### The LoST-Validation S-NAPTR Application Service Tag
### draft-gellens-lost-validation-05

Abstract

   This document adds the LoST-Validation service tag to the S-NAPTR
   Application Service Tag IANA registry.  This tag is used by clients
   of the Location-to-Service Translation Protocol (LoST).

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF).  Note that other groups may also distribute
   working documents as Internet-Drafts.  The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   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."

   This Internet-Draft will expire on August 24, 2020.

Table of Contents

## 1.  Document Scope

   This document only adds an additional entry for 'LoST-Validation' to
   the S-NAPTR Application Service Tag IANA registry.  This tag is used
   by clients of the Location-to-Service Translation Protocol (LoST)
   [RFC5222].

## 2.  Introduction

   The Location-to-Service Translation Protocol, LoST [RFC5222] defines
   a mapping service with the additional ability to request that a civic
   address be validated.  The National Emergency Number Association
   (NENA) has defined an architecture for all-IP emergency services
   (known as "i3" [NENA-i3]), which defines the mapping (routing) and
   validation functions as two distinct functional elements, defined as
   an Emergency Call Routing Function (ECRF) and a Location Validation
   Function (LVF).  NENA i3 requires that the mapping (ECRF) and
   validation (LVF) functions be separable, so that an entity
   responsible for a LoST server cluster can decide to provide mapping
   and validation services using consolidated or separate server
   clusters (i.e., using the same or separate boxes).  The rationale is
   that the mapping service is used in real-time during emergency call
   routing, while the validation service is used in advance, typically
   when data is provisioned, and therefore the mapping service has much
   higher availability and response time requirements than the
   validation service.  An organization might choose to deploy these
   services using different server clusters to make it easier to provide

higher levels of service for the mapping function while shielding it
from the potentially bursty load of validation, while another
organization might choose to use the same sets of servers for both,
configured and deployed to offer the high service level demanded of
the mapping service.

In order to permit this separability, any entity querying a LoST
server needs to be able to resolve an Application Unique String (AUS)
into a URL for a server that offers the required service (mapping or
validation).  This separability needs to be maintained throughout the
LoST tree structure, from forest guide to leaf node.  Because LoST
referrals return an AUS rather than a URL, either a different Service
Tag or a DNS name convention (e.g., "ecrf.example.org" and
"lvf.example.org") is needed to differentiate the different services.
DNS name conventions are inflexible and fragile, so a different
service tag is the preferred approach.

## [3](#).  The LoST-Validation Application Service Tag

This document adds 'LoST-Validation' to the S-NAPTR Application
Service Tag registry created by [RFC3958].  The 'LoST-Validation' tag
serves as a counterpart to the 'LoST' tag added by [RFC5222]: The
'LoST' tag identifies servers able to perform the core mapping
function, while 'LoST-Validation' identifies servers explicitly
willing to perform the validation function.

Because some servers might be configured to provide both mapping and
validation functions, a server identified using the 'LoST' service
tag might also perform the validation function (and resolving the two
tags might result in the same URL).  Because the two functions might
be separate, clients seeking a LoST server for location validation
should first try U-NAPTR resolution using the 'Lost-Validation'
service tag, and may fallback to the 'LoST' service tag if the 'Lost-
Validation' service tag cannot be resolved to a usable LoST server.

LoST [RFC5222] specifies that LoST servers are located by resolving
an application Unique String (AUS) using U-NAPTR/DDDS (URI-Enabled
NAPTR/Dynamic Delegation Discovery Service) [RFC4848], and defines
the 'LoST' Application service tag.  In order to permit separability
of the mapping and validation services performed using LoST, this
document defines the 'LoST-Validation' service tag.  NAPTR records
for LoST servers available for location validation contain the 'LoST-
Validation' service tag.  An entity needing to perform location
validation using LoST performs the discovery procedure as described
in [RFC5222], except that the 'LoST-Validation' service tag is used
in preference to the 'LoST' service tag.  For both service tags, the
HTTP and HTTPS URL schemes are used.  In the absense of any NAPTR
records containing the 'LoST-Validation' service tag, the 'LoST'

service tag is used.  Fallback to the 'LoST' service tag may follow
if the 'Lost-Validation' service tag fails to result in a usable LoST
server.  Using the 'LoST-Validation' service tag might result in the
same URL as the 'LoST' service tag, or it may result in a different
URL.  The URLs might result in the same physical servers being
contacted, or different servers.

## [4](#).  Backwards Compatability

The primary use of LoST in general, and the location validation
functionality in particular, is within the emergency services area.
Within North America, the NENA i3 [[NENA-i3](#)] document specifies how
protocols including LoST are used.  The i3 document is expected to
reference the 'LoST-Validation' service tag, and specify its use in
both server DNS records and client resolution of Application Unique
Strings (AUS).

LoST allows a server to refuse to perform location validation, and
defines the 'locationValidationUnavailable' warning.  LoST also
allows a server to refer to another server rather than answering
itself.  So, in a deployment where a LoST tree has separate server
clusters for mapping and for validation, the mapping servers could
either perform the validation as requested, or return the
'locationValidationUnavailable' warning, and potentially also include
a <redirect> element to redirect to the validation server.  However,
the <redirect> element contains an Application Unique String, so
unless the AUSs for validation and mapping are different (e.g.,
'ecrf.example.org' and 'lvf.example.org'), we still need a different
service tag to allow for flexible deployment choices (i.e., not
requiring a DNS name convention).

LoST clients performing emergency services operations are expected to
comply with the latest NENA i3 specification, and hence support the
'LoST-Validation' service tag when defined.  A LoST client
implemented prior to the addition of the 'LoST-Validation' tag would
use the 'LoST' tag to resolve an AUS.  Such a client might not be
performing location validation, but if it is, the LoST server it
contacts may perform the service.  Even in a deployment where mapping
and validation are split, the data is identical; the split is a load
and deployment optimization strategy.  The server designated for
mapping is likely to perform validation when requested, potentially
unless it is under load.  If an older client attempts validation
using a designated mapping server that refuses the request, the
client will retry later, at which point the server may no longer be
under load and may provide the function.  Even in the (unlikely) case
of a designated mapping server that refuses to perform validation at
any time, the server is likely to return a redirect with a different
AUS (e.g., "lvf.example.com") that resolves to a designated

validation server.  In the (unlikely) worst case, the client will be
unable to reach a server willing to perform validation, and will
submit a discrepancy report, as specified in NENA i3.  The
discrepancy report resolution would be to update the client with the
'LoST-Validation' service tag, update the AUS returned in a redirect
and DNS to use a different DNS name, or permit the server to perform
validation when not under stress (or a combination).  Note that,
because LoST does not require servers to perform validation, the
situation described can exist regardless of the addition of the
'LoST-Validation' service tag.  The addition of the tag improves the
situation.

## 5.  Security Considerations

The security considerations described in [RFC3958], [RFC4848], and
[RFC5222] apply here.  No additional security aspects are foreseen by
the addition of an extra tag.  Separation of services might be
desired, for example, to be able to allocate different levels of
resources (such as server capacity, attack mitigation, bandwidth,
etc.) to the mapping and validation services, in which case separate
tags are needed to allow LoST clients (which may include other LoST
servers) to identify the correct server cluster.

## 6.  IANA Considerations

IANA is requested to add 'LoST-Validation' to the S-NAPTR Application
Service Tag registry created by [RFC3958]  This tag serves as a
counterpart to the 'LoST' tag added by [RFC5222].

(Note that IANA and [RFC3958] call this registry "S-NAPTR Application
Service Tags" while [RFC5222] calls it "U-NAPTR application service
tag".)

### 6.1.  S-NAPTR Registration

This document registers an S-NAPTR application service tag:

   Application Service Tag: LoST-Validation

   Defining Publication: This document.

## 7.  Acknowledgements

Many thanks to Ted Hardie and Ben Campbell for their helpful reviews
and suggestions.

8.  Changes from Previous Versions

8.1.  Changes from -00 to -01

   o  Fixed incorrect tag in Section 6

   o  Clarified background and explanation in Section 2

   o  Clarified text in Section 3

   o  Expanded text in Section 5

8.2.  Changes from -01 to -02

   o  Fixed bug in .xml file

8.3.  Changes from -02 to -03

   o  Reworded fallback text in Section 2

8.4.  Changes from -03 to -04

   o  Fixed some references to [RFC4848] that should be to [RFC5222] in
      sections Section 2 and Section 3

   o  Added clarifying text in Abstract

   o  Copied text from Abstract to Section 1

   o  Added clarifying text in Section 2

8.5.  Changes from -04 to -05

   o  Added reference to [RFC5222] in Section 5

   o  Added clarifying text to Section 2

   o  Moved some text from Section 2 to Section 3

   o  Added new section Section 4

9.  References

9.1.  Normative References

   [RFC3958]  Daigle, L. and A. Newton, "Domain-Based Application
              Service Location Using SRV RRs and the Dynamic Delegation
              Discovery Service (DDDS)", RFC 3958, DOI 10.17487/RFC3958,
              January 2005, <https://www.rfc-editor.org/info/rfc3958>.

   [RFC4848]  Daigle, L., "Domain-Based Application Service Location
              Using URIs and the Dynamic Delegation Discovery Service
              (DDDS)", RFC 4848, DOI 10.17487/RFC4848, April 2007,
              <https://www.rfc-editor.org/info/rfc4848>.

   [RFC5222]  Hardie, T., Newton, A., Schulzrinne, H., and H.
              Tschofenig, "LoST: A Location-to-Service Translation
              Protocol", RFC 5222, DOI 10.17487/RFC5222, August 2008,
              <https://www.rfc-editor.org/info/rfc5222>.

## 9.2.  Informative references

   [NENA-i3]  National Emergency Number Association (NENA)
              Interconnection and Security Committee, i3 Architecture
              Working Group, , "Detailed Functional and Interface
              Standards for the NENA i3 Solution", 2016,
              <https://www.nena.org/page/i3_Stage3>.

Authors' Addresses

   Randall Gellens
   Core Technology Consulting
   US

   Email: rg+ietf@coretechnologyconsulting.com
   URI:   http://www.coretechnologyconsulting.com


   Brian Rosen
   470 Conrad Dr
   Mars, PA   16046
   US

   Email: br@brianrosen.net