ecrit B. Rosen
Internet-Draft NeuStar
Expires: April 26, 2006 October 23, 2005

Emergency Call Information in the Domain Name System
draft-rosen-dns-sos-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire on April 26, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

Location of a caller is essential to processing an emergency call. Location is needed to correctly route the call, and to correctly dispatch help to the right place. Location can be specified in geographic (latitude, longitude) or civic (country, province, locality) forms. This document proposes a DNS-based mechanism to lookup emergency calling URIs and related emergency information from a known civic location in a specific form. Other companion documents propose a non DNS-based approach to determine civic location from geographic location, and describe how to discover a civic location in

the appropriate local form(s) for this application.

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 [RFC2119].

2. What's Changed

Version 2

Minor refresh to keep proposal alive

Version 1

Major simplifications have been made to this version from the initial.

The contents of proposed entries in the DNS has been simplified to several NAPTRs; no new DNS objects are proposed, and specifically, the proposed POLY object is replaced with a NAPTR to a boundary description document in XML.

3. Problem

Placing an emergency call to get help depends on location = where the caller is located at the time of the call. Location is needed for two fundamental reasons:

1. To determine which Public Safety Answering Point (PSAP) also known as an Emergency Communications Center (ECC) to direct the call to.
2. To direct responders (police, fire, ambulance) to the caller.

Location, within the context of emergency calls, can be expressed in two different forms, geographic (geo) - latitude, longitude, altitude and civic - county, province or state, city, ...

Determining the correct PSAP is not trivial. PSAPs have service boundaries. If a caller is inside the service boundary, that PSAP should get the call. Nearest PSAP, home PSAP or other, simpler mechanisms will not work. One must either know, from some kind of authenticated database, the PSAP that serves a given civic address, or have a geo location and use a network service or local algorithm to determine the correct PSAP from the geographic coordinates. (For example, a service may know the service boundaries for a region and compare the location of the caller with all of the PSAP service boundaries to determine which boundary the geo location falls

within.) There are about 6,000 PSAPs in North America, and perhaps 3 times that number in the rest of the world (ed note, anyone have a better number?).

With the advent of Voice over IP, the Internet presents daunting problems to emergency calls because users can be anywhere in the world relative to the elements that are processing the call. Consider for example, a user sitting in a cafe' in Chicago with a laptop connected to the Internet via a hotspot, communicating with her employer's SIP proxy through a VPN tunnel. An accident occurs and the patron calls for help. What if the employer is in Sierra Leone, and has Sierra Leone based VoIP service provider? The employer's proxy server must determine, based on the actual location of the user, that the PSAP is in Chicago!

In processing a call to an PSAP using a protocol such as SIP [RFC3261], a routing element must determine the location of the caller, and depending on the form of the location either have access to all the PSAP service boundaries, run an intersection algorithm between a geo location of the caller and all possible PSAP boundaries, or have a civic address and a database that contains the PSAP that serves that address. Having determined the correct PSAP, the routing element must forward the call to it (which implies knowing the URI of that PSAP). At present, there is no standard mechanism to discover the correct PSAP from either civil or geographic addresses.

Once the correct PSAP is determined, the call will be forwarded to it. The PSAP will then answer the call, and determine what response is required. The responders are then dispatched to the location of the caller. Dispatch is typically based on civic location. If the location is reported by the caller in geo form, it must be translated to civic form in the PSAP, which requires an accurate translation database.

Each of the responders (e.g. police, fire, emergency medical) have their own service boundaries, and they do not correspond to the service boundary of the PSAP. A mechanism is needed to publish responder service boundaries.

If location is available as a civic, access to a database that enumerates all known street addresses is used to validate the address prior to its being used for an emergency call. This database (called a "Master Street Address Guide" or "MSAG") must be made available to the entities that supply location to the endpoints. Validation against the MSAG is essential because there are many variations in naming locations (First Street vs 1st Street, New York Avenue Northwest, vs New York Ave. NW). Accurate dispatch requires

uniformity of reporting civic addresses, and thus all addresses must be verified against some form of the MSAG prior to an emergency. This implies the MSAG, which in some areas is commonly available to PSTN carriers and in use by PSAPs, must be more publicly available.

Organizing PSAPs and responders is a government function. Governments determine where boundaries are, how coverage is handled in less populated areas, etc. In smaller countries, the national government organizes the entire system. More commonly, while some aspects are organized and regulated at the national level, much of the organization is delegated to state/province/district level, and often further delegation to country and/or city/township level is done. Any organization of the data here must mirror this delegation. On the other hand, for historical reasons, many service boundaries do not follow government entity boundaries. Therefore, there is not necessarily a correlation between the delegation boundaries and the service boundaries.

There are areas of the world that are disputed - more than one country claims the area as part of its territory. This gives rise to multiple PSAPs having a service boundary including disputed territory. While such areas are few and relatively small, the problem exists and must be accounted for in the design of systems and databases.

4. Overview of the Solution

SIP has been extended to carry a location object [REF]. Emergency calls will be required to include this object in the first message (INVITE) of an emergency call. The location can be determined by a measurement method (such as a Global Positioning Satellite (GPS) receiver in the endpoint, or the endpoint can learn its location from the local infrastructure using, for example, the location option of Dynamic Host Configuration Protocol (DHCP) [REF].

We propose to use the Domain Name System (DNS) to hold a hierarchy of civic locations. We think the DNS is particularly appropriate for this purpose because of its delegation mechanism, which we will show matches the need very closely. Starting at the root sos.arpa (sos being the universal symbol for emergency), we propose that the next level be a two-character iso country code, e.g. au.sos.arpa. We propose that an international agency be delegated the sos.arpa domain, and that it delegate au.sos.arpa to an agency selected by the government of Australia. The national agency can, if appropriate, make further delegations. For example, there might be a domain such as pittsburgh.allegheny.pa.us.sos.arpa representing the City of Pittsburgh, Allegheny County, in the Commonwealth (state) of

Pennsylvania, in the United States. A city could, for example, create subdomains in its domain representing streets, and within those street domains, subdomains for addresses. For example, we might find an entry at 123.main.pittsburgh.allegheny.pa.us.sos.arpa. There is no requirement for each subdomain in a domain to have the same semantics (for example, rural and urban areas might use different parallel civic location schemes). Nor is there a requirement for a particular level of hierarchy within two different countries or regions to share the same semantics.

The contents of the domains are primarily Naming Authority Pointers (NAPTRs) [RFC2915]. For example, some of these domains may have NAPTR records representing the service URIs for the PSAP or responders that cover that boundary. These may exist at any level.

Besides NAPTRs that represent service boundaries for PSAPs or responders, there can also be NAPTRs to additional information. These NAPTRs are expected to resolve to HTPPS URLs which point to XML documents with specific semantics. This document describes several such NAPTRs:

o a pointer to a document containing a set of polygons: each a sequence of geospatial coordinates describing the boundary of a domain;
o a pointer to a list of subdomains of a domain to facilitate searching;
o a pointer to a set of information about a structure (building) provided by the actual owner of the domain, and not essential for routing or dispatch, but potentially usefull for the PSAP and responder. For example, an after hours contact;

For location information within a building, a city or township may delegate a street address to a building owner. In turn, the building owner may delegate subdomains to suite tenants. The tenant, or building owner, would enter floor subdomains, and within those, room domains. For example, one might find a entry at 235-5.5.123.main.pittsburgh.allegheny.pa.us.sos.arpa representing cubicle 235-5 on the 5th floor of 123 Main Street. Interior information is optional, and intended for non-private data.

Of course, any administrative entity in the hierarchy could contract with a registrar to manage the delegation of its subdomains if it so chose. It could also create an administrative mechanism to obtain lower level data, and publish lower levels itself, rather than delegate.

We note that the actual meaning of any level in this hierarchy is not defined, and the number of levels is not significant. What matters is that the names mean something to the (human) dispatcher and

responder and there is a reasonably consistant style within larger (e.g. country) levels that facilitates construction of a query string from a location representation.

Creation of the database may look daunting, but in many areas it already exists, albeit in different forms. The hierarchical nature of DNS can simplify the data that needs to be assembled where the data does not yet exist. In many cases, PSAP boundaries actually are aligned to political boundaries. A large city, for example, typically has only one PSAP, whose service boundary matches the city boundary. Thus, street level information is not needed for a civic location to find the serving PSAP, if the city entry has an PSAP NAPTR. It is common for an PSAP to serve more than one township or smaller city, but the mechanism would work equally well for such a circumstance. There are some circumstances where PSAP boundaries do not align well. Some PSAPs only serve a part of a city, and an adjacent PSAP serves the remainder. The basic mechanism works quite well, because an PSAP NAPTR can be put in the upper level domain that covers the majority of the served area, and only subdomains for exception, either within the majority area -- all except these streets -- or within the minority area -- all plus these streets, need be populated with domains containing the correct PSAP NAPTR. It is also possible for a routing proxy to be designated as the PSAP for an entire city, state, or even a country, and for that proxy to have the information needed to determine which PSAP serves the caller location, forwarding the call to it.

Clearly, the existence of a street address entry indicates a valid civic Location. The jurisdiction responsible for defining valid addresses within its domain would enter its preferred spelling/ representation of that name. Any entity assigning civic locations would verify an address by looking it up in the sos.arpa tree. In this regard, the tree is the MSAG. Alternate spellings, and alternate forms of the address (for example, a postal address) can also be placed in the sos.arpa tree, with a CNAME element pointing to the correctly spelled DNS entry.

For locations provided in geo form, we propose that the sos.arpa domain have entries for each PSAP, which contains a NAPTR with the URI to reach that PSAP and a NAPTR with the polygon lists defining its service boundaries. For convenience, we define a mechanism for a DNS name server to accept a query with a lat/lon/altitude as two name components and return the URI of the PSAP boundary the lat/lon/ altitude lies within.

5. The SOS Application Specifications

The following text is based on the equivalent text in [RFC2916].

This template defines the SOS DDDS Application according to the rules and requirements found in [RFC3402]. The DDDS database used by this Application is found in [RFC3403] which is the document that defines the NAPTR DNS Resource Record type.

5.1. Application Unique String

The Application Unique String for a civic location expressed as a series of increasingly specific regions starting at national (country), with the components separated by periods, and in reverse order (i.e., country code appears just to the left of "sos.arpa").

There is no significance to the meaning of the components as long as the civic location is interpretable by residents in the specified location, and they are in increasingly specific. Implementations SHOULD use the components listed in [DHCP civic ref] to allow direct mapping between locations reported by DHCP and locations in the DNS.

Where local convention omits levels of hierarchy that are required in other regions within a country (for example, use of county in some provinces but not in others), the omitted element would be specified as ".null".

The application unique string for a geo location is expressed by placing latitude, longitude and altitude (in decimal degrees/meters) as three components (left to right), dot separatated and appending ".geo". The character "d" is used as the separator between the whole and fractional part of the degree/meter.

5.2. First Well Known Rule

The First Well Known Rule for this Application is the identity rule. The output of this rule is the same as the input. This is because this Application's databases are organized in such a way that it is possible to go directly from the name to the smallest granularity of the namespace directly from the name itself.

5.3. Expected Output

The output of the last DDDS loop is a set of Uniform Resource Identifiers in absolute form according to the 'absoluteURI' production in the Collected ABNF found in [RFC2396].

5.4. Valid Databases

At present only one DDDS Database is specified for this Application. "Dynamic Delegation Discovery System (DDDS) Part Three: The DNS

Database [RFC3403] specifies a DDDS Database that uses the NAPTR DNS resource record to contain the rewrite rules. The Keys for this database are encoded as domain-names.

The output of the First Well Known Rule for the SOS Application is the input string with the string "sos.arpa" appended.

This domain-name is used to request NAPTR records which may contain the end result or, if the flags field is blank, produces new keys in the form of domain-names from the DNS.

The character set used to encode the substitution expression is UTF-8. The allowed input characters are and the characters allowed to be in a Key are those that are currently defined for DNS domain-names. Spellings SHOULD use local conventions, but MUST match the same conventions used for DHCP reported location.

5.4.1. Flags

This Database contains a field that contains flags that signal when the DDDS algorithm has finished. At this time only one flag, "U", is defined. This means that this Rule is the last one and that the output of the Rule is a URI. See [RFC3403].

If a client encounters a record with an unknown flag, it MUST ignore it and move to the next Rule. This test takes precedence over any ordering since flags can control the interpretation placed on fields. A novel flag might change the interpretation of the regexp and/or replacement fields such that it is impossible to determine if a record matched a given target.

If this flag is not present then this rule is non-terminal. If a Rule is non-terminal, then clients MUST use the Key produced by this Rewrite Rule as the new Key in the DDDS loop (i.e., causing the client to query for new NAPTR records at the domain-name that is the result of this Rule).

5.4.2. Services Parameters

Service Parameters for this Application take the following form and are found in the Service field of the NAPTR record.

```
service_field = "SOS" 1*(servicespec)
servicespec   = "+" sosservice
sosservice    = type 0*(subtypespec)
subtypespec   = ":" subtype
type          = 1*32(ALPHA / DIGIT)
subtype       = 1*32(ALPHA / DIGIT)
```


•

In other words, a non-optional "SOS" (used to denote SOS-only Rewrite Rules in order to mitigate record collisions) followed by 1 or more or more sosservices which indicate what class of functionality a given end point offers. Each sosservice is indicated by an initial '+' character.

No use for subtypes is presently contemplated, but is left defined as in [RFC2916] for possible future use.

5.4.2.1. SOS Services

sosservice specifications contain the functional specification (i.e., what it can be used for), the valid protocols, and the URI schemes that may be returned. Note that there is no implicit mapping between the textual string "type" or "subtype" in the grammar for the sosservice and URI schemes or protocols. The mapping, if any, must be made explicit in the specification for the sosservice itself. A registration of a specific Type also has to specify the Subtypes allowed.

The registration mechanism is specified in Section 6.

5.5. What constitutes an 'Sos Resolver'?

The algorithm defined above always returns a single rule. Specific applications may have application-specific knowledge or facilities that allow them to present multiple results or speed selection, but these should never change the operation of the algorithm.

6. Registration mechanism for sosservices

As specified in the ABNF found in Section 5.4.2, an 'sosservice' is made up of 'types' and 'subtypes'. For any given 'type', the allowable 'subtypes' must be specified in the registration. There is currently no concept of a registered 'subtype' outside the scope of a given 'type'. Thus, the registration process uses the 'type' as the main key within the IANA Registry. While the combination of each type and all of its subtypes constitutes the allowed values for the 'enumservice' field, it is not sufficient to simply document those values. A complete registration will also include the allowed URI schemes, a functional specification, security considerations, intended usage, and any other information needed to allow for interoperability within the application. In order to be a registered sos service, the entire specification, including the template, requires publication of the sosservice registration specification as an RFC.

•

6.1. Registration Requirements

Service registration proposals are all expected to conform to various requirements laid out in the following sections.

6.1.1. Functionality Requirement

A registered sosservice must be able to function as a selection mechanism when choosing one NAPTR resource record from another. That means that the registration MUST specify what is expected when using that very NAPTR record, and the URI that is the outcome of the use of it.

6.1.2. Naming requirement

An sosservice MUST be unique in order to be useful as a selection criteria. Since an sosservice is made up of a type and a type-dependent subtype, it is sufficient to require that the 'type' itself be unique. The 'type' MUST be unique, and conform to the ABNF specified in Section 5.4.2.

The subtype, being dependent on the type, MUST be unique within a given 'type'. It must conform to the ABNF specified in Section 5.4.2. The subtype for one type MAY be the same as a subtype for a different registered type but it is not sufficient to simply reference another type's subtype. The function of each subtype must be specified in the context of the type being registered.

6.1.3. Security requirement

An analysis of security issues is required for all registered sosservices. (This is in accordance with the basic requirements for all IETF protocols.) In most cases, it is expected that the security considerations will be the same as those services defined in this memo, but new services could have different security considerations.

All descriptions of security issues must be as accurate as possibly regardless of registration tree. In particular, a statement that there are "no security issues associated with this sosservice" must not be confused with "the security issues associated with this sosservice have not been assessed".

There is no requirement that an sosservice must be secure or completely free from risks. Nevertheless, all known security risks must be identified in the registration of an sosservice.

The security considerations section of all registrations is subject to continuing evaluation and modification.

6.1.4. Publication Requirements

Proposals for sosservice registrations MUST be published as an RFC.

6.2. Registration procedure

6.2.1. IANA Registration

IANA will register the sosservice and make the sosservice registration available to the community in addition to the RFC/BCP publication.

6.2.1.1. Location of sosservice Registrations

sosservice registrations will be published in the IANA repository and made available via anonymous FTP at the following URI: "ftp://ftp.iana.org/assignments/sos-services/".

6.2.1.2. Change Control

Change control of sosservice stay with the IETF via the RFC publication process. sosservice registrations may not be deleted; sosservice which are no longer believed appropriate for use can be declared OBSOLETE by publication of a new RFC and a change to their "intended use" field; such sosservices will be clearly marked OBSOLETE in the lists published by IANA.

Registration Template
   sosservice Type:
   sosservice Subtype(s):
   URI Scheme(s):
   Functional Specification:
   Security considerations:
   Intended usage: (One of COMMON, LIMITED USE or OBSOLETE)
   Author:
   Any other information that the author deems interesting:

Note: In the case where a particular field has no value, that field is left completely blank, especially in the case where a given type has no subtypes.

6.2.2. Initial Registrations

The following services are defined in this memo

Type sos+PSAP

   Subtypes: none
   URI Schemes: sips: [RFC3261] and tel: [RFC2806]
   Functional Specification: Provides a contact uri for the emergency call center (public safety answering point) that serves the civic address corresponding to this DDDS entry. It is not necessary for

the uri to be the uri of the PSAP itself; it can be a uri of a proxy server which can route the call to the correct PSAP
Security considerations: As this URI reaches the PSAP, directly or indirectly, it can be a target for a denial of service attack.
Intended usage: COMMON
Author: Brian Rosen
Other Information: None

Type sos+fire
Subtypes: none
URI Schemes: sips: [RFC3261] and tel: [RFC2806]
Functional Specification: Provides a contact uri for the fire department/brigade that serves the civic address corresponding to this DDDS entry.
Security considerations: As this URI reaches the responder, directly or indirectly, it can be a target for a denial of service attack.
Intended usage: COMMON
Author: Brian Rosen
Other Information: In many jurisdictions, emergency calls should be routed to an PSAP rather than a specific service such as a direct call to the fire department/brigade. The agency can refuse such direct calls by, e.g. requiring authentication.

Type sos+rescue
Subtypes: none
URI Schemes: sips: [RFC3261] and tel: [RFC2806]
Functional Specification: Provides a contact uri for the rescue/ emergency medical service/ambulance service that serves the civic address corresponding to this DDDS entry.
Security considerations: As this URI reaches the responder, directly or indirectly, it can be a target for a denial of service attack.
Intended usage: COMMON
Author: Brian Rosen
Other Information: In many jurisdictions, emergency calls should be routed to an PSAP rather than a specific service such as a direct call to the rescue/EMS/ambulance service. The agency can refuse such direct calls by, e.g. requiring authentication.

Type sos+marine

Subtypes: none
URI Schemes: sips: [RFC3261] and tel: [RFC2806]
Functional Specification: Provides a contact uri for the maritime rescue service that serves the civic address corresponding to this DDDS entry.
Security considerations: As this URI reaches the responder, directly or indirectly, it can be a target for a denial of service attack.
Intended usage: COMMON
Author: Brian Rosen
Other Information: The concept of a "civic address" for a marine emergency is somewhat strange. Entries should be made in the DDDS for territory within a jurisdiction that is served by a maritime emergency response service. For example, one could have an entry such as 5.atlantic.us for the Coast Guard District 5 in the Atlantic region of the United States.

Type sos+police
Subtypes: none
URI Schemes: sips: [RFC3261] and tel: [RFC2806]
Functional Specification: Provides a contact uri for the police department that serves the civic address corresponding to this DDDS entry.
Security considerations: As this URI reaches the responder, directly or indirectly, it can be a target for a denial of service attack.
Intended usage: COMMON
Author: Brian Rosen
Other Information: In many jurisdictions, emergency calls should be routed to an PSAP rather than a specific service such as a direct call to the police. The agency can refuse such direct calls by, e.g. requiring authentication.

Type sos+mountain
Subtypes: none
URI Schemes: sips: [RFC3261] and tel: [RFC2806]
Functional Specification: Provides a contact uri for the mountain rescue service point that serves the civic address corresponding to this DDDS entry.
Security considerations: As this URI reaches the responder, directly or indirectly, it can be a target for a denial of service attack.
Intended usage: COMMON
Author: Brian Rosen

Other Information: In many jurisdictions, emergency calls should be routed to an PSAP rather than a specific service such as a direct call to the mountain rescue. The agency can refuse such direct calls by, e.g. requiring authentication.

Type sos+subdomain
Subtypes: none
URI Schemes: http or https [RFC2616]
Functional Specification: Pointer to an XML document as defined in Section 8 containing a list of subdomains. Facilitates searching the sos.arpa tree.
Security considerations: The DNS system is usually considered more secure against various forms of attack than most web servers. Thus, in situations where there are major disruptions to the Internet (which may be exactly when the data is most needed), the DNS may work, while the web server may not. Routing proxies SHOULD NOT assume that they can use this NAPTR to access the list of subdomains, at the time an emergency call is being routed.
Intended usage: COMMON
Author: Brian Rosen
Other Information: none.

Type sos+polygon
Subtypes: none
URI Schemes: http or https [RFC2616]
Functional Specification: Pointer to an XML document as defined in Section 7 containing a list of polygons describing the boundaries of psaps within the domain. May be protected by TLS if needed.
Security considerations: If the information must be kept private,

the document should be protected with TLS. Polygons representing boundaries within a building are often considered private and thus should be protected.
The DNS system is usually considered more secure against various forms of attack than most web servers. Thus, in situations where there are major disruptions to the Internet (which may be exactly when the data is most needed), the DNS may work, while the web server may not. Routing proxies SHOULD NOT assume that they can use this NAPTR to access the list of polygons, at the time an emergency call is being routed.
Intended usage: COMMON
Author: Brian Rosen
Other Information: none.

Type sos+structure

Subtypes: none
URI Schemes: http or https [RFC2616]
Functional Specification: Pointer to an XML document as defined in Section 9.
Security considerations: In many cases, this information is private and the document should be protected with TLS.
Intended usage: COMMON
Author: Brian Rosen
Other Information: none.

7. Polygon Document

The Polygon document MUST be a well-formed XML document meeting the following schema, which is derived from Geography Markup Language (GML) as defined by the OpenGIS Consortium [1].

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           targetNamespace="urn:ietf:params:xml:ns:sos-boundary"
    xmlns:gml="http://www.opengis.net/gml"
    xmlns:sos-boundary="urn:ietf:params:xml:ns:sos-boundary"
          elementFormDefault="qualified"
          attributeFormDefault="unqualified">
    <xs:import namespace="http://www.opengis.net/gml"
               schemaLocation="feature.xsd"/>
    <xs:import namespace="http://www.opengis.net/gml"
               schemaLocation="geometryPrimitives.xsd"/>
    <xs:sequence>
       <xs: complexType name="psap">
          <xs:element type="xsType:anyURI" name="psapURI"/>
          <xs:complexType name="boundary">
          <!--xs:restriction base="gml:AbstractFeatureType"-->
            <xs:sequence>
                <xs:sequence>
                    <xs:element ref="gml:boundedBy" minOccurs="0"/>
                </xs:sequence>
                <xs:sequence>
                    <xs:element ref="gml:extentOf"/>
                </xs:sequence>
             </xs:sequence>
```

```
          <!--/xs:restriction-->
          </xs:complexType>
        </xs:complexType>
      </xs:sequence>
   </xs:schema>
```


8. Subdomain Document

The subdomain document shall be a well-structured XML document accessed by HTTP or HTTPS. The schema of this document is:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
       targetNamespace="urn:ietf:params:xml:ns:sos-subdomain"
       xmlns:sos-sd="urn:ietf:params:xml:ns:sos-sd"
       elementFormDefault="qualified">
     <xs:element name="sos-subdomain">
             <xs:complexType>
                     <xs:list type="xs:anyURI" minOccurs="0"/>
             </xs:complexType>
     </xs:element>
</xs:schema>
```

9. Structure Document

The structure document shall be a well-structured XML document accessed by HTTP or HTTPS. The schema of this document is:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
        targetNamespace="urn:ietf:params:xml:ns:sos-structure"
        xmlns:sos-sd="urn:ietf:params:xml:ns:sos-sr"
        elementFormDefault="qualified">
     <xs:element name="sos-structure">
             <xs:complexType>
                     <TBD>
             </xs:complexType>
     </xs:element>
</xs:schema>
```

10. Resolving geo locations

Within any civic level (country, state/province, county, city>, a polygon NAPTR may occur. The URI points to a list of pairs of "psapUri" and "boundary" elements, where the URI is the target of any call within the boundary. In simple situations, a single boundary representing an entire country may exist at the country code level of the civic namespace, for example to.sos.arpa may have a polygon NAPTR with a single URI and boundary of the country. In the United States, it may be more convenient to put the polygons in the state and/or county levels.

Any element can use the subdomain NAPTR to "walk" the entire tree and discover all the polygon NAPTRs in the tree to produce a complete set of polygons. The element could then use standard techniques that can quickly determine which polygon a particular point lies within.

As a convenience, any name server can, if it chooses, do such a "walk", and subsequently resolve a query of the form: 101d221.93d0345.0.geo.sos.arpa, where the meaning of such a query would be to ask for the RRs (presumably, the PSAP NAPTR) for the geo 101.221 degrees latitude, 93.0354 degrees longitude and 0 meters altitude. Such a resolution is NOT standard DNS name server behavior, and clients cannot necessarily depend on their local name server providing resolution of such a query. Specifically, the "geo.sos,arpa" subdomain is NOT delegated to any entity, and an attempt to query with a valid geo using the .geo.sos.arpa tree with no name servers in the path that support the geo query will fail.

11. Notes and things to do

Need text on i18n names.

12. Security Considerations

Details of building interiors and structure documents may not be public data. Revealing this data to unauthorized users (PSAPs and responders) could provide attackers with information that could be exploited to burgle, inflict damage on, or otherwise do significant harm to the owners and occupants of the structure. Where the data is not public, accessing the data MUST be restricted to authorized entities using HTTPS.

If the data in the DNS is forged, or a man in the middle attack is mounted, emergency calls could be directed to the wrong place. The call could be directed to the wrong PSAP, could be directed to a valid URI which was not an PSAP, to a completely invalid URI. Worse the call could be directed to an entity impersonating an PSAP, which could leave the caller believing help was coming when in fact it was not.

Data in the DNS sos.arpa tree includes a URI that can directly or indirectly reach the PSAP, which may be used to mount a Denial of Service attack.

For these reasons, clients and servers SHOULD use protected services such as HTTPS and sips: which could authenticate that the destination is the desired one.

If the caller provides an incorrect location, the call could be directed to the wrong PSAP. An inadvertent error could be detected before a call by verifying that the call exists in the sos.arpa tree. Indeed validation of address is one of the reasons we propose that the address data be in a publicly accessible database.

13. Acknowledgements

This document has benefited greatly from numerous comments from both Henning Schulzrinne and Rohan Mahy.

14. Normative References

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

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC2535] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2806] Vaha-Sipila, A., "URLs for Telephone Calls", RFC 2806, April 2000.

[RFC2915] Mealling, M. and R. Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record", RFC 2915, September 2000.

[RFC2916] Faltstrom, P., "E.164 number and DNS", RFC 2916, September 2000.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3402] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm", RFC 3402, October 2002.

[RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.

•

[1] <http://www.opengis.org>

•

Author's Address

Brian Rosen
NeuStar
470 Conrad Dr.
Mars, PA 16046
US

Phone: +1 724 382 1051
Email: br@brianrosen.net

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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