                Requirements for Emergency Context Resolution with
                              Internet Technologies

Status of This Memo

   This memo provides information for the Internet community. It does
   not specify an Internet standard of any kind. Distribution of this
   memo is unlimited.

Abstract

   This document defines terminology and enumerates requirements for the
   context resolution of emergency calls placed by the public using
   voice-over-IP (VoIP) and general Internet multimedia systems, where
   Internet protocols are used end to end.

Table of Contents

1. Introduction

    Users of both voice-centric (telephone-like) and non-voice services,
    such as text communication for hearing-disabled users (see [RFC3351]
    and [toip]), expect to be able to initiate a request for help in case
    of an emergency.

    Unfortunately, the existing mechanisms to support emergency calls
    that have evolved within the public circuit-switched telephone
    network (PSTN) are not appropriate to handle evolving IP-based voice,
    text, and real-time multimedia communications. This document
    outlines the key requirements that IP-based end systems and network
    elements, such as Session Initiation Protocol (SIP) [RFC3261]
    proxies, need to satisfy in order to provide emergency call services,
    which at a minimum, offer the same functionality as existing PSTN
    services, with the additional overall goal of making emergency
    calling more robust, less costly to implement, and multimedia-
    capable.

    This document only focuses on end-to-end IP-based calls, i.e., where
    the emergency call originates from an IP end system and terminates in
    an IP-capable public safety answering point (PSAP), conveyed entirely
    over an IP network.

    We first define terminology in Section 3. The document then outlines
    various functional issues that relate to placing an IP-based
    emergency call, including a description of baseline requirements
    (Section 5), identification of the emergency caller's location
    (Section 6), use of a service identifier to declare a call to be an
    emergency call (Section 7), and finally, the mapping function
    required to route the call to the appropriate PSAP (Section 8).

    The primary purpose of the mapping protocol is to produce a PSAP URI
    drawn from a preferred set of URI schemes such as SIP or SIPS URIs,
    based on both location information [RFC4119] and a service identifier
    in order to facilitate the IP end-to-end completion of an emergency
    call.

    Aside from obtaining a PSAP URI, the mapping protocol is useful for
    obtaining other information as well. There may be a case, for
    example, where an appropriate emergency number is not known, only the
    location. The mapping protocol can then return a geographically
    appropriate emergency number based on the input.

Since some PSAPs may not immediately support IP, or because some user
equipment (UE) may not initially support emergency service
identifiers, it may be necessary to also support emergency service
identifiers that utilize less-preferred URI schemes, such as a tel
URI in order to complete an emergency call via the PSTN.

Identification of the caller, while not incompatible with the
requirements for messaging outlined within this document, is
considered to be outside the scope of this document.

Location is required for two separate purposes: first, to support the
routing of the emergency call to the appropriate PSAP and second, to
display the caller's location to the call taker to help in
dispatching emergency assistance to the appropriate location.

This latter use, the display of location information to the PSAP, is
orthogonal to the mapping protocol, and is outside the scope of this
document.

2. Requirements 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 RFC 2119 [RFC2119],
with the important qualification that, unless otherwise stated, these
terms apply to the design of the mapping protocol, not its
implementation or application.

3. Terminology

3.1. Emergency Services

Basic emergency service: Basic emergency service allows a caller to
   reach a PSAP serving its current location, but the PSAP may not be
   able to determine the identity or geographic location of the
   caller, except by the call taker asking the caller.

Enhanced emergency service: In enhanced emergency service, the PSAP
   call taker can determine the caller's current location.

3.2. Service Providers

Internet Access Provider (IAP): An organization that provides
   physical and data link (layer 2) network connectivity to its
   customers or users, e.g., through digital subscriber lines, cable
   TV plants, Ethernet, leased lines, or radio frequencies. Examples
   of such organizations include telecommunication carriers,

municipal utilities, larger enterprises with their own network
infrastructure, and government organizations, such as the
military.

Internet Service Provider (ISP): An organization that provides IP
network-layer services to its customers or users. This entity may
or may not provide the physical-layer and data link (layer-2)
connectivity, such as fiber or Ethernet, i.e., it may or may not
play the role of an IAP.

Application Service Provider (ASP): The organization or entity that
provides application-layer services, which may include voice (see
"Voice Service Provider"). This entity can be a private
individual, an enterprise, a government, or a service provider.
An ASP is more general than a Voice Service Provider, since
emergency calls may use other media beyond voice, including text
and video. For a particular user, the ASP may or may not be the
same organization as his IAP or ISP.

Voice Service Provider (VSP): A specific type of Application Service
Provider that provides voice related services based on IP, such as
call routing, a SIP URI, or PSTN termination. In this document,
unless noted otherwise, any reference to "Voice Service Provider"
or "VSP" may be used interchangeably with "Application/Voice
Service Provider" or "ASP/VSP".

3.3. Actors

(Emergency) caller: The term "caller" or "emergency caller" refers
to the person placing an emergency call or sending an emergency
instant message (IM).

User Equipment (UE): User equipment is the device or software
operated by the caller to place an emergency call. A SIP user
agent (UA) is an example of user equipment.

Call taker: A call taker is an agent at the PSAP that accepts calls
and may dispatch emergency help. Sometimes the functions of call
taking and dispatching are handled by different groups of people,
but these divisions of labor are not generally visible to the
caller and thus do not concern us here.

3.4. Call Routing Entities

   Emergency Service Routing Proxy (ESRP): An ESRP is an emergency call
      routing support entity that invokes the location-to-PSAP URI
      mapping function, to return an appropriate PSAP URI, or the URI
      for another ESRP. Client mapping requests could also be performed
      by a number of entities, including entities that instantiate the
      SIP proxy role and the SIP user agent client role.

   Public Safety Answering Point (PSAP): A PSAP is a facility where
      emergency calls are received under the responsibility of a public
      authority. (This terminology is used by both the European
      Telecommunications Standards Institute (ETSI), in ETSI SR 002 180,
      and the National Emergency Number Association (NENA).) In the
      United Kingdom, PSAPs are called Operator Assistance Centres; in
      New Zealand, Communications Centres. Within this document, it is
      assumed, unless stated otherwise, that PSAPs support the receipt
      of emergency calls over IP, using appropriate application layer
      protocols, such as SIP for call signaling and RTP for media.

3.5. Location

   Location: A geographic identification assigned to a region or
      feature based on a specific coordinate system, or by other precise
      information such as a street number and name. It can be either a
      civic or geographic location.

   Civic location: A described location based on some reference system,
      such as jurisdictional region or postal delivery grid. A street
      address is a common example of a civic location.

   Geographic location: A reference to a point that is able to be
      located, as described by a set of defined coordinates within a
      geographic coordinate system, such as latitude and longitude
      within the WGS-84 datum. For example, a 2-D geographic location
      is defined as an (x,y) coordinate value pair according to the
      distance north or south of the equator and east or west of the
      prime meridian.

   Location validation: A caller location is considered valid if the
      civic or geographic location is recognizable within an acceptable
      location reference system (e.g., United States Postal Address or
      the WGS-84 datum) and can be mapped to one or more PSAPs. While
      it is desirable to determine that a location exists, validation
      may not ensure that such a location exists, but rather may only

ensure that the location falls within some range of known values.
Location validation ensures that a location is able to be
referenced for mapping, but makes no assumption about the
association between the caller and the caller's location.

3.6. Identifiers, Numbers, and Dial Strings

   (Emergency) service number: The (emergency) service number is a
      string of digits used to reach the (emergency) service. The
      emergency service number is often just called the emergency
      number. It is the number typically dialed on devices directly
      connected to the PSTN and the number reserved for emergency calls
      by national or regional numbering authorities. It only contains
      the digits 0 through 9, #, and *. The service number may depend
      on the location of the caller. For example, the general emergency
      service number in the United States is 911 and the poison control
      service number is 18002221222. In most cases, the service number
      and dial string are the same; they may differ in some private
      phone networks. A service number may be carried in tel URLs
      [RFC3966], along with a context identifier. In the North American
      numbering plan, some service numbers are three-digit N11 or
      service codes, but not all emergency numbers have three digits. A
      caller may have to dial a service dial string (below) that differs
      from the service number when using a PBX.

   (Emergency) service dial string: The service dial string identifies
      the string of digits that a caller must dial to reach a particular
      (emergency) service. In devices directly connected to the PSTN,
      the service dial string is the same as the service number and may
      thus depend on the location of the caller. However, in private
      phone networks, such as in PBXs, the service dial string consists
      of a dialing prefix to reach an outside line, followed by the
      emergency number. For example, in a hotel, the dial string for
      emergency services in the United States might be 9911. Dial
      strings may contain indications of pauses or wait-for-secondary-
      dial-tone indications. Service dial strings are outside the scope
      of this document.

   (Emergency) service identifier: The (emergency) service identifier
      describes the emergency service, independent of the user interface
      mechanism, the signaling protocol that is used to reach the
      service, or the caller's geographic location. It is a protocol
      constant and used within the mapping and signaling protocols. An
      example is the service URN [RFC5031].

(Emergency) service URL: The service URL is a protocol-specific
   (e.g., SIP) or protocol-agnostic (e.g., im: [RFC3860]) identifier
   that contains the address of the PSAP or other emergency service.
   It depends on the specific signaling or data transport protocol
   used to reach the emergency service.

Service URN: A service URN is an implementation of a service
   identifier, which can be applied to both emergency and non-
   emergency contexts, e.g., urn:service:sos or
   urn:service:counseling. Within this document, service URNs are
   referred to as 'emergency service URNs' [RFC5031].

Home emergency number: A home emergency number is the emergency
   number valid at the caller's customary home location, e.g., his
   permanent residence. The home location may or may not coincide
   with the service area of the caller's VSP.

Home emergency dial string: A home dial string is the dial string
   valid at the caller's customary home location, e.g., his permanent
   residence.

Visited emergency number: A visited emergency number is the
   emergency number valid at the caller's current physical location.
   We distinguish the visited emergency number if the caller is
   traveling outside his home region.

Visited emergency dial string: A visited emergency dial string is
   the dial string number valid at the caller's current physical
   location.

3.7. Mapping

Mapping: Mapping is the process of resolving a location to one or
   more PSAP URIs that directly identify a PSAP, or point to an
   intermediary that knows about a PSAP and that is designated as
   responsible for serving that location.

Mapping client: A mapping client interacts with the mapping server
   to learn one or more PSAP URIs for a given location.

Mapping protocol: A protocol used to convey the mapping request and
   response.

Mapping server: The mapping server holds information about the
   location-to-PSAP URI mapping.

   Mapping service: A network service that uses a distributed mapping
      protocol to perform a mapping between a location and a PSAP, or
      intermediary that knows about the PSAP, and is used to assist in
      routing an emergency call.

4. Basic Actors

   In order to support emergency services covering a large physical
   area, various infrastructure elements are necessary, including
   Internet Access Providers (IAPs), Application/Voice Service Providers
   (ASP/VSPs), Emergency Service Routing Proxy (ESRP) providers, mapping
   service providers, and PSAPs.

   This section outlines which entities will be considered in the
   routing scenarios discussed.

```
     Location
     Information     +-----------------+
        |(1)         |Internet         |      +-----------+
        v            |Access           |      |           |
     +-----------+   |Provider         |      | Mapping   |
     |           |   |   (3)           |      | Service   |
     | Emergency |<---+-----------------+-->|           |
     | Caller    |   |  (2)            |      +-----------+
     |           |<---+-------+        |          ^
     +-----------+   |  +----|---------+------+   |
          ^         |  |  Location    |      |   |
          |         |  |  Information<-+      |   |
          |         +--+-------------+ |(5)   |   |   (6)
          |         |  |             |         |   |
          |         |  +----------v+ |   |   |
          |   (4)   |  |            |         |   |
     +-------------+--->|   ESRP    |<--+---+
          |         |  |            |     |
          |         |  +-----------+     |
          |         |       ^            |
          |         |   (7) |            |   +----+--+
          |   (8)   |       +-----------+-->|       |
     +-------------+---------------------->| PSAP  |
          |         |                    |   |       |
                    |Application/        |   +----+--+
                    |Voice               |
                    |Service             |
                    |Provider            |
                    +--------------------+
```
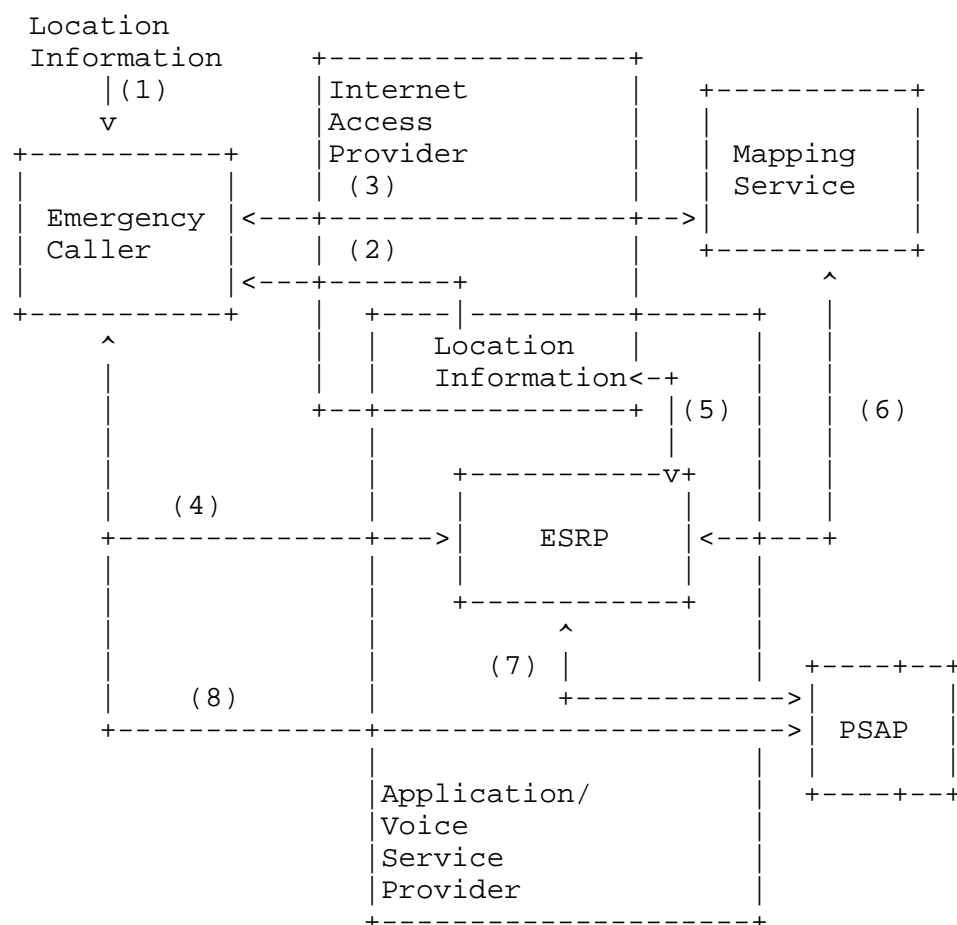
                Figure 1: Framework for Emergency Call Routing

Figure 1 shows the interaction between the entities involved in the
call. There are a number of different deployment choices, as can be
easily seen from the figure.

Is the Internet Access Provider also the Application/Voice Service
Provider? In the Internet today, the roles of Internet access
provider and application/voice service provider are typically
provided by different entities. As a consequence, the Application/
Voice Service Provider is typically not able to directly determine
the physical location of the emergency caller.

The overlapping squares in the figure indicate that some functions
can be collapsed into a single entity. As an example, the
Application/Voice Service Provider might be the same entity as the
Internet Access Provider. There is, however, no requirement that
this must be the case. Additionally, we consider that end systems
might act as their own ASP/VSP, e.g., either for enterprises or for
residential users.

Various potential interactions between the entities depicted in
Figure 1 are described below:

1. Location information might be available to the end host itself.

2. Location information might, however, also be obtained from the
    Internet Access Provider.

3. The emergency caller might need to consult a mapping service to
    determine the PSAP (or other relevant information) that is
    appropriate for the physical location of the emergency caller,
    possibly considering other attributes, such as appropriate
    language support by the emergency call taker.

4. The emergency caller might get assistance for emergency call
    routing by infrastructure elements that are emergency call
    routing support entities, such as an Emergency Service Routing
    Proxy (ESRP) in SIP.

5. Location information is used by emergency call routing support
    entities for subsequent mapping requests.

6. Emergency call routing support entities might need to consult a
    mapping service to determine where to route the emergency call.

7. For infrastructure-based emergency call routing (in contrast to
    UE-based emergency call routing), the emergency call routing
    support entity needs to forward the call to the PSAP.

   8. The emergency caller may interact directly with the PSAP, where
       the UE invokes mapping, and initiates a connection, without
       relying on any intermediary emergency call routing support
       entities.

5. High-Level Requirements

   Below, we summarize high-level architectural requirements that guide
   some of the component requirements detailed later in the document.

   Re1. Application/Voice service provider existence: The initiation
      of an IP-based emergency call SHOULD NOT assume the existence of
      an Application/Voice Service Provider (ASP/VSP).

      Motivation: The caller may not have an application/voice service
      provider. For example, a residence may have its own DNS domain
      and run its own SIP proxy server for that domain. On a larger
      scale, a university might provide voice services to its students
      and staff, but might not be a telecommunication provider.

   Re2. International applicability: Regional, political, and
      organizational aspects MUST be considered during the design of
      protocols and protocol extensions that support IP-based emergency
      calls.

      Motivation: It must be possible for a device or software developed
      or purchased in one country to place emergency calls in another
      country. System components should not be biased towards a
      particular set of emergency numbers or languages. Also, different
      countries have evolved different ways of organizing emergency
      services, e.g., either centralizing them or having smaller
      regional subdivisions, such as the United States or
      municipalities, handle emergency calls within their jurisdiction.

   Re3. Distributed administration: Deployment of IP-based emergency
      services MUST NOT depend on a single central administrative
      authority.

      Motivation: The design of the mapping protocol must make it
      possible to deploy and administer emergency calling features on a
      regional or national basis without requiring coordination with
      other regions or nations. The system cannot assume, for example,
      that there is a single global entity issuing certificates for
      PSAPs, ASP/VSPs, IAPs, or other participants.

Re4. Multi-mode communication: IP-based emergency calls MUST
    support multiple communication modes, including, for example,
    audio, video, and text.

    Motivation: Within the PSTN, voice and text telephony (often
    called TTY or text-phone in North America) are the only commonly
    supported media. Emergency calling must support a variety of
    media. Such media should include voice, conversational text (RFC
    4103 [RFC4103]), instant messaging, and video.

Re5. Mapping result usability: The mapping protocol MUST return one
    or more URIs that are usable within a standard signaling protocol
    (i.e., without special emergency extensions).

    Motivation: For example, a SIP URI that is returned by the mapping
    protocol needs to be usable by any SIP-capable phone within a SIP-
    initiated emergency call. This is in contrast to a "special
    purpose" URI, which may not be recognizable by a legacy SIP
    device.

Re6. PSAP URI accessibility: The mapping protocol MUST support
    interaction between the client and server where no enrollment to a
    mapping service exists or is required.

    Motivation: The mapping server may well be operated by a service
    provider, but access to the server offering the mapping must not
    require use of a specific ISP or ASP/VSP.

Re7. Common data structures and formats: The mapping protocol
    SHOULD support common formats (e.g., PIDF-LO) for location data.

    Motivation: Location databases should not need to be transformed
    or modified in any unusual or unreasonable way in order for the
    mapping protocol to use the data. For example, a database that
    contains civic addresses used by location servers may be used for
    multiple purposes and applications beyond emergency service
    location-to-PSAP URI mapping.

Re8. Anonymous mapping: The mapping protocol MUST NOT require the
    true identity of the target for which the location information is
    attributed.

    Motivation: Ideally, no identity information is provided via the
    mapping protocol. Where identity information is provided, it may
    be in the form of an unlinked pseudonym (RFC 3693 [RFC3693]).

6. Identifying the Caller's Location

   Location can either be provided directly (by value), or via a pointer
   (by reference), and represents either a civic location, or a
   geographic location. An important question is how and when to attach
   location information to the VoIP emergency signaling messages. In
   general, we can distinguish three modes of operation of how a
   location is associated with an emergency call:

   UA-inserted: The caller's user agent inserts the location
      information into the call-signaling message.

   UA-referenced: The caller's user agent provides a pointer (i.e., a
      location reference), via a permanent or temporary identifier, to
      the location information, which is stored by a location server
      somewhere else and then retrieved by the PSAP, ESRP, or other
      authorized entity.

   Proxy-inserted: A proxy along the call path inserts the location or
      location reference.

   The following requirements apply:

   Lo1. Reference datum: The mapping protocol MUST support the WGS-84
      coordinate reference system and MAY support other coordinate
      reference systems.

      Motivation: Though many different datums exist around the world,
      this document recommends the WGS-84 datum since it is designed to
      describe the whole earth, rather than a single continent or other
      region, and is commonly used to represent Global Positioning
      System coordinates.

   Lo2. Location delivery by-value: The mapping protocol MUST support
      the delivery of location information using a by-value method,
      though it MAY also support de-referencing a URL that references a
      location object.

      Motivation: The mapping protocol is not required to support the
      ability to de-reference specific location references.

   Lo3. Alternate community names: The mapping protocol MUST support
      both the jurisdictional community name and the postal community
      name fields within the PIDF-LO [RFC4119] data.

   Motivation: The mapping protocol must accept queries with either a
   postal or jurisdictional community name field, or both, and
   provide appropriate responses. If a mapping query contains only
   one community name and the database contains both jurisdictional
   and postal community names, the mapping protocol response SHOULD
   return both community names.

Lo4. Validation of civic location: The mapping protocol MUST be
   able to report the results of validating civic locations (street
   addresses).

   Motivation: Location validation provides an opportunity to help
   ascertain ahead of time whether or not a successful mapping to the
   appropriate PSAP will likely occur when it is required.
   Validation may also help to avoid delays during emergency call
   setup due to invalid location data.

Lo5. Information about location data used for mapping: The mapping
   protocol MUST support the ability to provide ancillary information
   about the resolution of location data used to retrieve a PSAP URI.

   Motivation: The mapping server may not use all the data elements
   in the provided location information to determine a match, or may
   be able to find a match based on all of the information except for
   some specific data elements. The uniqueness of this information
   set may be used to differentiate among emergency jurisdictions.
   Precision or resolution in the context of this requirement might
   mean, for example, explicit identification of the data elements
   that were used successfully in the mapping.

Lo6. Contact for location problems: The mapping protocol MUST
   support a mechanism to contact an appropriate authority to resolve
   mapping-related issues for the queried location. For example, the
   querier may want to report problems with the response values or
   indicate that the mapping database is mistaken on declaring a
   civic location as non-existent.

   Motivation: Initially, authorities may provide URLs where a human
   user can report problems with an address or location. In
   addition, web services may be defined to automate such reporting.
   For example, the querier may wish to report that the mapping
   database may be missing a newly built or renamed street or house
   number.

Lo7. Limits to validation: Successful validation of a civic
   location MUST NOT be required to place an emergency call.

Motivation: In some cases, a civic location may not be considered valid. This fact should not result in the call being dropped or rejected by any entity along the call setup signaling path to the PSAP.

Lo8. 3D sensitive mapping: The mapping protocol MUST implement support for both 2D and 3D location information, and MAY accept either a 2D or 3D mapping request as input.

Motivation: It is expected that queriers may provide either 2D or 3D data. When a 3D request is presented within an area only defined by 2D data within the mapping server, the mapping result would be the same as if the height or altitude coordinate had been omitted from the mapping request.

Lo9. Database type indicator: The mapping protocol MAY support a mechanism that provides an indication describing a specific type of location database used.

Motivation: It is useful to know the source of the data stored in the database used for location validation, either for civic or geographic location matching. In the United States, sources of data could include the United States Postal Service, the Master Street Address Guide (MSAG), or commercial map data providers.

7. Emergency Service Identifier

   Emergency service identifiers are protocol constants that allow protocol entities, such as SIP proxy servers, to distinguish emergency calls from non-emergency calls and to identify the specific emergency service desired. Emergency service identifiers are a subclass of service identifiers that more generally identify services reachable by callers. An example of a service identifier is the service URN [RFC5031], but other identifiers, such as tel URIs [RFC3966], may also serve this role during a transition period.

   Since this document only addresses emergency services, we use the terms "emergency service identifier" and "service identifier" interchangeably. Requirements for these identifiers include:

   Id1. Multiple emergency services: The mapping protocol MUST be able to support different emergency services distinguished by different service identifiers.

      Motivation: Some jurisdictions may offer multiple types of emergency services that operate independently and can be contacted directly; for example, fire, police, and ambulance services.

Id2. Extensible emergency service identifiers: The mapping protocol
   MUST support an extensible list of emergency identifiers, though
   it is not required to provide mappings for every possible service.

   Motivation: Extensibility is required since new emergency services
   may be introduced over time, either globally or in some
   jurisdictions. The availability of emergency services depends on
   the locations. For example, the Netherlands are unlikely to offer
   a mountain rescue service.

Id3. Discovery of emergency number: The mapping protocol MUST be
   able to return the location-dependent emergency number for the
   location indicated in the query.

   Motivation: Users are trained to dial the appropriate emergency
   number to reach emergency services. There needs to be a way to
   figure out the emergency number at the current location of the
   caller.

Id4. Home emergency number recognition: User equipment MUST be able
   to translate a home emergency number into an emergency service
   identifier.

   Motivation: The UE could be pre-provisioned with the appropriate
   information in order to perform such a translation or could
   discover the emergency number by querying the mapping protocol
   with its home location.

Id5. Emergency number replacement: There SHOULD be support for
   replacement of the emergency number with the appropriate emergency
   service identifier for each signaling protocol used for an
   emergency call, based on local conventions, regulations, or
   preference (e.g., as in the case of an enterprise).

   Motivation: Any signaling protocol requires the use of some
   identifier to indicate the called party, and the user equipment
   may lack the capability to determine the actual service URL (PSAP
   URI). The use of local conventions may be required as a
   transition mechanism. Since relying on recognizing local
   numbering conventions makes it difficult for devices to be used
   outside their home context and for external devices to be
   introduced into a network, protocols should use standardized
   emergency service identifiers.

Id6. Emergency service identifier marking: Signaling protocols MUST
   support emergency service identifiers to mark a call as an
   emergency call.

Motivation: Marking ensures proper handling as an emergency call
by downstream elements that may not recognize, for example, a
local variant of a logical emergency address. This marking
mechanism is related to, but independent of, marking calls for
prioritized call handling [RFC4412].

Id7. Handling unrecognized emergency service identifiers: There
MUST be support for calls that are initiated as emergency calls
even if the specific emergency service requested is not recognized
by the ESRP. Such calls will then be routed to a generic
emergency service.

Motivation: Fallback routing allows new emergency services to be
introduced incrementally, while avoiding non-routable emergency
calls. For example, a call for marine rescue services would be
routed to a general PSAP if the caller's location does not offer
marine rescue services yet.

Id8. Return fallback service identifier: The mapping protocol MUST
be able to report back the actual service mapped if the mapping
protocol substitutes another service for the one requested.

Motivation: A mapping server may be configured to automatically
look up the PSAP for another service if the user-requested service
is not available for that location. For example, if there is no
marine rescue service, the mapping protocol might return the PSAP
URL for general emergencies and include the "urn:service.sos"
identifier in the response to alert the querier to that fact.

Id9. Discovery of visited emergency numbers: The mapping protocol
MUST support a mechanism to allow the end device to learn visited
emergency numbers.

Motivation: Travelers visiting a foreign country may observe the
local emergency number, e.g., seeing it painted on the side of a
fire truck, and then rightfully expect to be able to dial that
emergency number. Similarly, a local "good Samaritan" may use a
tourist's cell phone to summon help.

8. Mapping Protocol

There are two basic approaches to invoke the mapping protocol. We
refer to these as caller-based and mediated. In each case, the
mapping client initiates a request to a mapping server via a mapping
protocol. A proposed mapping protocol, LoST, is outlined in [lost].

For caller-based resolution, the caller's user agent invokes the
mapping protocol to determine the appropriate PSAP based on the

location provided. The resolution may take place well before the
actual emergency call is placed, or at the time of the call.

For mediated resolution, an emergency call routing support entity,
such as a SIP (outbound) proxy or redirect server, invokes the
mapping service.

Since servers may be used as outbound proxy servers by clients that
are not in the same geographic area as the proxy server, any proxy
server has to be able to translate any caller location to the
appropriate PSAP. (A traveler may, for example, accidentally or
intentionally configure its home proxy server as its outbound proxy
server, even while far away from home.)

Ma1. Baseline query protocol: A mandatory-to-implement protocol
   MUST be specified.

   Motivation: An over-abundance of similarly capable choices appears
   undesirable for interoperability.

Ma2. Extensible protocol: The mapping protocol MUST be designed to
   support the extensibility of location data elements, both for new
   and existing fields.

   Motivation: This is needed, for example, to accommodate future
   extensions-to-location information that might be included in the
   PIDF-LO ([RFC4119]).

Ma3. Incrementally deployable: The mapping protocol MUST be
   designed to support its incremental deployment.

   Motivation: It must not be necessary, for example, to have a
   global street level database before deploying the system. It is
   acceptable to have some misrouting of calls when the database does
   not (yet) contain accurate PSAP service area information.

Ma4. Any time mapping: The mapping protocol MUST support the
   ability of the mapping function to be invoked at any time,
   including while an emergency call is in process and before an
   emergency call is initiated.

   Motivation: If the mapping query fails at call time, it may be
   advantageous to be able to fall back to the result of an earlier
   mapping query. This prior knowledge would be obtained by
   performing a mapping query at any time prior to an emergency call.

   Ma5. Anywhere mapping: The mapping protocol MUST support the
      ability to provide mapping information in response to an
      individual query from any (earthly) location, regardless of where
      the mapping client is located, either geographically or by network
      location.

      Motivation: The mapping client, such as an ESRP, may not
      necessarily be anywhere close to the caller or the appropriate
      PSAP, but must still be able to obtain mapping information.

   Ma6. Appropriate PSAP: The mapping protocol MUST support the
      routing of an emergency call to the PSAP responsible for a
      particular geographic area.

      Motivation: Routing to the wrong PSAP will result in delays in
      handling emergencies as calls are redirected, and therefore will
      also result in inefficient use of PSAP resources at the initial
      point of contact. It is important that the location determination
      mechanism not be fooled by the location of IP telephony gateways
      or dial-in lines into a corporate LAN (and dispatch emergency help
      to the gateway or campus, rather than the caller), multi-site LANs
      and similar arrangements.

   Ma7. Multiple PSAP URIs: The mapping protocol MUST support a method
      to return multiple PSAP URIs, which cover the same geographic
      area.

      Motivation: Different contact protocols (e.g., PSTN via tel URIs
      and IP via SIP URIs) may be routed to different PSAPs. Less
      likely, two PSAPs may overlap in their coverage region.

   Ma8. Single primary URI per contact protocol: Though the mapping
      protocol may be able to include multiple URIs in the response, it
      SHOULD return only one primary URI per contact protocol used, so
      that clients are not required to select among different targets
      for the same contact protocol.

      Motivation: There may be two or more URIs returned when multiple
      contact protocols are available (e.g., SIP and SMS). The client
      may select among multiple contact protocols based on its
      capabilities, preference settings, or availability.

   Ma9. Non-preferred URI schemes: The mapping protocol MAY support
      the return of a less-preferred URI scheme, such as a tel URI.

      Motivation: In order to provide incremental support to non-IP
      PSAPs, it may be necessary to be able to complete an emergency
      call via the PSTN.

Ma10. URI properties: The mapping protocol MUST support the ability
   to provide ancillary information about a contact that allows the
   mapping client to determine relevant properties of the PSAP URI.

   Motivation: In some cases, the same geographic area is served by
   several PSAPs; for example, a corporate campus might be served by
   both a corporate security department and the municipal PSAP. The
   mapping protocol should then return URIs for both, with
   information allowing the querying entity to choose one or the
   other. This determination could be made by either an ESRP, based
   on local policy, or by direct user choice, in the case of caller-
   based methods.

Ma11. Mapping referral: The mapping protocol MUST support a
   mechanism for the mapping client to contact any mapping server and
   be referred to another mapping server that is more qualified to
   answer the query.

   Motivation: Referrals help mitigate the impact of incorrect
   configuration that directs a client to the wrong initial mapping
   server.

Ma12. Split responsibility: The mapping protocol MUST support the
   division of data subset handling between multiple mapping servers
   within a single level of a civic location hierarchy.

   Motivation: For example, two mapping servers for the same city or
   county may handle different streets within that city or county.

Ma13. URL for error reporting: The mapping protocol MUST support
   the ability to return a URL that can be used to report a suspected
   or known error within the mapping database.

   Motivation: If an error is returned, for example, there needs to
   be a URL that points to a resource that can explain or potentially
   help resolve the error.

Ma14. Resilience to mapping server failure: The mapping protocol
   MUST support a mechanism that enables the client to fail over to
   different (replica) mapping server.

   Motivation: The failure of a mapping server should not preclude
   the mapping client from receiving an answer to its query.

Ma15. Traceable resolution: The mapping protocol SHOULD support the
   ability of the mapping client to be able to determine the entity
   or entities that provided the emergency address resolution
   information.

Motivation: To improve reliability and performance, it is
important to be able to trace which servers contributed to the
resolution of a query.

Ma16. Minimal additional delay: Mapping protocol execution SHOULD
minimize the amount of delay within the overall call-setup time.

Motivation: Since outbound proxies will likely be asked to resolve
the same geographic coordinates repeatedly, a suitable time-
limited caching mechanism should be supported.

Ma17. Freshness indication: The mapping protocol SHOULD support an
indicator describing how current the information provided by the
mapping source is.

Motivation: This is especially useful when an alternate mapping is
requested, and alternative sources of mapping data may not have
been created or updated with the same set of information or within
the same time frame. Differences in currency between mapping data
contained within mapping sources should be minimized.

9. Security Considerations

Threats and security requirements are discussed in a separate
document [RFC5069].

10. Contributors

The information in this document is partially derived from text
written by the following contributors:

Nadine Abbott   nabbott@telcordia.com

Hideki Arai   arai859@oki.com

Martin Dawson   Martin.Dawson@andrew.com

Motoharu Kawanishi   kawanishi381@oki.com

Brian Rosen   br@brianrosen.net

Richard Stastny   Richard.Stastny@oefeg.at

Martin Thomson   Martin.Thomson@andrew.com

James Winterbottom   James.Winterbottom@andrew.com

11. Acknowledgments

12. References

12.1. Normative References

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

12.2. Informative References

   [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.

   [RFC3351]   Charlton, N., Gasson, M., Gybels, G., Spanner, M., and A.
               van Wijk, "User Requirements for the Session Initiation
               Protocol (SIP) in Support of Deaf, Hard of Hearing and
               Speech-impaired Individuals", RFC 3351, August 2002.

   [RFC3693]   Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and
               J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

   [RFC3860]   Peterson, J., "Common Profile for Instant Messaging
               (CPIM)", RFC 3860, August 2004.

   [RFC3966]   Schulzrinne, H., "The tel URI for Telephone Numbers",
               RFC 3966, December 2004.

   [RFC4103]   Hellstrom, G. and P. Jones, "RTP Payload for Text
               Conversation", RFC 4103, June 2005.

   [RFC4119]   Peterson, J., "A Presence-based GEOPRIV Location Object
               Format", RFC 4119, December 2005.

   [RFC4412]   Schulzrinne, H. and J. Polk, "Communications Resource
               Priority for the Session Initiation Protocol (SIP)",
               RFC 4412, February 2006.

   [RFC5031]   Schulzrinne, H., "A Uniform Resource Name (URN) for
               Emergency and Other Well-Known Services", RFC 5031,
               January 2008.

   [RFC5069]   Taylor, T., Ed., Tschofenig, H., Schulzrinne, H., and M.
               Shanmugam, "Security Threats and Requirements for
               Emergency Call Marking and Mapping", RFC 5069,
               January 2008.

   [lost]   Hardie, T., "LoST: A Location-to-Service Translation
               Protocol", Work in Progress, August 2007.

   [toip]   Wijk, A. and G. Gybels, "Framework for real-time text over
               IP using the Session Initiation Protocol (SIP)", Work
               in Progress, August 2006.

Authors' Addresses

   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

   Roger Marshall (editor)
   TeleCommunication Systems, Inc.
   2401 Elliott Avenue
   2nd Floor
   Seattle, WA 98121
   US

   Phone: +1 206 792 2424
   EMail: rmarshall@telecomsys.com
   URI: http://www.telecomsys.com

Full Copyright Statement

Intellectual Property