Network Working Group
Internet-Draft
Expires: August 30, 2006

T. Hardie
Qualcomm, Inc.
A. Newton
Verisign, Inc.
H. Schulzrinne
Columbia U.
H. Tschofenig
Siemens

February 26, 2006

LoST: A Location-to-Service Translation Protocol
draft-hardie-ecrit-lost-00.txt

Abstract

This document describes an XML-based protocol for mapping service identifiers and geospatial or civic location information to service contact URIs. In particular, it can be used to determine the

location-appropriate PSAP for emergency services.

Table of Contents

1. Requirements notation

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 [3].

2. Introduction

This document describes a protocol for mapping a service identifier and location information compatible with PIDF-LO [9] to one or more service contact URIs. These URIs may have any reasonable scheme, including sip, xmpp, and tel. While the initial focus is on providing mapping functions for emergency services, it is likely that the protocol is applicable to any service URN. For example, in the United States, the "2-1-1" and "3-1-1" services follow a similar location-to-service behavior as emergency services.

This document names this protocol usage "LoST" for Location-to-Service Translation Protocol. The features of LoST are:

- Supports queries using civic as well as geospatial location information.
- Can be used in both recursive and iterative resolution.
- Can be used for civic address validation.
- A hierarchical deployment of mapping servers is independent of civic location labels.
- Can indicate errors in the location data to facilitate debugging and proper user feedback while simultaneously providing best-effort answers.
- Mapping can be based on either civic or geospatial location

information, with no performance penalty for either.

- Service regions can overlap.

- Satisfies the requirements [5] for mapping protocols.

- Minimizes round trips by caching individual mappings as well as coverage regions ("hinting"). Unless otherwise desired, there is only one message exchange (roundtrip delay) between the client requesting a mapping and the designated resolver. This also facilitates reuse of TLS or other secure transport association across multiple queries.

This document focuses on the description of the protocol between the mapping client (seeker or resolver) and the mapping server (resolver or other servers). The relationship between other functions, such as discovery of mapping servers, data replication and the overall mapping server architecture in general, will be described in a separate document. [10] is a first attempt to describe such a mapping

server architecture.

3. Usage

The client queries a server, indicating the desired service and the location object. If the query succeeds, the server returns a result that includes one or more URIs for reaching the appropriate service for the location indicated. Depending on the query, the result may contain a region where the same mapping would apply, a reference to another server to which the client should send a query, and error messages indicating problems with interpretation of location information. The combination of these components are left to the needs and policy of the jurisdiction where the server is being operated.

The interaction between the client and server is triggered by four types of events:

1. When the client starts up and/or attaches to a new network location.

2. When the client detects that its location has changed sufficiently that it is outside the bounds of the region returned in an earlier query.

3. When cached mapping information has expired.

4. When calling for a particular service. During such calls, a client MAY request a short response that contains only the mapping data, omitting region information. The use of a different transport protocol is TBD.

Cached answers are expected to be used by clients only after failing to accomplish a location-to-URI mapping at call time. Cache entries may expire according to their time-to-live value, or they may become invalid if the location of the caller's device moves outside the boundary limits of the cache entry. Boundaries for cache entries may be set in both geospatial and civic terms.

4. Server Discovery

There are likely to be a variety of ways that clients can discover appropriate LoST servers, including DHCP, SIP device configuration, or DNS records for their signaling protocol domain, e.g., the AOR domain for SIP. The appropriate server depends on, among other considerations, who operates LoST services, including the Internet Service Provider (ISP), Voice Service Provider (VSP), or the user's

home domain. In each case, the host name returned may be resolved using DDDS methods. [Details TBD.]

5. Service Types

The type of service desired is specified by the <service> element. The emergency identifiers listed in the registry established with [6] will be used in this document.

If a more specific service is requested but does not exist, information for the more generic service SHOULD be returned. For example, a request for urn:service:sos.fire might return urn:service:sos in the United States since citizens in that country reach the fire department through the common emergency service.

6. Example

After performing link layer attachment and end host performs stateful address autoconfiguration (in our example) using DHCP. DHCP provides the end host with civic location information (encoded in UTF-8 format):

CAtype	CAvalue
0	US
1	New York
3	New York
6	Broadway
22	Suite 75
24	10027-0401

Figure 1: DHCP Civic Information Example

Additionally, DHCP provides information about the LoST server that can be contacted. An additional step of indirection is possible, for example by having DHCP return a domain name that has to be resolved to one or more IP addresses hosting LoST servers.

Both at attachment time and call time, the client places a LoST request, including its civic location and the desired service. A snippet of the request that omits encapsulating protocol information and namespace declarations is shown below:

```
<mapping>
  <request>
    <operation>recurse</operation>
    <service>urn:service:sos</service>
    <gp:location-info>
      <cl:civicAddress>
        <cl:country>US</cl:country>
        <cl:A1>New York</cl:A1>
        <cl:A3>New York</cl:A3>
        <cl:A6>Broadway</cl:A6>
        <cl:HNO>123</cl:HNO>
        <cl:LOC>Suite 75</cl:LOC>
        <cl:PC>10027-0401</cl:PC>
      </cl:civicAddress>
    </gp:location-info>
  </request>
```

```
    </mapping>
```


Since the contacted LoST server has the requested information available the following response is returned. The response indicates, as a human readable display string that the 'New York City Police Department' is responsible for the given geographical area. The indicated URI allows the user to start communication using SIP or XMPP. The 'civicMatch' elements indicates which parts of the civic address were matched successfully. Other parts of the address, here, the suite number, were ignored and not validated. The region part of the response indicates that all of New York City would result in the same response. The dialstring element indicates that the service can be reached via the dial string 9-1-1. A snippet of the response is shown below, omitting namespace details and protocol wrappers:

```
  <mapping>
    <response expires="2006-03-09T01:53:33.396Z">
      <service>urn:service:sos</service>
      <displayName>New York City Police Department</displayName>
      <uri>sip:nypd@example.com xmpp:nypd@example.com</uri>
      <civicMatch>
        <gp:location-info>
          <cl:civicAddress>
            <cl:country>US</cl:country>
            <cl:A1>New York</cl:A1>
            <cl:A3>New York</cl:A3>
            <cl:A6>Broadway</cl:A6>
            <cl:HNO>123</cl:HNO>
            <cl:PC>10027-0401</cl:PC>
          </cl:civicAddress>
        </gp:location-info>
      </civicMatch>
      <region>
        <gp:location-info>
          <cl:civicAddress>
            <cl:country>US</cl:country>
            <cl:A1>New York</cl:A1>
            <cl:A3>New York</cl:A3>
          </cl:civicAddress>
        </gp:location-info>
      </region>
```

```
        <dialstring>911</dialstring>
      </response>
    </mapping>
```


7. Deployment Methods

Because services for emergency contact resolution may differ depending on local or service needs, this document only specifies the "wire format" for LoST services and explicitly leaves open the possibility for many different types of deployment.

For instance:

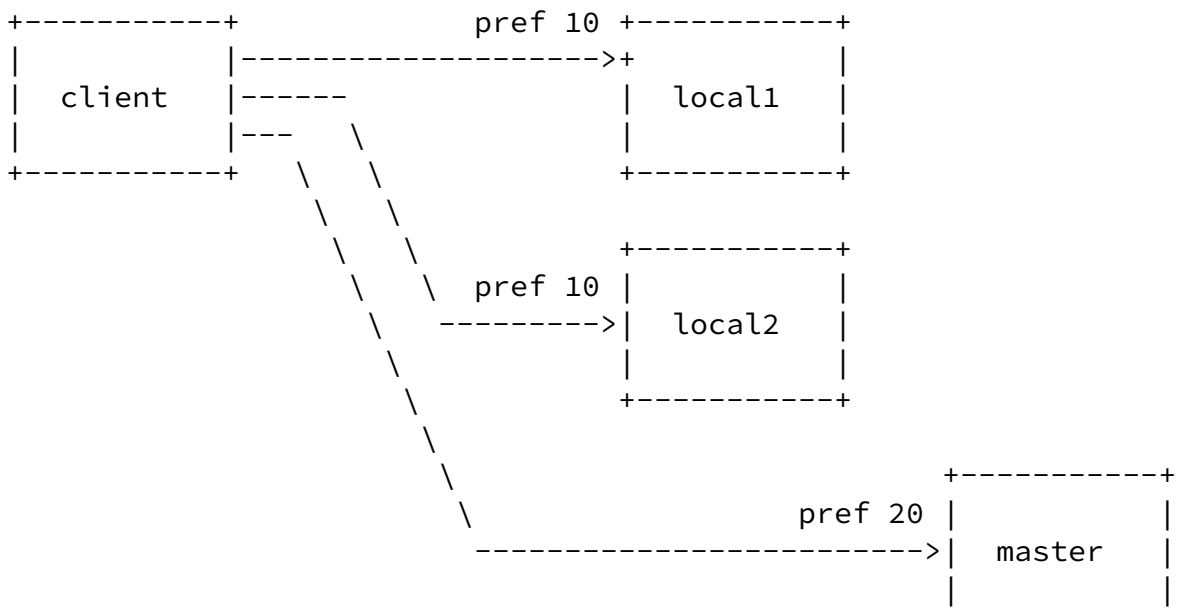
During discovery, a client may be directed to issue all queries to an LoST service completely authoritative for a given jursidiction.

A client may be directed to issue queries to an LoST server that acts as a reflector. In such a case, the LoST server analyzes the query to determine the best server to wich to refer the client.

Or the client may be directed to a server that performs further resolution on behalf of the client.

A LoST service may also be represented by multiple LoST servers, either grouped together or at multiple network locations. Using S-NAPTR [11], clients may be given a list of multiple servers to which queries can be sent for a single service.

For instance, the service at emergency.example.com may advertise LoST service at local1.emergency.example.com, local2.emergency.example.com, and master.emergency.example.com. Each server may given a different preference. In this case, 'local1' and 'local2' may be given a lower preference (more preferred) than 'master', which might be a busier server or located further away.


pref 10
client
local1
pref 10
local2
pref 20
master

8. IANA Considerations

TBD, such as namespace registrations.

9. Security Considerations

There are multiple threats to the overall system of which service mapping forms a part. An attacker that can obtain service contact URIs can use those URIs to attempt to disrupt those services. An attacker that can prevent the lookup of contact URIs can impair the reachability of such services. An attacker that can eavesdrop on the communication requesting this lookup can surmise the existence of an emergency and possibly its nature, and may be able to use this to launch a physical attack on the caller.

To avoid that an attacker can modify the query or its result, LoST RECOMMENDS the use of channel security, such as TLS.

A more detailed description of threats and security requirements are provided in [4].

[Editor's Note: A future version of this document will describe the countermeasures based on the security requirements outlined in [4].]

10. Open Issues

A number of open issues have been identified that are not yet addressed by this draft version:

- The transport mechanism, such as "plain" HTTP or SOAP.
- The appropriate transport protocols beyond TLS/TCP, such as whether UDP is to be supported.
- LoST service operators may determine which transfer protocol most meets their needs, and advertise their availability using the DNS DDDS application S-NAPTR [11]. The aspect of service discovery and load balancing needs to be described.
- Error conditions and codes.
- The inclusion of dial string information.
- The name 'LoST' is a placeholder before a better name is found.
- An internationalization considerations section is needed.
- The XML schema's are not yet provided.
- Full-fletched examples are missing.
- The security consideration section is incomplete.
- The IANA consideration section is missing.

11. References

11.1 Normative References

[1] World Wide Web Consortium, "XML Schema Part 2: Datatypes", W3C XML Schema, October 2000, <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>.

[2] World Wide Web Consortium, "XML Schema Part 1: Structures", W3C XML Schema, October 2000, <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>.

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

[4] Schulzrinne, H., "Security Threats and Requirements for Emergency Calling", draft-taylor-ecrit-security-threats-01 (work in progress), December 2005.

[5] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", draft-ietf-ecrit-requirements-03 (work in progress), February 2006.

[6] Schulzrinne, H., "A Uniform Resource Name (URN) for Services", draft-schulzrinne-sipping-service-01 (work in progress), October 2005.

[7] Mealling, M., "The IETF XML Registry", draft-mealling-iana-xmlns-registry-03 (work in progress), November 2001.

[8] OpenGIS, "Open Geography Markup Language (GML) Implementation Specification", OGC OGC 02-023r4, January 2003.

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

11.2 Informative References

[10] Schulzrinne, H., "Location-to-URL Mapping Architecture and Framework", draft-schulzrinne-ecrit-mapping-arch-00 (work in progress), October 2005.

[11] Daigle, L. and A. Newton, "Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)", RFC 3958, January 2005.

Authors' Addresses

Ted Hardie
Qualcomm, Inc.

Andrew Newton
Verisign, Inc.

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7004
Email: hgs+ecrit@cs.columbia.edu
URI: http://www.cs.columbia.edu

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

Email: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com

Intellectual Property Statement

Disclaimer of Validity

WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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