Geopriv
Internet-Draft
Expires: January 10, 2005

H. Tschofenig
Siemens
F. Adrangi
Intel
A. Lior
M. Jones
Bridgewater

July 12, 2004

# Carrying Location Objects in RADIUS
# draft-tschofenig-geopriv-radius-lo-00.txt

## Status of this Memo



This Internet-Draft will expire on January 10, 2005.

## 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 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 incumbent operators such as cellular carriers (GSM and CDMA), Wireless Internet Service Providers (WISP), and fixed broadband operators.

When an end host authenticates itself to such a network, information about the location and operational ownership of this network needs to be conveyed to the users'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), 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 [RFC2865].

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 privacy of the owner of the location information. With [I-D.ietf-geopriv-reqs] 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 enforce access control policies on access to 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 [RFC2119].

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

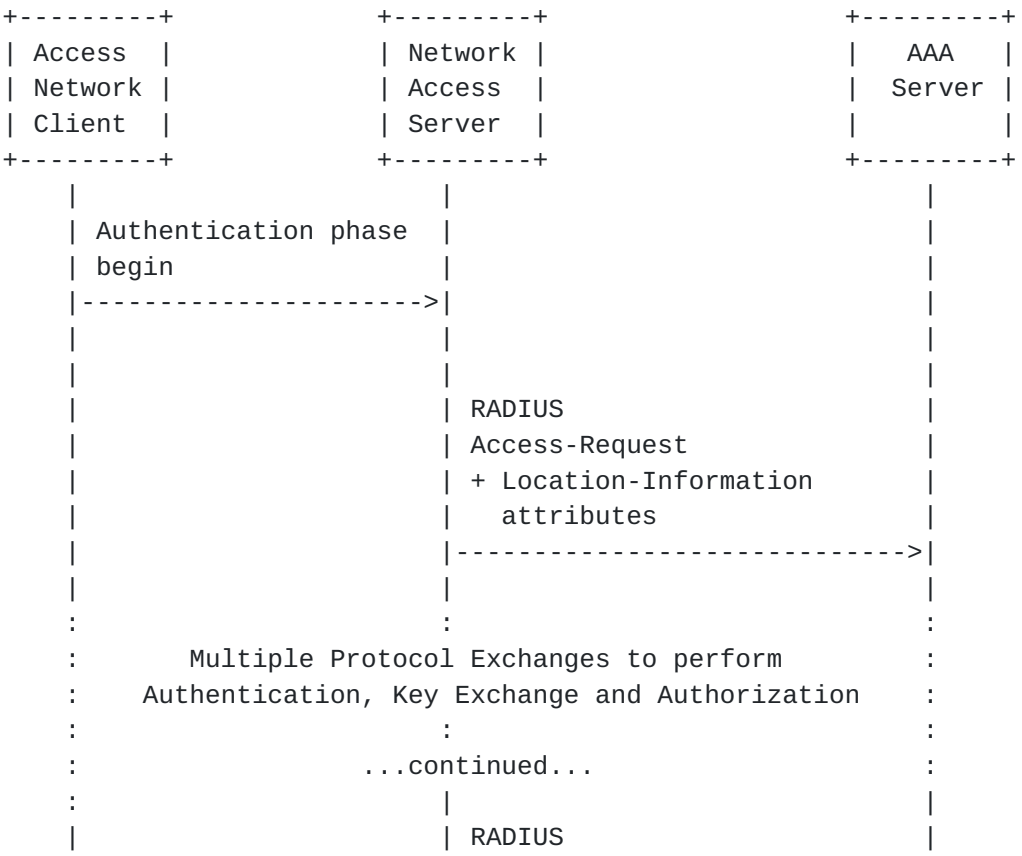
Terminology related to privacy issues, location information and authorization policy rules are taken from [I-D.ietf-geopriv-reqs].

## 3. Delivery Methods for Location Information

Location Infomation Objects defined in this document are transported over RADIUS protocol from visited access network to the AAA server. The information 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 message 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 again allowed to carry location specific attributes.



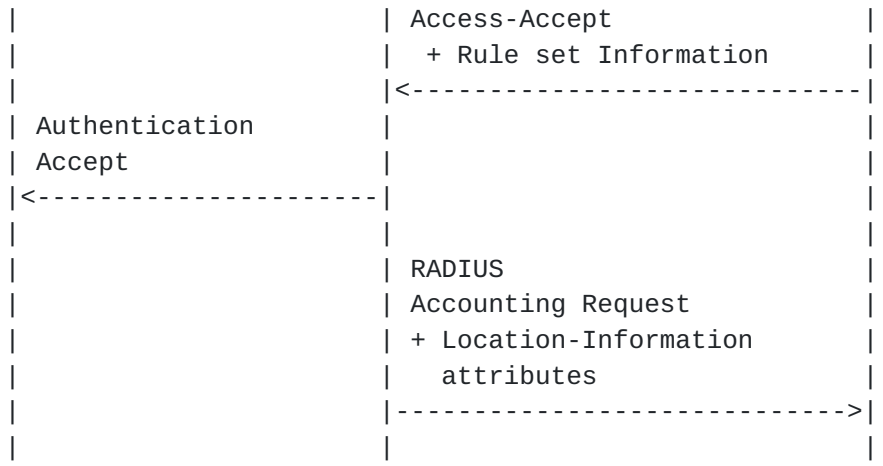



Figure 1: Message Flow: Authentication/Authorization Phase Delivery

### 3.2 Mid-session Delivery

Mid-session delivery method uses the Change of Authorization (COA) message as defined in [RFC3576]. In accordance to [RFC3576], at anytime during the session the AAA server may send the access network a COA message containing session identification attributes (see [RFC3576] for the possible options). 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.

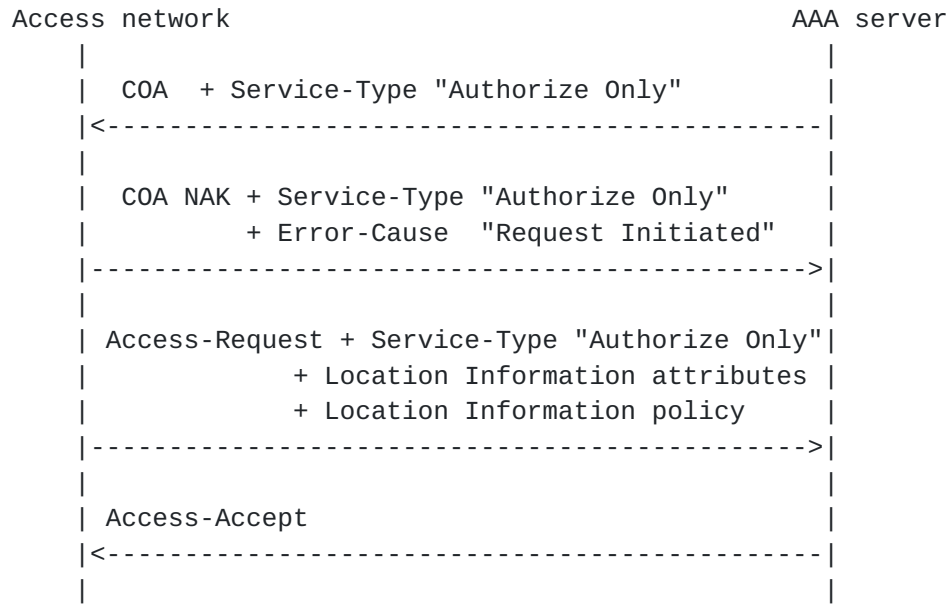



Figure 2: Message Flow: Mid-session Delivery

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 13.

### 4.1 Use Case 1 - Use of Location Information in AAA

An 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 and 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 authroizes the session. If the user's location policies are available to the RADIUS server, the RADIUS server may deliver those policies in an Access Accept. 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 users bill. For example, there may be different tarrif rates applied based on the location and their maybe different tax rates applied based on the location. Unless otherwise specified, 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. For the purpose of this scenario Location servers are the NAS, and RADIUS servers. The RADIUS servers are in the home network, in the visited network, or in

broker networks.

Unless otherwise specified, excluding the proxy chain from the NAS to the Home RADIUS, the Location Server may not transmit the location information to other parties.

Upon authentication and authorization, the Home RADIUS may transmit the Rule set in an Access-Accept to the other Location Server allowing them to transmit location information. Then and only then they are allowed to share the information.

Note since the NAS is the source of all Location information that is disimenated by RADIUS, the NAS could tag the location information with the location rules or a reference for the location rules received in an Access-Accept. All location information in the Accounting Stream will now be tagged.

## 5. Overview

The location information and operational ownership of the access network is conveyed in five AAA attributes which are: Operator-Name, Location-Information, Location-Type , Policy-Information and Billing-Description. Furthermore, basic authorization policy rules are attached to the Location-Information attribute turning Location Information into a Location Object as defined in [I-D.ietf-geopriv-reqs].

### 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 the prefix and the 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 ogranization 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 Precision field provides further information about the location information provided via Radius. For large networks information about the location of the user can be provided in different degrees of accuracy. This field gives a hint. Ideally the location of the user is returned to the home network but in some cases it might not be available. It has to be noted that the user does not provide the location information itself.

### 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 [I-D.ietf-geopriv-dhcp-civil].

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

For completeness we include more detailed information from [I-D.ietf-geopriv-dhcp-civil] with regard to the defined civil location elements (A1 through A6):

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

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

Table 1

Additional CA types are defined in Section 3.4 of [I-D.ietf-geopriv-dhcp-civil]. These types are useful to express further information about the location, language specific settings via the 'language' item and encoding information via the 'script' item. Section 12 shows usage examples of this attribute.

All attributes are optional and can appear in any order. The values are encoded using UTF-8 [RFC3629].

### 5.2.2 Geospatial Location Information

This document reusing geospatial location information from [I-D.ietf-geopriv-dhcp-lci-option] 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 [I-D.ietf-geopriv-dhcp-lci-option] 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. Policy-Information Attribute

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:

- The user hides its location information from the access network and from intermediate networks using the appropriate network access authentication mechanism. Section 13 discusses these issues in more details.
- 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 [I-D.ietf-geopriv-rules] and [I-D.ietf-geopriv-rules].

With regard to authorization policies this document reuses work done in [I-D.peterson-geopriv-pidf-lo] and encodes it in an non-XML format.

## 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 [I-D.ietf-simple-rpid] which is reused by [I-D.ietf-geopriv-dhcp-civil] 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. Billing-Description Attribute

The Billing-Description Attribute contains unstructured text to be printed on the users bill.

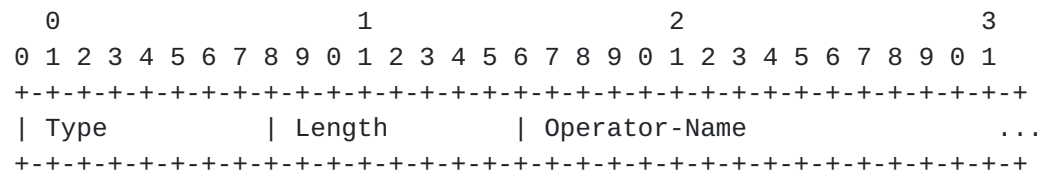
## 9. Attributes

This section defines attributes for access network operational ownership, Location Name, Location Information and Billing Description.

### 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.




Type:
To Be Assigned by IANA - Operator-Name

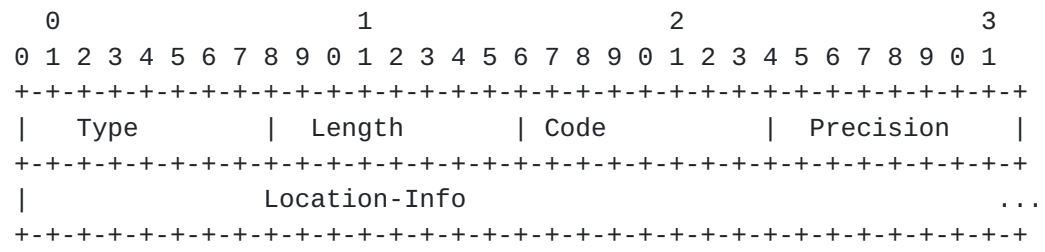
Length:
>= 3

Operator-Name:
The text field contains an Access Network Operator Name in prefix-based format as describe above.
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.




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

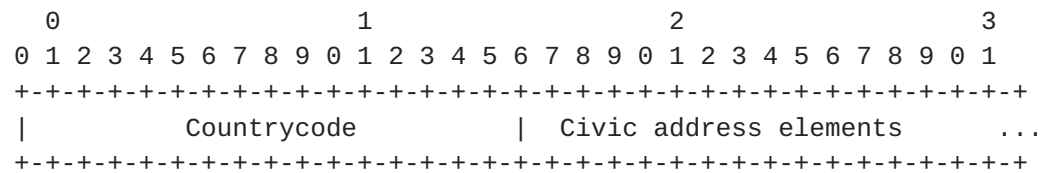
Length (8 bits):
>= 3

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

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

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

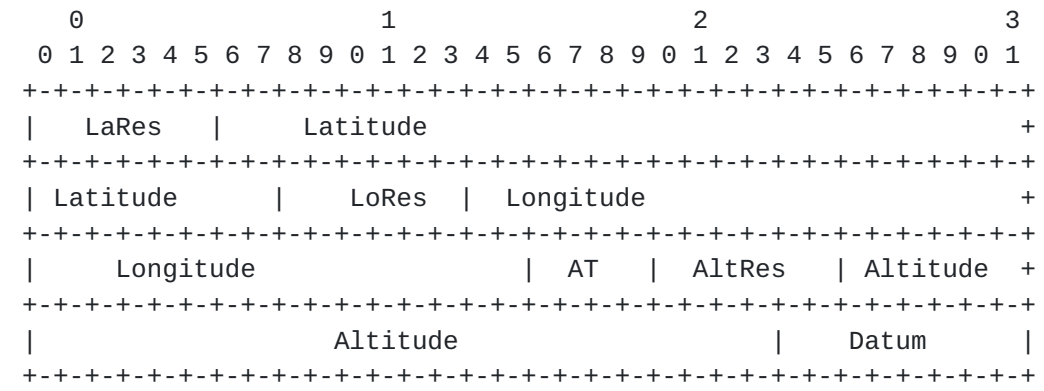



Countrycode (16 bits):
Two-letter ISO 3166 country code in capital ASCII leters.

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 [I-D.ietf-geopriv-dhcp-civil] with a TLV pair (whereby the Type and Length fields are one-octed long). An example is given in Section 12.

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




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

(3) NAD 83

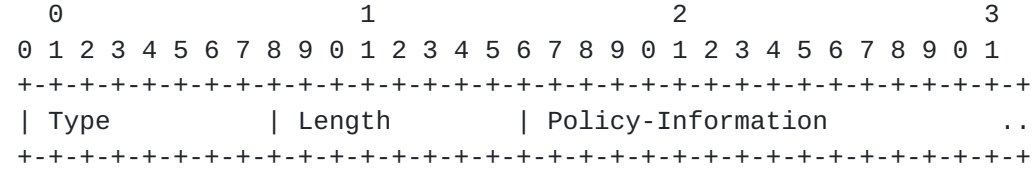
The length of the Location-Information Attribute MUST NOT exceed 253 octets. The length of the geospatial location information format is fixed with 16 bytes plus a four byte header.

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 [I-D.ietf-geopriv-dhcp-lci-option].

## 9.3 Policy-Information Attribute

Policy-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.

A summary of the Policy-Information attribute is shown below.




Type :
To Be Assigned by IANA - Policy-Information

Length:
>= 3

Policy-Information:
The text field contains information about the 'usage-rules' element described below. Its length MUST NOT exceed 64 octets.

For this document we use the following fields of the 'usage-rules' element, described in [I-D.peterson-geopriv-pidf-lo]:

- 'retransmission-allowed' (R): 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.
- '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 [RFC1305].

- 'ruleset-reference': This field contains a URI that indicates where a fuller ruleset of policies related to this object can be found. As a deviation from [I-D.peterson-geopriv-pidf-lo] 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. Per-default this field has a null-size. The content of this field is of variable length.

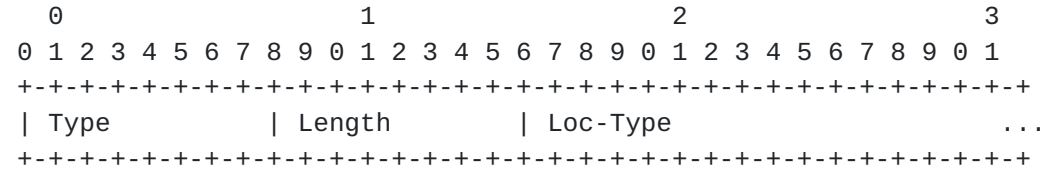
We use the following encoding for the Policy-Information element. The 'retransmission-allowed' flag consumes 1 bit, followed by 64 bits for the NTP timestamp and a variable length 'ruleset-reference'.

We do not use the 'note-well' element since it contains a block of text with generic privacy directives which are human-readable only.

### 9.4 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.



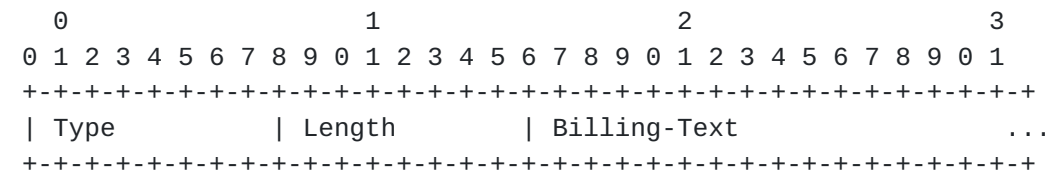

Type (8 bits):
To Be Assigned by IANA - Location-Name

Length (8 bits):
>= 3

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

### 9.5 Billing-Description Attribute

The Billing-Description Attribute contains unstructured text to be printed on the users bill.




Type (8 bits):
To Be Assigned by IANA - Billing-Description

Length (8 bits):
>= 3

Billing-Text (variable):
The content of this field contains text for billing purpose.

The length of the Billing-Description Attribute MUST NOT exceed 32 octets.

## 10. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, 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 | 0 | 0 | 0-1 | TBD | Policy-Information |
| 0-1 | 0 | 0 | 0 | 0-1 | TBD | Location-Type |
| 0-1 | 0 | 0 | 0 | 0 | TBD | Billing-Description |

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.

## 11. IANA Considerations

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

Operator-Name
Location-Information
Policy-Information
Location-Name
Billing-Description

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

## 12. 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 [I-D.ietf-geopriv-dhcp-lci-option].

Due to the size limitations of the RADIUS attributes we give a more detailed example borrowed from Section 4 of [I-D.ietf-geopriv-dhcp-civil].

| 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.

## 13. Privacy Considerations

This section discusses privacy implications for the distribution of location lnformation 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, to determine the location, update frequence, where the location was generated, size of the network and other mechanism (such as movement traces or interpolation).

Two entities act as location servers in the configuration shown in Section 4:

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

Entity in the home network (e.g., home AAA server): The AAA server in the home network might be an ideal place for storing authorization policies. 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 [I-D.ietf-geopriv-rules] and in [I-D.ietf-geopriv-rules] are tailored for this environment. The user typically has a contractual relationship to his home network and hence the trust relationship between them are higher. 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. As a default policy we specify that the home network MUST NOT distribute the user's location information to other entities.

For the envisioned usage scenarios the network access authentication procedure is tighly coupled to the transfer of location information. If the authentication mechanism allows the visited networks or brokers to learn the user's identity then it is possible to correleate location information with a particular user. This 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 (where possibly no direct relationship between

the visited and the home network operator is available and some AAA brokers need to be consulted) since the NAS and the home AAA are in the same administrative domain. 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 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 14.

One way to ensure that the visited network and intermediate networks are incapable to learn the user identity is to use EAP methods which hide the user identity either actively or passively. Some EAP methods (such as [I-D.arkko-pppext-eap-aka]) 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 [I-D.arkko-roamops-rfc2486bis].

For stronger security and privacy protection active user identity confidentiality is highly suggested. EAP methods such as [I-D.josefsson-pppext-eap-tls-eap] or [I-D.tschofenig-eap-ikev2] 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 features which mainly aims to prevent eavesdroppers on the wireless link to learn the user identity of the attached users. Awareness for this type of threat model 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 granualrity of location information can be provided to the home network. From a privacy point of view lower

granularity is preferrable. The user, however, has no control over the granularity and cannot lie about its location.

## 14. Security Considerations

Requirements for the security protection of a Location Object is defined in [I-D.ietf-geopriv-reqs]: 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 [I-D.peterson-geopriv-pidf-lo]. 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 [I-D.ietf-geopriv-reqs] are inline with threats which appear in the relationship with disclosure of location information as described in [I-D.ietf-geopriv-threat-analysis]. [I-D.peterson-geopriv-pidf-lo] proposes S/MIME to protect the Location Object against modifications and against eavesdropping. To provide mutual authentication confidentiality protection and a digital signature is necessary. Furthermore, to offer replay protection a gurantee of freshness is necessary (for example, based on timestamps).

The security of S/SIME is based on public key cryptography which raises performance, deployment and size considerations. Encryption requires that the local AAA server knows the recipient's public key (e.g., the public key of the home AAA server). Some sort of public key infrastructure is therfore 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.

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

- [RFC2865] proposes the usage of a static key which is not appropriate for protection of location information due to the missing dynamic key management and absent confidentiality protection. If no authentication, integrity and replay protection between the participating entities are provided then an adversaries can spoof and modify transmitted AVPs.
- RADIUS over IPsec [RFC3579] allows to run standard key management mechanisms, such as KINK [I-D.ietf-kink-kink], IKE and IKEv2 [I-D.ietf-ipsec-ikev2], to establish IPsec security associations. Confidentiality protection MUST be used to prevent eavesdropper gaining access to location information. Confidentiality protection is not only a property required by this document, it is also required for the transport of keying material in the context of EAP authentication and authorization. Hence, this requirement is, in many environments, already fulfilled. Mutual authentication must be provided between the local AAA server and the home AAA server to prevent man-in-the-middle attacks. This is another requirement raised in the area of key transport with RADIUS and does not represent a deployment obstacle. The performance advantages a superior compared to the usage of S/MIME and object security since the expensive authentication and key exchange protocol run needs to be provided only once (at for a long time). Symmetric channel security with IPsec is highly efficient. Since IPsec protection is suggested as a mechanism to protect RAIDUS already no additional considerations need to be addressed beyond those described in [RFC3579]. Where an untrusted AAA intermediary is present, the Location Object MUST NOT be provided to the intermediary.

## 15. Open Issues

A future version of this document will describe the described Radius attributes work with Diameter.

Furthermore, the scenarios described in Section 4 need to be described in more detail.

## 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.

This document is partially based on the discussions within the IETF GEOPRIV working group. Therefore, the authors thank Henning Schulzrinne, James Polk and John Morris for their work they have done in the Geopriv working group.

Furthermore, we also have to thank Allison Mankin, Randall Gellens, Andrew Newton, Ted Hardie, Jon Peterson for their time discussing a number of details with us.

# 17. References

## 17.1 Normative References

[I-D.ietf-geopriv-dhcp-civil]
Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses", draft-ietf-geopriv-dhcp-civil-02 (work in progress), March 2004, <reference.I-D.ietf-geopriv-dhcp-civil.xml>.

[I-D.ietf-geopriv-dhcp-lci-option]
Polk, J., Schnizlein, J. and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", draft-ietf-geopriv-dhcp-lci-option-03 (work in progress), December 2003, <reference.I-D.ietf-geopriv-dhcp-lci-option.xml>.

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

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

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000, <reference.RFC.2866.xml>.

[RFC3576] 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, <reference.RFC.3576.xml>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003, <reference.RFC.3629.xml>.

## 17.2 Informative References

[I-D.adrangi-radius-bandwidth-capability]
Adrangi, F., "Access Network Bandwidth Capability", draft-adrangi-radius-bandwidth-capability-00 (work in progress), February 2004, <reference.I-D.adrangi-radius-bandwidth-capability.xml>.

[I-D.arkko-pppext-eap-aka]
Arkko, J. and H. Haverinen, "EAP AKA Authentication", draft-arkko-pppext-eap-aka-11 (work in progress), October

2003, <reference.I-D.arkko-pppext-eap-aka.xml>.

[I-D.arkko-roamops-rfc2486bis]
Aboba, B., "The Network Access Identifier", draft-arkko-roamops-rfc2486bis-00 (work in progress), February 2004, <reference.I-D.arkko-roamops-rfc2486bis.xml>.

[I-D.ietf-geopriv-common-rules]
Schulzrinne, H., Morris, J., Tschofenig, H. and J. Polk, "Geopriv Rules", draft-ietf-common-rules-00 (work in progress), January 2004, <reference.I-D.ietf-geopriv-common-rules.xml>.

[I-D.ietf-geopriv-reqs]
Cuellar, J., Morris, J., Mulligan, D., Peterson, D. and D. Polk, "Geopriv requirements", draft-ietf-geopriv-reqs-04 (work in progress), October 2003, <reference.I-D.ietf-geopriv-reqs.xml>.

[I-D.ietf-geopriv-rules]
Schulzrinne, H., Morris, J., Tschofenig, H., Polk, J. and J. Rosenberg, "Common Rules", draft-ietf-common-rules-00 (work in progress), January 2004, <reference.I-D.ietf-geopriv-common-policy.xml>.

[I-D.ietf-geopriv-threat-analysis]
Danley, M., "Threat Analysis of the Geopriv Protocol", draft-ietf-geopriv-threat-analysis-01 (work in progress), September 2003, <reference.I-D.ietf-geopriv-threat-analysis.xml>.

[I-D.ietf-ipsec-ikev2]
Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-13 (work in progress), March 2004, <reference.I-D.ietf-ipsec-ikev2.xml>.

[I-D.ietf-kink-kink]
Thomas, M. and J. Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)", draft-ietf-kink-kink-05 (work in progress), January 2003, <reference.I-D.ietf-kink-kink.xml>.

[I-D.ietf-simple-rpid]
Schulzrinne, H., Gurbani, V., Kyzivat, P. and J. Rosenberg, "RPID: Rich Presence: Extensions to the Presence Information Data Format (PIDF)", draft-ietf-simple-rpid-02 (work in progress), March 2004,

<reference.I-D.ietf-simple-rpid.xml>.

[I-D.josefsson-pppext-eap-tls-eap]
Josefsson, S., Palekar, A., Simon, D. and G. Zorn, "Protected EAP Protocol (PEAP)", draft-josefsson-pppext-eap-tls-eap-07 (work in progress), October 2003, <reference.I-D.josefsson-pppext-eap-tls-eap.xml>.

[I-D.peterson-geopriv-pidf-lo]
Peterson, J., "A Presence-based GEOPRIV Location Object Format", draft-peterson-geopriv-pidf-lo-02 (work in progress), October 2003, <reference.I-D.peterson-geopriv-pidf-lo.xml>.

[I-D.tschofenig-eap-ikev2]
Tschofenig, H., Kroeselberg, D. and Y. Ohba, "EAP IKEv2 Method (EAP-IKEv2)", draft-tschofenig-eap-ikev2-03 (work in progress), February 2004, <reference.I-D.tschofenig-eap-ikev2.xml>.

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

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


## 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.