approval it is possible to mark entries as

"deprecated". A designated expert will be appointed by the IESG.

Each registration must include the value and the corresponding semantic of the defined location profile.

### 8.3. New Registry: Location-Capable Attribute

Section 4.6 defines the Location-Capable Attribute that contains a bit map. 32 bits are available whereby a 5 bits are defined by this document. This document creates a new IANA registry for the Requested-Location-Info Attribute. IANA is requested to add the following values to this registry:

| Value | Capability Token |
|---|---|
| 1 | CIVIC_LOCATION |
| 2 | GEO_LOCATION |
| 4 | USERS_LOCATION |
| 8 | NAS_LOCATION |

Following the policies outline in [RFC3575] the available bits with a description of their semantic will be assigned after the expert review process. Updates can be provided based on expert approval only. Based on expert approval it is possible to mark entries as "deprecated". A designated expert will be appointed by the IESG.

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-Location-Info Attribute.

### 8.4. New Registry: Entity Types

Section 4.2 defines the Location-Information Attribute that contains an 8 bit Entity field. Two values are registered by this document, namely:

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

Value (1) describes the location of the RADIUS client

All other values are reserved for future use.

Following the policies outline in [RFC3575] the available bits with a description of their semantic will be assigned after the expert review process. Updates can be provided based on expert approval only. Based on expert approval it is possible to mark entries as "deprecated". A designated expert will be appointed by the IESG.

Each registration must include the value and a corresponding description.

### 8.5. New Registry: Privacy Flags

Section 4.4 defines the Basic-Location-Policy-Rules Attribute that contains flags indicating privacy settings. 16 bits are available whereby a single bit, bit (0), indicating 'retransmission allowed' is defined by this document. Bits 1-15 are reserved for future use.

Following the policies outline in [RFC3575] the available bits with a description of their semantic will be assigned after the expert review process. Updates can be provided based on expert approval only. Based on expert approval it is possible to mark entries as "deprecated". A designated expert will be appointed by the IESG.

Each registration must include the bit position and the semantic of the bit.

### 8.6. New Registry: Requested-Location-Info Attribute

Section 4.7 defines the Requested-Location-Info Attribute that contains a bit map. 32 bits are available whereby a 5 bits are defined by this document. This document creates a new IANA registry for the Requested-Location-Info Attribute. IANA is requested to add the following values to this registry:

| Value | Capability Token |
|---|---|
| 1 | CIVIC_LOCATION |
| 2 | GEO_LOCATION |
| 4 | USERS_LOCATION |
| 8 | NAS_LOCATION |
| 16 | FUTURE_REQUESTS |
| 32 | NONE |

The semantic of these values is defined in Section 4.7.

Following the policies outline in [RFC3575] new Capability Tokens with a description of their semantic for usage with the Requested-Location-Info Attribute will be assigned after the expert review process. Updates can be provided based on expert approval only. Based on expert approval it is possible to mark entries as "deprecated". A designated expert will be appointed by the IESG.

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-Location-Info Attribute.

## 9. Acknowledgments

The authors would like to thank the following people for their help with an initial 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, and 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 James Polk, John Schnizlein and Marc Linsner. The authorization policy format is based on the work done by Jon Peterson.

The authors would like to thank Victor Lortz, Anthony Leibovitz, 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, Victor Fajardo, Tolga Asveren and John Loughney helped us with the Diameter RADIUS interoperability section. Andreas Pashalidis reviewed a later version document and provided a number of comments. Alan DeKok, Lionel Morand, Jouni Korhonen, David Nelson and Emile van Bergen provided guidance on the Requested-Location-Info Attribute and participated in the capability exchange discussions. Allison Mankin, Jouni Korhonen and Pasi Eronen provided text for the operator namespace identifier registry. Jouni Korhonen interacted with the GSMA to find a contact person for the TADIG operator namespace and Scott Bradner consulted the ITU-T to find a contact person for the E212 and the ICC operator namespace.

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.

We would like to thank members of the Wimax Forum Global Roaming Working Group (GRWG) for their feedback on the Operator-Name attribute. Ray Jong Kiem helped us with his detailed description to correct the document.

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.

Finally, we would like to thank Dan Romascanu, Glen Zorn, Russ Housley, Jari Arkko, Ralph Droms, Adrial Farrel, Tim Polk, and Lars Eggert for the IETF Last Call comments, Derek Atkins for his security area directorate review and Yoshiko Chong for spotting a bug in the IANA consideration section.

# 10. References

## 10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, March 2003.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

[RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

[RFC5176] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

## 10.2. Informative References

[GMLv3] "Open Geography Markup Language (GML) Implementation Specification", OGC 02-023r4, http://www.opengis.org/techno/implementation.htm", , January 2003.

[GSM] "TADIG Naming Conventions, Version 4.1", GSM Association Official Document TD.13", , June 2006.

[I-D.ietf-geopriv-policy]
Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., and J. Polk, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", draft-ietf-geopriv-policy-20 (work in progress), February 2009.

[I-D.josefsson-pppext-eap-tls-eap]
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.

[ISO] "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes, ISO 3166-1", , 1997.

[ITU1400] "Designations for interconnections among operators' networks, ITU-T Recommendation M.1400", , January 2004.

[ITU212] "The international identification plan for mobile terminals and mobile users, ITU-T Recommendation E.212", , May 2004.

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, D., and D. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4017] Stanley, D., Walker, J., and B. Aboba, "Extensible

Authentication Protocol (EAP) Method Requirements for Wireless LANs", RFC 4017, March 2005.

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4372] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

[RFC4745] Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences", RFC 4745, February 2007.

[RFC4825] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", RFC 4825, May 2007.

[RFC5106] Tschofenig, H., Kroeselberg, D., Pashalidis, A., Ohba, Y., and F. Bersani, "The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method", RFC 5106, February 2008.

[RFC5281] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC 5281, August 2008.

## Appendix A. Matching with Geopriv Requirements

This section compares the requirements for a GEOPRIV Using Protocol, described in [RFC3693], against the approach of distributing Location Objects with RADIUS.

In Appendix A.1 and Appendix A.2 we discuss privacy implications when RADIUS entities make location information available to other parties. In Appendix A.3 the requirements are matched against these two scenarios.

### A.1. Distribution of Location Information at the User's Home Network

When location information is conveyed from the RADIUS client to the RADIUS server then it might subsequently be made available for different purposes. This section discusses the privacy implication for making location information available to other entities.

To use a more generic scenario we assume that the visited RADIUS and the home RADIUS server belong to different administrative domains. The Location Recipient obtains location information about a particular Target via protocols specified outside the scope of this document (e.g., SIP, HTTP or an API).

The subsequent figure shows the interacting entities graphically.

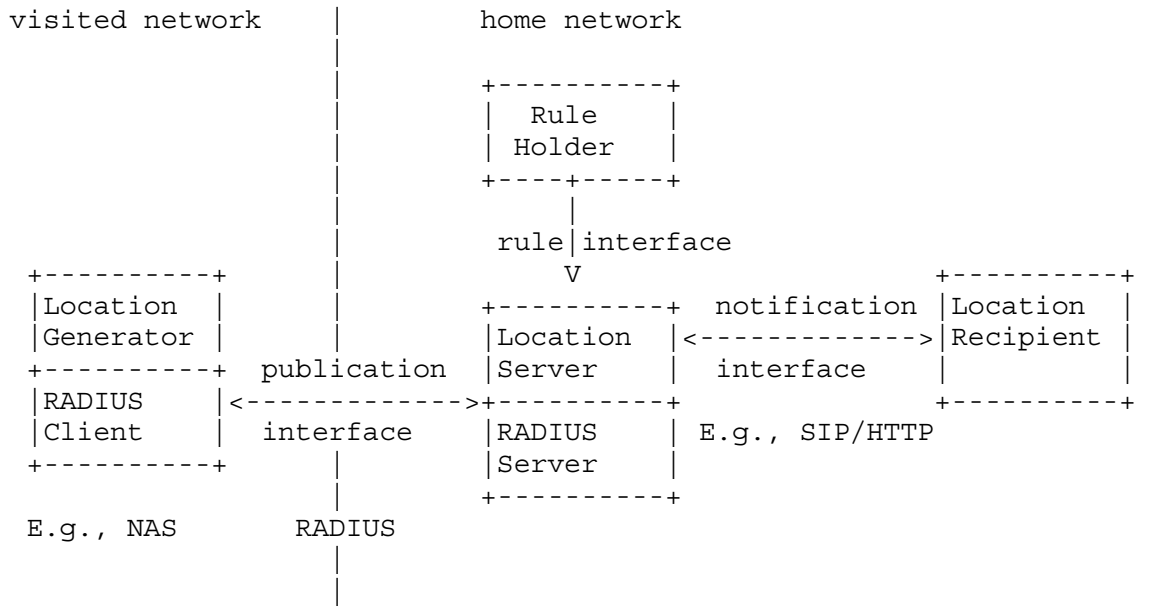



Figure 8: Location Server at the Home Network

The term 'Rule Holder' in Figure 8 denotes the entity that creates the authorization rule set.

## A.2. Distribution of Location Information at the Visited Network

This section describes a scenario where location information made available to Location Recipients by a Location Server in the visited network. Some identifier needs to be used as an index within the location database. One possible identifier is the Network Access Identifier. RFC 4282 [RFC4282] and RFC 4372 [RFC4372] provide background whether entities in the visited network can obtain the user's NAI in cleartext.

The visited network provides location information to a Location Recipient (e.g., via SIP or HTTP). This document enables the NAS to obtain the user's privacy policy via the interaction with the RADIUS server. Otherwise only default policies, which are very restrictive, are available. This allows the Location Server in the visited network to ensure act according to the user's policies.

The subsequent figure shows the interacting entities graphically.

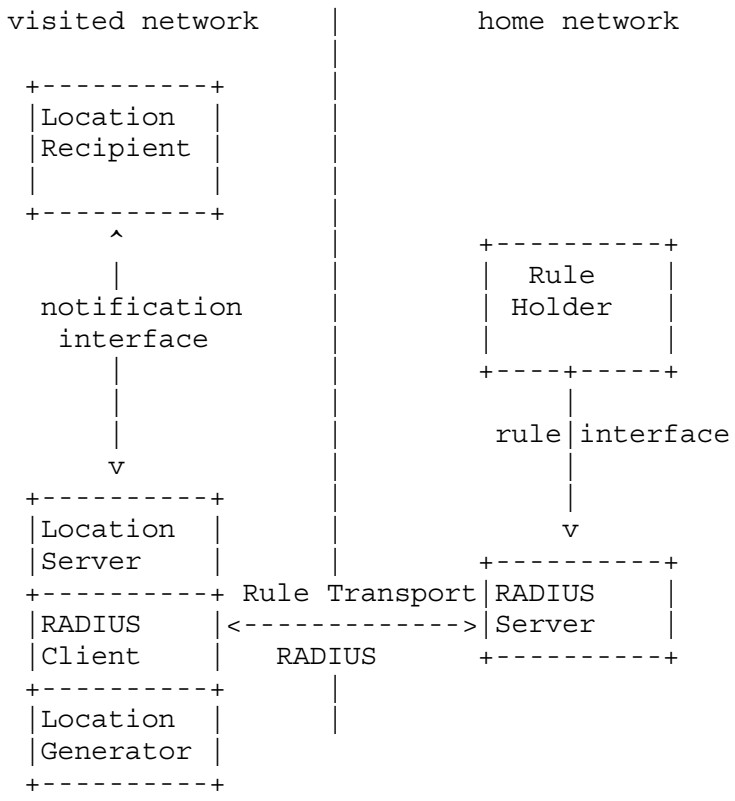



Figure 9: Location Server at the Visited Network

Location information always travels with privacy policies. This document enables the RADIUS client to obtain these policies. The Location Server can subsequently act according to these policies to provide access control using the Extended-Location-Policy-Rules and to adhere the privacy statements in the Basic-Location-Policy-Rules.

## A.3. Requirements matching

Section 7.1 of [RFC3693] details the requirements of a "Location Object". We discuss these requirements in the subsequent list.

Req. 1. (Location Object generalities):

* Regarding requirement 1.1, the syntax and semantic of the location object is taken from the [RFC3825] and [RFC4776]. It is furthermore possible to convert it to the format used in GMLv3 [GMLv3], as used with PIDF-LO [RFC4119].

* 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) used in the DHCP civic format gives a further classification of the location. This attribute can be seen as an extension.

* Regarding requirement 1.4, this document does not define the format of the location information.

* Regarding requirement 1.5, location information is only sent from the RADIUS client to the RADIUS server.

* Regarding requirement 1.6, the Location Object contains both location information and privacy rules. Location information is described in Section 4.2, in Section 4.3.1 and in Section 4.3.2. The corresponding privacy rules are detailed in Section 4.4 and in Section 4.5.

* 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 Section 4.2, Section 4.3.1, Section 4.3.2 Section 4.4 and in Section 4.5).

* Regarding requirement 1.8, the encoding of the Location Object has an emphasis on a lightweight encoding format to be used with RADIUS.

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 7.2 it has a number of advantages if this identifier is not carried in clear. 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 RADIUS 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 7 describes these security mechanisms offered by the RADIUS protocol. The same is true for requirement 2.4.

* Regarding requirement 2.5, Section 4.2, Section 4.3.1 and Section 4.3.2 describe the content of the location fields. 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 provides the capability for the RADIUS server to indicate what type of location information it would like to see from the RADIUS client.

* Regarding requirement 2.7, timing information is provided with 'sighting time' and 'time-to-live' field defined in Section 4.2.

* Regarding requirement 2.8, a reference to an external (more detailed rule set) is provided with the Extended-Location-Policy-Rules attribute Section 4.5 .

* 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 4.3.2 and in Section 4.3.1.

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

* Regarding requirement 3.3, the geospatial location information used by 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 [RFC3825].

* Regarding requirement 3.4, further Location Data Types can be added via new coordinate reference systems (CRSs) (see Datum field in [RFC3825]) and via extensions to [RFC3825] and [RFC4776].

Section 7.2 of [RFC3693] 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 regarding the transmission and storage of the LO. This document requires that entities that aim to make location information available to third parties are required to obey the privacy 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 7 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 7.2) 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.

Section 7.3 of [RFC3693] 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 8 the decision of a Location Server to provide a Location Recipient access to location information is based on Rule Maker-defined Privacy Rules that are stored at the home network. With regard to the scenario shown in Figure 9 the Rule Maker-defined Privacy Rules are sent from the RADIUS server to the NAS (see Section 4.4, Section 4.5 and Section 7.2 for more details).

Req. 8. (LG Rules): For all usage scenario it is possible to consider the privacy rule before transmitting location information from the NAS to the RADIUS server or even to third parties. In the case of an out-of-band agreement between the owner of the NAS and the owner of the RADIUS server privacy might be applied on a higher granularity. For the scenario shown in Figure 8 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 7.2). A Location Server in the visited network has to evaluate available rulesets.

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-Location-Policy-Rules Attribute Section 4.4. A reference to the extended ruleset is carried in Section 4.5. The format of these rules are described in [RFC4745] and [I-D.ietf-geopriv-policy].

Req. 11. (Limited Rule language): A limited (or basic) ruleset is provided by the Policy-Information Attribute Section 4.4 (and as introduced with PIDF-LO [RFC4119]).

Section 7.4 of [RFC3693] 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 7. The importance for user identity confidentiality and identity protection has already been recognized as an important property (see, for example, a document on 'EAP Method Requirements for Wireless LANs' [RFC4017]).

Req. 13. (Credential Requirements): As described in Section 7 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 7 these requirements are fulfilled with the usage of IPsec if 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 RADIUS 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).

Authors' Addresses

Hannes Tschofenig (editor)
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

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

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Email: bernarda@microsoft.com