ECRIT H. Schulzrinne
Internet-Draft Columbia U.
Expires: November 3, 2006 R. Marshall, Ed.
TCS
May 2, 2006

Requirements for Emergency Context Resolution with Internet Technologies
draft-ietf-ecrit-requirements-08.txt

Status of this Memo

Copyright Notice

Abstract

This document 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 type services (e.g., text communication for hearing disabled users (RFC 3351 [8]) have an expectation 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 SIP 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 into an IP-capable PSAP, conveyed entirely over an IP network.

This document outlines the various functional issues which relate to placing an IP-based emergency call, including a description of baseline requirements (Section 4), identification of the emergency caller's location (Section 5), use of an emergency identifier to declare a call to be an emergency call (Section 6), and finally, the mapping function required to route the call to the appropriate PSAP (Section 7).

Ideally, the mapping protocol would yield a URI from a preferred set of URIs (e.g., SIP:URI, SIPS:URI) which would allow an emergency call to be completed using IP end-to-end. Despite this goal, some PSAPs may not immediately have IP based connectivity, and therefore it is imperative that the URI scheme not be fixed, in order to ensure support for a less preferred set of URIs such as, for example, a TEL URI which may be used to complete a 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 the ECRIT charter.

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

As used in this document, validation of location does not require

that we ascertain as to whether or not the location actually exists. For example, validation might only check that the house number in a civic address falls within the assigned range, not whether a building, known by a specific building number, exists at that location. However, such higher precision validation is desirable.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [1], with the qualification that unless otherwise stated these words apply to the design of the mapping protocol, not its implementation or application.

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

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.

Basic Emergency Service: Basic Emergency Service allows a user 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 having the call taker ask the caller.

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 outside and thus do not concern us here.

Civic location: A described location based on some defined grid, such as a jurisdictional, postal, metropolitan, or rural reference system, (e.g., street address).

Emergency address: The URI (e.g., SIP:URI, SIPS:URI, XMPP:URI, IM: URI, etc.) which represents the address of the PSAP useful for the completion of an emergency call.

Emergency call routing support: An intermediary function which assists in the routing of an emergency call via IP. An ESRP is an example of an Emergency call routing support entity.

Emergency caller: The user or user device entity which sends his/her location to another entity in the network.

Emergency identifier: An identifier that marks a call as an emergency call.

Emergency Service Routing Proxy (ESRP): An ESRP is an emergency call routing support entity that invokes the location-to-PSAP URI mapping, to return either the URI for the appropriate PSAP, or the URL for another ESRP. (In a SIP system, the ESRP would typically be a SIP proxy, but may also be a Back-to-back user agent (B2BUA)).

Enhanced emergency service: Enhanced emergency services add the ability to identify the caller's identity or location to basic emergency services. (Sometimes, only the caller location may be known, e.g., when a call is placed from a public access point that is not owned by an individual.)

Geographic location: A reference to a locatable point described by a set of defined coordinates within a geographic coordinate system, (e.g., lat/lon within the WGS-84 datum). For example, (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.

Home emergency dial string: A home emergency dial string represents a (e.g., dialed) sequence of digits, that is used to initiate an emergency call within a geographically correct location of a caller if it is considered to be a user's "home" location or vicinity.

Internet Attachment Provider (IAP): An organization that provides physical and 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 layer-2 connectivity, such as fiber or Ethernet, i.e., it may or may not be the role of an IAP.

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.

Location-dependent emergency dial string: Location-dependent emergency dial strings should be thought of as the digit sequence that is dialed in order to reach emergency services. There are two dial strings, namely either a "home emergency dial string", or a "visited emergency dial string", and is something separate from an emergency identifier, since each represents specific emergency dial string key sequences which are recognized within a local geographic area or jurisdiction.

Location validation: A caller location is considered valid if the civic or geographic location is recognizable within an acceptable location reference system (e.g., USPS, WGS-84, etc.), 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. 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.

Mapping: The process of resolving a location to one or more PSAP URIs which directly identify a PSAP, or point to an intermediary which knows about a PSAP and that is designated as responsible to serve 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 which uses a distributed mapping protocol, to perform a mapping between a location and a PSAP, or intermediary which knows about the PSAP, and is used to assist in routing an emergency call.

PSAP (Public Safety Answering Point): Physical location where emergency calls are received under the responsibility of a public authority. (This terminology is used by both ETSI, in ETSI SR 002 180, and 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 PSAP is that which supports the receipt of emergency calls over IP. It is also assumed that the PSAP is reachable by IP-based protocols, such as SIP for call signaling and RTP for media.

PSAP URI: PSAP URI is a general term, used to refer to the output of the mapping protocol, and represents either the actual PSAP IP address, or the IP address of some other intermediary, e.g., an ESRP, which points to the actual PSAP.

Visited emergency dial string: A visited emergency dial string represents a sequence of digits that is used to initiate an emergency call within a geographically correct location of the caller if outside the caller's "home" location or vicinity.

Voice Service Provider (VSP): A specific type of Application Service Provider which 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. Basic Actors

In order to support emergency services covering a large physical area, various infrastructure elements are necessary, including: Internet Attachment Providers (IAPs), Application/Voice Service Providers (ASP/VSPs), PSAPs as endpoints for emergency calls, mapping services or other infrastructure elements that assist during the call routing.

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

```
      Location
      Information     +-----------------+
          |(1)        |Internet         |   +-----------+
          v           |Attachment       |   |           |
     +-----------+    |Provider         |   | Mapping   |
     |           |    | (3)             |   | Service   |
     | Emergency |<---+-----------------+-->|           |
     | Caller    |    | (2)             |   +-----------+
     |           |<---+-------+         |          ^
     +-----------+    |  +----|---------+------+   |
          ^           |  |   Location   |      |   |
          |           |  |   Information<-+    |   |
          |           +--+--------------+ |(5) |   | (6)
          |              |                |    |   |
          |              |    +-----------v+   |   |
          |   (4)        |    |Emergency   |   |   |
          +--------------+--->|Call Routing|<--+---+
          |              |    |Support     |   |
          |              |    +------------+   |
          |              |          ^          |
          |              |      (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.

o How is location information provided to the end host? It might either be known to the end host itself via manual configuration, provided via GPS, or obtained via a third party method. Even if location information is known to the network it might be made available to the end host via DHCP (RFC 3825 [2]) or some other mechanism. Alternatively, location information is used as part of call routing and inserted by intermediaries.

o Is the Internet Attachment Provider also the Application/Voice Service Provider? In the Internet today these roles are typically provided by different entities. As a consequence, the Application/ Voice Service Provider is typically not able to learn 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 Attachment 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 in the following:

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

(2) Location information might, however, also be obtained from the Internet Attachment Provider (e.g., using DHCP or application layer signaling protocols).

(3) The emergency caller might need to consult a mapping service to determine the PSAP 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, e.g., an Emergency Service Routing Proxy (ESRP), in SIP).

(5) Location Information is used by emergency call routing 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 (UE) may interact directly with the PSAP (e.g., UE invokes mapping, and initiates a connection), without relying on any intermediary emergency call routing support entities.

4. 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 not be a telecommunication provider.

Re2. International applicability: Regional, political and organizational aspects MUST be considered during the design of protocols and protocol extensions which 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 United States counties or municipalities handle emergency calls.

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

Motivation: The design 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: In 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 [10]),

instant messaging and video.

Re5. Alternate mapping sources: The mapping protocol MUST implement a mechanism that allows for the retrieval of mapping information from different sources.

Motivation: This provides the possibility of having available alternative sources of mapping information when the normal source is unavailable or unreachable.

Re6. Currency 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 timeframe. Differences in currency between mapping data contained within mapping sources should be minimized.

Re7. 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 specific URI which 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.

Re8. 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.

Re9. Common data structures and formats: The mapping protocol SHOULD support common data structures and formats from the mapping server.

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 which contains civic addresses used by location servers may be used for multiple purposes and applications beyond emergency service location-to-PSAP URI mapping.

Re10. 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 [9]).

5. Identifying the Caller's Location

Location can either be provided directly, or by reference, and represents either a civic location, or as a geographic location. How does the location (or location reference) become associated with the call? 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. The location information is derived from sources such as GPS, DHCP (RFC 3825 [2]) and I-D.ietf-geopriv-dhcp-civil [7]) or utilizing the Link Layer Discovery Protocol (LLDP) [see IEEE8021AB].

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

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

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

Lo2. Location object/info preservation: The mapping protocol MUST retain any location information which is provided to it, even after mapping is performed.

Motivation: The ESRP and the PSAP use the same location information object, but for a different purpose. Therefore, it is imperative that the mapping protocol not remove location Information so that the PSAP can still receive the caller location.

Lo3. 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.

Lo4. Alternate community names: The mapping protocol MUST support both the jurisdictional community name and the postal community name fields within the PIDF-LO data.

Motivation: A mapping query must be accepted with either or both community name fields, and provide appropriate responses. If a mapping query is made with only one field present, and if the database contains both jurisdictional and postal, the mapping protocol response should return both.

Lo5. Validation of civic location: The mapping protocol MUST support location validation for civic location (street addresses), prior to initiating an emergency call.

Motivation: Location validation provides an opportunity to help assure ahead of time, whether or not 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 locations.

Lo6. Validation resolution: 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.

Lo7. Indication of non-existent location: The mapping protocol MUST support a mechanism to indicate and resolve any associated issues attributed to a location or a part of a location that is known to not exist, despite the receipt of a successful mapping response.

Motivation: The emergency authority for a given jurisdiction may provide a means to resolve addressing problems, e.g., a URI for a web service that can be used to report problems with an address.

Lo8. 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.

Lo9. 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 provisioning systems will accept both 2D and 3D data. When a 3D request is presented to an area only defined by 2D data, the mapping result would be the same as if the height/altitude dimension was omitted in the request.

Lo10. Location validation indicator: The mapping protocol MAY support a mechanism which indicates whether a civic location does or does not fall within an existing range of addresses listed within a referenced address database.

Motivation: It is helpful to get an indication of whether the validation process worked or not.

Lo11. Matched element indication: The mapping protocol MAY support a mechanism which returns an indication of specific data elements which were matched as a result of a validation query.

Motivation: Given a query using "123 Main St. Anytown" (represented, as A1, A2, A3, A5 in this example) it may be helpful to receive an indication that the validation process matched only elements A2, A3, A5 (but not A1).

Lo12. Database type indicator: The mapping protocol MAY support a mechanism which 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. This is applicable for either civic or geographic location matching (e.g., USPS, MSAG, GDT, etc.).

6. Emergency Identifier

Id1. Emergency identifier support: The mapping protocol MUST support one or more emergency identifiers for delivery back to mapping clients to be used for call setup purposes.

Motivation: Since there is a need for any device or network element to recognize an emergency call throughout the call setup, there is also a need to have the mapping protocol provide support for such an identifier. This is regardless of the device location or the ASP/VSP used. An example of this kind of identifier might be "urn:service:sos".

Id2. Emergency identifier resolution: Where multiple emergency identifiers exist, the mapping protocol MUST be able to differentiate between identifiers based on the specific type of emergency help requested.

Motivation: Some jurisdictions may have multiple types of emergency services available, (e.g., fire, police, ambulance), in which case, it is important that any one could be selected directly.

Id3. Emergency identifier marking: The mapping protocol MUST include an emergency identifier with the signaling, if one does not exist, for the purpose of marking the 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, etc. This marking mechanism is assumed to be different than a QoS marking mechanism.

Id4. Prevention of fraud: If a call is identified as an emergency call, the mapping protocol MUST support that call being successfully routed to a PSAP.

Motivation: This prevents use of the emergency call indication to gain access to call features or authentication override for non-emergency purposes.

Id5. Extensible emergency identifiers: The mapping protocol MUST support an extensible list of emergency identifiers, though it is not required to provide mapping for every possible service.

Motivation: The use of an emergency identifier is locally determined.

Id6. Discovery of emergency dial string: The mapping protocol MUST support a mechanism to discover an existing location-dependent emergency dial string, (e.g., "9-1-1", "1-1-2"), which are contextually appropriate for the location of the caller.

Motivation: Users are trained to dial the appropriate emergency dial string to reach emergency services. There needs to be a way to figure out what the dial string is within the local environment of the caller.

Id7. Home emergency dial string translation: The mapping protocol MUST support end device translation (e.g. SIP UA) of a home emergency dial string into an emergency identifier.

Motivation: The UA would most likely be pre-provisioned with the appropriate information in order to make such a translation. The mapping protocol would be able to support either type for those clients which may not support dial string translation.

Id8. Emergency dial string replacement: The mapping protocol SHOULD support replacement of the original dial string with a reserved emergency identifier for each signaling protocol used for an emergency call. This replacement of the original dial string should be 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 terminal may lack the capability to determine the actual emergency address (PSAP URI). The use of local conventions may be required as a transition mechanism. Note: Such use complicates international movement of the user terminal. Evolution to a standardized emergency identifier or set of identifiers is preferred.

Id9. Emergency identifier not recognized: The mapping protocol MUST support calls which are initiated as emergency calls even if the specific emergency service requested is not recognized, based on the emergency identifier used.

Motivation: In order to have a robust system that supports incremental service deployment while still maintaining a fallback capability.

Id10. Discovery of visited emergency dial strings: The mapping protocol MUST support a mechanism to allow the end device to learn visited emergency dial strings.

Motivation: Scenarios exist where a user dials a visited emergency dial string that is different from the home emergency dial string: If a user (i.e., UA operator) visits a foreign country, observes a fire truck with 999 on the side, the expectation is one of being able to dial that same number to summon a fire truck. Another use case cited is where a tourist collapses, and a "good Samaritan" uses the tourist's cell phone to enter a home emergency dial string appropriate for that foreign country.

7. Mapping Protocol

There are two basic approaches to invoking a mapping service. 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 is outlined in the document I-D.hardie-ecrit-lost [6].

For caller-based resolution, the caller's user agent invokes a mapping service 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, a call signaling server, 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. 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 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.

Ma2. 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.

Ma3. 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: To help avoid the case of relying on incorrect configuration data which may cause calls to fail, particularly for caller-based mapping queries.

Ma4. Multiple response URIs: The mapping protocol MUST support the possible inclusion of multiple URIs in a mapping response.

Motivation: Multiple URIs may be available from the mapping server.

Ma5. URI alternate contact: In addition to returning a primary contact, the mapping protocol MUST support the return of a URI or contact method explicitly marked as an alternate contact.

Motivation: In response to a mapping request, the mapping server may return an alternate URI. Implementation details to be described within an operational document.

Ma6. URL properties: The mapping protocol MUST support the ability to provide ancillary information about a contact or URI that allows the mapping client to determine relevant properties of the URL.

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 URLs 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.

Ma7. Traceable resolution: The mapping protocol SHOULD support the ability of the mapping client to be able to determine the entity or entities which provided the emergency address resolution information.

Motivation: It is important for public safety reasons, that there is a method to provide operational traceability in case of errors.

Ma8. URI for error reporting: The mapping protocol MUST support the return of a URI 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 URI which points to a resource which can explain or potentially help resolve the error.

Ma9. Resilience against failure: The mapping protocol MUST support a mechanism which enables fail over to different (replica) mapping server in order to obtain a successful mapping.

Motivation: It is important that the failure of a single mapping server does not preclude the mapping client's ability to receive mapping from a different mapping server.

Ma10. Incrementally deployable: The mapping protocol MUST be designed in such a way that supports the incremental deployment of mapping services.

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.

Ma11. 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.

Motivation: Used as a fallback mechanism only, if a mapping query fails at emergency call time, it may be advantageous to have prior knowledge of the PSAP URI. This prior knowledge would be obtained by performing a mapping query at any time prior to an emergency call.

Ma12. 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.

Ma13. 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 (RFC 4119 [3]).

Ma14. 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.

Ma15. Baseline query protocol: A mandatory-to-implement protocol MUST be specified.

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

Ma16. Multiple PSAP URIs: The mapping protocol MUST support a method to receive multiple PSAP URIs which cover the same geographic area.

Motivation: Two different mapping servers may cover the same geographic area, and therefore have the same set of coverage information.

Ma17. Single URI per contact protocol: Though the mapping protocol supports the return of multiple URIs, it SHOULD return only one URI per contact protocol, 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.

8. Security Considerations

Security considerations are discussed in the ECRIT security document I-D.ietf-ecrit-security-threats [4] .

9. Contributors

The information contained in this document is a result of a joint effort based on individual contributions by those involved in the ECRIT WG. The contributors include Nadine Abbott, Hideki Arai, Martin Dawson, Motoharu Kawanishi, Brian Rosen, Richard Stastny, Martin Thomson, James Winterbottom.

The contributors can be reached at:

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

10. Acknowledgments

In addition to thanking those listed above, we would like to also thank Guy Caron, Barry Dingle, Keith Drage, Tim Dunn, Patrik Faeltstroem, Clive D.W. Feather, Raymond Forbes, Randall Gellens, Michael Haberler, Michael Hammer, Ted Hardie, Gunnar Hellstrom, Cullen Jennings, Marc Linsner, Rohan Mahy, Patti McCalmont, Don Mitchell, John Morris, Andrew Newton, Steve Norreys, Jon Peterson, James Polk, Benny Rodrig, John Rosenberg, Jonathan Rosenberg, John Schnizlein, Shida Schubert, James Seng, Byron Smith, Tom Taylor, Barbara Stark, Hannes Tschofenig, and Nate Wilcox, for their invaluable input.

11. References

11.1. Normative References

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

[2] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

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

[4] Taylor, T., "Security Threats and Requirements for Emergency Call Marking and Mapping", draft-ietf-ecrit-security-threats-01 (work in progress), April 2006.

[5] Schulzrinne, H., "A Uniform Resource Name (URN) for Services", draft-ietf-ecrit-service-urn-02 (work in progress), April 2006.

[6] Hardie, T., "LoST: A Location-to-Service Translation Protocol", draft-hardie-ecrit-lost-00 (work in progress), March 2006.

[7] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", draft-ietf-geopriv-dhcp-civil-09 (work in progress), January 2006.

11.2. Informative References

[8] 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.

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

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

[11] Wijk, A., "Framework for real-time text over IP using SIP", draft-ietf-sipping-toip-04 (work in progress), March 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
2401 Elliott Avenue
2nd Floor
Seattle, WA 98121
US

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

Acknowledgment

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