

Internet Engineering Task Force
Internet Draft
Document: [draft-tang-spatial-payload-reqs-00.txt](#)
Expires: May 2001

Haitao Tang
Nokia
James M. Polk
Cisco Systems
Mari Korkea-aho
Nokia
Kenji Takahashi
NTT

Nov. 2000

Spatial Location Payload Requirements with Protocol Recommendations

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#). Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

1. Abstract

This document describes the requirements placed on the Spatial Location Payload (SLO), as well as its specific protocol recommendations, regardless of the Protocol utilized.

Internet Draft [draft-tang-spatial-payload-reqs-00.txt](#) Nov.2000

2. Conventions used in this document

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 [RFC-2119](#) [2].

3. Definition of Terms

Although the following terms cannot be IANA registered (because we are not defining a Protocol), they are included here for clarification purposes.

Target: The entity whose location is known by the server and desired by the client. The protocol does not specify how the server learns the location of the target.

Server: Entity that supplies the location of the target to the client. One end of the protocol.

Client: The entity that desired to learn the location of the target. One end of the protocol.

Coordinate: An ordered set of N numbers designating the position of a point in an N-dimensional space.

Geodetic Datum: A set of parameters describing the size and shape of the earth and the origin and orientation of the coordinate systems used to map the earth.

Location Accuracy: The measurement is correct to within this maximum expected error.

Time: Real time of the measurement/fix of the target location.

Speed: Ground speed and Vertical speed of the target.

Direction: The direction of the target movement, expressed in a 2-dimensional (horizontal) frame indicated by the magnetic (or true) North.

Course: The direction from the current position of the target to a defined destination, expressed in a 2-dimensional (horizontal) frame indicated by the magnetic (or true) North.

Orientation: The orientation of the target, expressed in a 2-dimensional (horizontal) frame indicated by the magnetic (or true) North, and a vertical element expressed by the angle between the horizontal plane and the main axis of the object.

4. Location Representation

A location representation is an instantiation of the location of a target. In SLO, location representations shall be determined through two levels of abstraction: schema and format.

"Schema" defines the logical scheme which the location representations are based on. For example, location is expressed with latitude, longitude, and altitude using WGS-84 as reference system. Velocity is expressed as horizontal and vertical elements. "Format" defines how a given schema is represented. For example, a location determined by longitude, latitude, and altitude can be represented by degrees, minutes, and seconds with arbitrary decimal fractions. The velocity can be represented in meters per second with arbitrary decimal fractions.

The payload must:

- a. Define one default location representation that must be supported by all SLO entities.
 - _ The scheme for the default location representation must specify an absolute location on the earth, using WGS-84 geodetic datum as reference system.
 - The format for the default location representation must specify the location in longitude, latitude, and altitude parameters.Altitude is a recommended (must be provided if available) parameter.
- b. Support other location representations than the default, including existing schemes and formats widely used in other contexts.
- c. Specify an IANA registration process for additional representations.
- d. Permit at a minimum, the following values to be included in a payload, providing that the entities have such capability to specify:
 - (1) Used Coordinate (e.g., long, lat., alt. in degrees) and datum (e.g., WGS-84)
 - (2) Geocentric Position
 - (3) Location Accuracy
 - (4) Time (date, time, time zone)
 - (5) Speed (ground speed, vertical speed)
 - (6) Direction
 - (7) Course
 - (8) Orientation
 - (9) Other un-specified attributes, such as descriptive location.
- e. Permit multiple scheme/format representations in a single payload.
- f. Be extendable to support new location representations.

5. Security Methods

Operations on SLO payloads, such as retrieval of a particular element of a payload, must be defined and implemented to enforce security (including privacy) protection. Such operations MUST:

- a. Provide a mandatory-to-implement, optional-to-use method for an entity to retrieve encrypted elements inside the payload. The method should allow a choice in the algorithm(s) used.

- b. The method SHALL work according to the policy attributes set to the elements, as well as other (possibly multiple) attributes such as the identity (or anonymity) of the target/client and its class-of-user.
- c. Provide a mandatory-to-implement, optional-to-use data integrity and data origin authentication method for the payload. The method should allow a choice in the algorithm(s) used.
- d. Not degrade a target/client's expectations of privacy.

6. Identity and Policy Attributes

The payload MUST:

- a. Specify the mandatory-to-implement, optional-to-use target identifier and policy attributes for an entity to retrieve the encrypted elements inside the payload, and for an entity to identify/name the target of the payload.
- b. Specify the way that the policy attributes and client identity/class-of-user are used to restrict location information (e.g., location accuracy and locatability) retrieved by interpreting policy selected for class-of-user.
- c. Protocols SHALL use the target identifier in any target-related actions (e.g., Server Discovery).
- d. Target identifier SHALL be given according to 8.2.c.

7. Payload Encoding

The payload encoding:

- a. MUST support multiple formats. Each format must be registered with IANA.
- b. MUST support a simple format for the values in Sec 4., 5., and 6.
- c. SHOULD have a provision to specify the location accuracy.
- d. MUST be able to infer the IANA type and the beginning and end of each format without parsing the entire message (as in TLV).
- e. MUST allow formats to contain UTF-8 (mandatory) and the optional (raw binary, local character sets, UTF-16, and UTF-32) content.
- f. Must support formats that contain human-readable text. Such text SHOULD specify the language to be used.
- g. MUST be extensible/flexible enough to support a future descriptive location format.

8. Protocol Recommendations

A SLO can be used/carried by various relevant protocols. Due to the nature of location information, the following recommendations are made to those protocols for the proper usage:

8.1 Representation Negotiation

The protocol must:

- a. Provide a mechanism for a client to indicate which additional representations it prefers.
- b. Provide a mechanism for the client to select which of said representations it prefers.
- c. Provide the capability to provide reports in any representation
- d. Provide that, following such selection, server reports in the format chosen by the client.

8.2. Server Discovery

- a. There SHALL be a server discovery mechanism for a client to find the appropriate server for a given target.
- b. The discovery mechanism SHALL work across domains. It SHOULD use widely deployed mechanisms such as DNS. It SHALL permit server locations to be changed with TTL's ranging from minutes to months.
- c. Targets SHALL be identified with an identifier. The target identifier SHALL be unique within the domain of the server.
- d. Servers SHALL be identified by an identifier. Server names SHALL

be globally unique. For example, a URI of the form "protocol:haitao-tangs-phone@airtouch.com" would be an appropriate way to identify a target. DNS is then used to find the server.

- e. Clients MUST be able to perform DNS A, A6, AAAA, and SRV lookups, and may support manual configuration and/or other methods to resolve the IP address of a suitable server in an unqualified domain.
- f. Translator services should be distinguishable from other servers during discovery.
- g. It is desirable that translator capabilities (supported formats) can be determined during discovery.

8.3. Protocol Security

The protocol must:

- a. Provide a mandatory-to-implement, optional-to-use authentication mechanism from client to server and from server to client. The mechanism should allow a choice in the algorithm(s) used.
- b. Specify how such a mechanism shall be used in the presence of firewalls and Network Address Translation (NAT) between client and server.
- c. Include mechanisms to allow subsequent location policy decisions to be based on (possibly multiple) factors in addition to the identity (or anonymity) of the target/client, e.g., authentication mechanism, group membership(s), and class-of-user.
- d. Support a mandatory-to-implement, optional-to-use data integrity and data origin authentication mechanism for all data. The mechanism should allow a choice in the algorithm(s) used.
- e. Provide a mandatory-to-implement, optional-to-use data confidentiality mechanism. The mechanism should allow a choice in the algorithm(s) used.
- f. Not degrade a target/client's expectations of privacy.
- g. Support anonymous use, authenticated use, as well as the combined use of the both. Anonymous use MAY require the server(s) to be able to associate location with the same (anonymous) target/client over time. The anonymous party MAY want to authenticate the other parties (i.e., who gets/provides the location). In addition, the legitimacy of the anonymous party MAY need to be authenticated.
- h. Specify a mechanism for extending the security mechanism for additional capability.
- i. Not dictate the ways how a target should communicate relevant information with a server, or/and a client, given such communication is needed. The ways MUST NOT degrade a target/client/server's expectations of privacy.

8.4. Protocol Policy

To direct the proper dealing with the target/client's information, the

protocol must:

- a. Specify a Policy Information Base (PIB), as well as classes of user for spatial location server.
- b. Specify the way that the PIB and classes of user are used to control the access of a client by the location server.
- c. Provide a mandatory-to-implement, optional-to-use Policy Enforcement Point_mechanism.
- d. Provide an optional Policy Decision Point_mechanism.
- e. Specify how servers obtain policy from a policy storage facility if the Policy Decision Point mechanism is implemented.

f. Provide a mechanism to direct the server's protection of the location information from any unwanted party by:

1. Locatability control
2. Security mechanisms.

9. References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", [BCP 9](#), [RFC 2026](#), October 1996.

[2] Bradner, S., "Key words for use in RFC's to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

[3] B. Rosen, J. Costa-Requena, M. Korkea-aho, M. Ylianttila, R. Mahy, [K. Takahashi](#), and [S. Farrell](#), "**Spatial Location Protocol Requirements**", Internet Draft [draft-rosen-spatial-requirements-00.txt](#), July 2000.

10. Author's Addresses

Haitao Tang
Nokia Research Center
P.O. BOX 407
FIN-00045 Nokia Group
Finland
Phone: +358 40 749 9256
Email: haitao.tang@nokia.com

James M. Polk
Office of the CTO
Cisco Systems, Inc.
[18581](#) North Dallas Parkway
Dallas, TX 75287 USA
Phone: +1 972 813 5208
Email: jmpolk@cisco.com

Mari Korkea-aho
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland
Phone: +358 40 733 9693
Email: mari.korkea-aho@nokia.com

Kenji Takahashi
Information Sharing Platform Laboratories
NTT
3-9-11 Midoricho

Musashino, Tokyo 180-8585 Japan
Phone: +81 422 59 6668
Email: kt@nttlabs.com

Copyright Statement

Copyright (C) The Internet Society (2000). All Rights Reserved.

Tang, Polk, Korkea-aho, and Takahashi

[Page 6]

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

