ECRIT H. Schulzrinne
Internet-Draft Columbia U.
Expires: August 31, 2006 R. Marshall, Ed.
TCS
February 27, 2006

Requirements for Emergency Context Resolution with Internet Technologies
draft-ietf-ecrit-requirements-05.txt

Status of this Memo

Copyright Notice

Abstract

This document enumerates requirements for 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 messaging for hearing disabled users, (RFC 3351 [7]) 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, (Internet device), and terminates to an IP-capable PSAP, done entirely over an IP network.

This document outlines the various functional issues which relate to making 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).

Identification of the caller, while not incompatible with the requirements for messaging outlined within this document, is not currently considered within the scope of the ECRIT charter, and is therefore, left for a future draft to describe.

Note: 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 correct location.

Ideally, the mapping protocol would yield a URI from a preferred set of URIs (e.g. sips:uri; sip:uri), which would allow an emergency call to be completed using IP end-to-end (possibly via the Internet). 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 a TEL URI which may be used to complete a call over the

PSTN.

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] and indicate requirement levels for compliant implementations.

Since a requirements document does not directly specify a protocol to implement, these compliance labels should be read as indicating requirements for the protocol or architecture, rather than an implementation.

For lack of a better term, we will use the term "caller" or "emergency caller" to refer to the person placing an emergency call or sending an emergency 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 defined as something more general than a Voice Service Provider, since emergency calls are sometimes likely to use other media, including text and video. Note: For a particular user, the ASP may or may not be the same organization as the IAP and/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 scheme (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 caller: The user or user device entity which sends his/her location to another entity in the network.

Emergency identifier: The numerical and/or text identifier which is supplied by a user or a user device, which identifies the call as an emergency call and is translated into an emergency address, useful for call routing and completion of the emergency call.

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

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

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)

Home emergency dial-string: A home emergency dial-string (ref. Location-dependent emergency identifier) represents a sequence of digits that is used to initiate an emergency call within a geographic vicinity considered to be a user's "home" location or vicinity.

Internet Attachment Provider (IAP): An organization that provides physical 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.

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. In the geocoding process, the location is defined with an x,y coordinate value according to the distance north or south of the equator and east or west of the prime meridian.

Location Context Mapping System (LCMS): A system defined as a set of mechanisms and services working together to perform a mapping, (or, direct association), between a location and a PSAP uri designated as responsibleto to serve that location.

Location-dependent emergency identifier: Location-dependent emergency identifiers, also referred to as "emergency dial-strings" within this document, 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 a universal emergency identifier, since each represents specific emergency identifiers 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 systems (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: Process of resolving a location to a URI (or multiple URIs).

Mapping client: A Mapping Client interacts with the Mapping Server to learn one or multiple 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 URI mappings.

Mapping service: A network service which uses a distributed mapping protocol to provide information about the 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.

Universal identifier: An emergency identifier which is recognized by any compatible endpoint, from any geographic location as useful for initiating an emergency request. A general approach to using universal identifiers is outlined in the service URN draft (I-D.schulzrinne-sipping-service [5]).

Visited emergency dial-string: A visited emergency dial-string (ref. Location-dependent emergency identifier) represents a sequence of digits that is used to initiate an emergency call within a geographic vicinity other than a user'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.

3. Basic Actors

In order to support emergency services covering a large physical area various infrastructure elements are necessary: Internet Attachment Providers, Application/Voice Service Providers, PSAPs as endpoints for emergency calls, mapping services or other infrastructure elements that assist in during the call routing and potentially many other entities.

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<-+    |   |
          |           +--+--------------+ |(8) |   | (5)
          |              |    +-----------v+   |   |
          |   (4)        |    |Emergency   |   |   |
          +--------------+--->|Call Routing|<--+---+
          |              |    |Support     |   |
          |              |    +------------+   |
          |              |       ^             |
          |              |   (6) |        +----+--+
          |    (7)       |       +-------->|       |
          +--------------+--------------->| PSAP  |
                         |                |       |
                         |Application/    +----+--+
                         |Voice                |
                         |Service              |
                         |Provider             |
                         +---------------------+
```

Figure 1: Framework

Figure 1 shows the interaction between the entities involved in the call. There are a number of different deployment choices, as it can be easily seen from the figure. The following deployment choices need to be highlighted:

- How is location information provided to the end host? It might either be known to the end host itself (due to manual configuration or provided via GPS) or available via a third party. Even if location information is known to the network it might be made available to the end host. Alternatively, location information is used as part of call routing and inserted by intermediaries.

- 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.

Please note that the overlapping squares aim to indicate that certain functionality 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 and they might also operate the PSAP. There is, however, no requirement that this must be the case. Additionally it is worth pointing out that end systems might be its own VSP, e.g., for enterprises or residential users.

Below, we describe various interactions between the entities shown in Figure 1 are described:

- (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 (and considering other attributes such as a certain language support by the Emergency Call Takers).

- (4) The Emergency Caller might get assistance for emergency call routing by infrastructure elements (referred as Emergency Call Routing Support entities). In case of SIP these entities are proxies.

- (5) Individual Emergency Call Routing Support entities might need to consult a mapping service to determine where to route the emergency call.

- (6) The Emergency Call Routing Support entities need to finally forward the call, if infrastructure based emergency call routing is used.

- o (7) The emergency caller might interact directly with the PSAP without any Emergency Call Routing Support entities.

- o (8) Location Information is used by emergency call routing entities to determine appropriate PSAP mapping.

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 Service Provider: The existence of an Application Service Provider (ASP) SHOULD NOT be assumed.

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: Regional, political and organizational aspects MUST be considered during the design of protocols and protocol extensions.

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 emergency services MUST NOT depend on a sole central administration authority.

Motivation: Once common standards are established, it must be 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, ASPs, IAPs or other participants.

Re4. Multiple Modes: Multiple communication modes, such as audio, video and text messaging MUST be supported (i.e. implemented in the protocol, though not necessarily used).

Motivation: In PSTN, voice and text telephony (often called TTY or textphone 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 [9]), instant messaging and video.

Re5. Alternate Mapping Sources: The mapping protocol SHOULD implement a mechanism that allows for the retrieval of mapping information, possibly of different degrees of currency.

Motivation: This provides the possibility of having available alternative sources of mapping information when the normal source is unavailable or unreachable, without specifying the means by which the alternative source is created or updated.

Re6. Incremental Deployment: The ECRIT mapping protocol MUST return URIs that are usable by a standard signaling protocol (i.e., without special emergency extensions) unless an error is returned.

Motivation: The format of the output returned by the mapping protocol is in a standard format for communication protocol. For example, it should return something SIP specific (e.g. URI), that any SIP capable phone would be able to use if used in a SIP context. Special purpose URIs would not be understood by "legacy" SIP devices since they do not have knowledge about the mapping protocol, and therefore are not to be used.

Re7. Ubiquitous Triggering: The mapping protocol MUST implement, (not necessarily use), the ability to be invoked at any time, from any location, by any client which supports the mapping protocol.

Motivation: While end devices are the typical initiators of mapping service requests, it is also expected that other mapping clients, such as relays, 3rd party devices, PSAPs, etc. may also trigger a mapping request.

Re8. PSAP Identification: The mapping information MUST be available without having to enroll with a service provider.

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 VSP.

Re9. No Modification of Location Databases: The mapping protocol SHOULD NOT require that data within location databases be transformed or modified in any unusual or unreasonable way in order for the mapping protocol to use the data.

Motivation: Databases which contain civic addresses (used within location information servers), may be used for multiple purposes and applications, (in addition to being used for emergency service mapping only).

5. Identifying the Caller 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, derived from sources such as GPS, DHCP (RFC 3825 [2]) and I-D.ietf-geopriv-dhcp-civil [6]) or utilizing the Link Layer Discovery Protocol (LLDP) [see IEEE8021AB].

UA-referenced: The caller's user agent provides a 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.

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

Lo1. Validation of Civic Location: The mapping protocol MUST implement a method that makes it possible for a mappng server to validate a civic location prior to that location's use in an actual emergency call.

Motivation: Location validation provides an opportunity to help assure ahead of time, whether 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.

Lo2. Validation Resolution: The mapping protocol MUST support (i.e. required to implement, though not required for use) the return of additional information which can be used to determine the precision or resolution of the data elements used to determine a PSAP URI, for example.

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.

Lo3. Indication of non-existent location: The protocol MUST support (i.e. must implement in the protocol, though not necessarily use) a mechanism to indicate that a location or a part of a location is known to not exist, even if a valid location-to-PSAP uri mapping can be provided. This mechanism includes a means to identify a separate mechanism that could be used to resolve the discrepancy.

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. The mapping response would allow this service to be identified.

Lo4. Limits to Validation: Successful validation of a civic location MUST NOT be required to enable any feature that is part of the emergency call process.

Motivation: In some cases, (based on a variety of factors), 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 signaling path to the PSAP.

Lo5. Reference Datum: The mapping server MUST implement support for the WGS-84 coordinate reference system and may implement support for use of other reference systems.

Lo6. Location Provided: An Emergency Services Routing Proxy (ESRP) MUST NOT remove location information after performing location based routing.

Motivation: The ESRP and the PSAP use the same location information object but for a different purpose. Therefore, the PSAP still requires the receipt of information which represents the end device's location.

Lo7. 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, so to return an appropriate result, based on which type of input is used.

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 on the request."

6. Emergency Identifier

Id1. Universal Identifier Setup: One or more universal emergency identifiers MUST be recognized by any device or network element for call setup purposes

Motivation: There must be some way for any device or element to recognize an emergency call throughout the call setup. This is regardless of the device location, the application (voice) service provider used (if any at all), or of any other factor. Examples of these might include: 911, 112, and sos.*.

Id2. Universal Identifier Resolution: Where multiple emergency service types exist, the mapping protocol MUST support (i.e. implement, though not necessarily use) the individual treatment of each emergency identifier used, based on the specific type of emergency help requested.

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

Id3. Emergency Marking: Any device in the signaling path that recognizes by some means that the signaling is associated with an emergency call MUST add a specific emergency indication, if it doesn't already exist, to the signaling before forwarding it. This marking mechanism must be different than QoS marking.

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.

Id4. Emergency Identifier-based Marking: User agents, proxies, and other network elements that process signaling associated with emergency calls SHOULD be configured to recognize a reasonable selection of logical emergency identifiers as a means to initiate emergency marking.

Motivation: Since user devices roam, emergency identifiers may vary from region to region. It is therefore important that a network entity be able to perform mapping and/or call routing within the context of its own point of origin rather than relying on non-local logical emergency identifiers as the only basis for emergency marking of calls.

Id5. Prevention of Fraud: A call MUST be routed to a PSAP if it is identified as an emergency call or is marked as such in accordance with the above emergency marking requirements.

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

Id6. Extensibility of emergency service types: The list of emergency service types MUST be extensible, and it is not necessary to provide mapping for every possible service type.

Motivation: The use of a service type is locally determined.

Id7. Discovery of emergency dial-string: The mapping protocol MUST support (i.e. implement, though not necessarily use) a mechanism to discover existing location-dependent emergency identifiers, known as emergency dial-strings, (e.g. 9-1-1, 1-1-2), 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.

Id8. Local Identifier Translation: The SIP UA SHOULD translate home emergency dial-strings to universal emergency identifiers. The UA would most likely be pre-provisioned with the appropriate information in order to make such a translation. This assumes that a mechanism to provide the user's home emergency dial-strings be available.

Id9. Emergency Identifier Replacement: For each signaling protocol that can be used in an emergency call, reserved identifiers SHOULD be allowed to replace the original emergency identifier, 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, and evolution to a standardized universal emergency identifier or set of identifiers is preferred.

Id10. Universal Identifier Recognition: Universal identifier(s), MUST be universally recognizable (as the label suggests), by any network element which supports the (ECRIT) mapping protocol.

Id11. Universal Identifier Unrecognized: A call MUST be recognized as emergency call even if the specific emergency service requested is not recognized.

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

Id12. Translation of emergency dial-strings: The SIP UA SHOULD translate both home and visited emergency dial-strings into a universal emergency identifier.

Id13. Detection of visited emergency dial-strings: The mapping protocol MUST support (i.e. implement, though not necessarily use), 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 of a UA visits a foreign country, observes a fire truck with 999 on the side, the expectation is to be 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 dial a local emergency number.

7. Mapping Protocol

Given the requirement from the previous section, that of a single (or small number of) emergency identifier(s) which are independent of the caller's location, and since PSAPs only serve a limited geographic region, and for reasons of jurisdictional and local knowledge, having the call reach the appropriate PSAP based on a mapping protocol, is crucial.

There are two basic architectures described for translating an emergency identifier into the appropriate PSAP emergency address. We refer to these as caller-based and mediated.

For caller-based resolution, the caller's user agent consults 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 performs this function (a request for mapping) by invoking the mapping protocol.

Note that this case relies on an architecture where the call is effectively routed to a copy of the database, rather than having some non-SIP protocol query the database.

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.)

The problem at hand is more difficult to resolve than that for traditional web or email services. In this case, the emergency caller only dialed an emergency identifier, and depending on the location, any one of several thousand PSAPs around the world could be appropriate PSAP. In addition, there may be a finer resolution of routing (which the caller isn't aware of), which results in a particular "accredited" PSAP (i.e. one run by local authorities) answering to call. (Many PSAPs are run by private entities. For example, universities and corporations with large campuses often have their own emergency response centers.)

Ma1. Appropriate PSAP: Calls MUST be routed to the PSAP responsible for this particular geographic area. In particular, the location determination should 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.

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.

Ma2. Mapping redirection: The mapping protocol MUST support (i.e. implement for use) redirection functionality, since in some cases, an initial mapping may provide a single URL for a large geographic area. Redirection is needed to then re-invokes the mapping protocol on a different database to obtain another URL for a more resolute ESRP or PSAP, which covers a smaller area.

Motivation: The more local the mapping output is, the more favorable (in most cases) the likely outcome will be for the emergency caller.

Ma3. Minimal additional delay: The execution of the mapping protocol SHOULD minimize the amount of additional delay to 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.

Ma4. Referral: The mapping protocol MUST support (i.e. Implement for use), a mechanism for the mapping client to be able to contact any mapping server and be referred to another server that is more qualified to answer the query.

Motivation: This requirement alleviates the potential for incorrect configurations to cause calls to fail, particularly for caller-based queries.

Ma5. Multiple Response URIs: The mapping protocol response MUST support (i.e. implement, though not necessarily use), the inclusion of multiple URIs in the response.

Motivation: In response to a mapping request, a server will normally provide a URI or set of URIs for contacting the appropriate PSAP.

Ma6. URI - Alternate Contact: The mapping protocol MUST support (i.e. implement, though not necessarily use), the return of a URI or contact method explicitly marked as an alternate contact.

Motivation: In response to a mapping request, if an expected URI is unable to be returned, then mapping server may return an alternate URI. When and how this would be used will be described in an operational document.

Ma7. Multiple PSAP URIs: The mapping protocol MUST support (i.e. implement, though not necessarily use), a method to be able to return multiple URIs for different PSAPs that cover the same area.

Ma8. URL properties: The mapping protocol MUST support (i.e. implement, though not necessarily use), the ability to provide additional information that allows the querying entity 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 trigger methods.

Ma9. 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: To provide operational traceability in case of errors.

Ma10. URI for error reporting: The mapping protocol MUST support (i.e. implement for use) a mechanism to return a URI that can be used to report a suspected or known error within the mapping database.

Ma11. Resilience against server failure: The mapping protocol MUST support (i.e. implement for use) a mechanism to enable the mapping client to be able to fail over to another replica of the mapping server, so that a failure of a server does not endanger the ability to perform the mapping.

Ma12. 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 boundary information.

Ma13. Mapping requested from anywhere: The mapping protocol MUST support (i.e. implement, though not necessarily use) the ability to provide mapping information in response to queries from any (earthly) location, regardless of where the mapping client is located, either geographically or by network location.

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

Ma14. Location Updates: The mapping protocol MUST support (i.e. implement, though not necessarily use) the ability to provide location updates. Mapping services should implement the mechanisms to provide updated location.

Motivation: Updated location information may have an impact on PSAP routing. In some cases it may be possible to redirect that call to a more appropriate PSAP (some device measurement techniques provide quick (i.e. early), but imprecise "first fix" location).

Ma15. 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]).

Ma16. Split responsibility: The mapping protocol MUST support (i.e. implement for use) the division of data subset handling between multiple mapping servers within a single level of a civic location hierarchy.

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

Ma17. Pervasive Mapping: The mapping protocol MUST support (i.e. implement for use) the ability of the mapping function to be invoked at any time, including while an emergency call is in process.

Ma18. Baseline query protocol: A mandatory-to-implement protocol MUST be specified.

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

Ma19. Single URI Scheme: The mapping protocol MAY return multiple URIs, though it SHOULD return only one URI per scheme, 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.

Ma20. Separation of Identity from mapping: The mapping protocol MUST NOT require the true identity of the target for which the location information is attributed. 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 as defined in RFC 3963.

Ma21. Location delivery by-value: The mapping protocol MUST support (i.e. implement, though not necessarily use) the delivery of location information by-value, though may alternatively support de-referencing of specific location references.

Motivation: Location by-reference is not one of the evaluation criteria for a mapping protocol presented here. (i.e. the mapping protocol is not required to support the ability to de-reference specific location references.)

Ma22. Alternate community names: The mapping protocol MUST support (i.e. implement, though not necessarily use) both the jurisdiction 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, given that the database has both fields populated, the mapping protocol response should return both available fields.

Ma23. Support for alias locations: The mapping protocol MUST support (i.e. implement, though not necessarily use) one or more aliases for a specific location entry.

Motivation: It should be possible to relate one entry to another and be able to determine which is the "primary" entry and which is the alias. The result of aliasing is always that mapping from the primary or any of the aliases is the same.

Ma24. Pre-call mapping for fallback: The mapping protocol MUST support (i.e. implement, though not necessarily use) LCMS queries prior to making an emergency call.

Motivation: Used as a fallback mechanism only, if a LCMS 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 an LCMS query at any time prior to an emergency call.

8. Security Considerations

Note: Security Considerations are referenced in the ECRIT security document [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 Michael Hammer, Ted Hardie, Marc Linsner, Barbara Stark, Clive D.W. Feather, Keith Drage, Raymond Forbes, Tim Dunn, Steve Norreys, Patti McCalmont, Rohan Mahy, Nate Wilcox, Michael Haberler, Jonathan Rosenberg, Shida Schubert, John Schnizlein, Benny Rodrig, John Rosenberg, Patrik Faeltstroem, Barry Dingle, Gunnar Hellstrom, James Seng, Byron Smith, Cullen Jennings, Don Mitchell, John Morris, Jon Peterson, Randall Gellens, Guy Caron, Andrew Newton, James Polk, Tom Taylor, and Hannes Tschofenig 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] Schulzrinne, H., "Security Threats and Requirements for Emergency Calling", draft-taylor-ecrit-security-threats-01 (work in progress), December 2005.

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

[6] 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

[7] 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.

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

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

[10] Wijk, A., "Framework of requirements for real-time text conversation using SIP", draft-ietf-sipping-toip-03 (work in progress), September 2005.

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

Intellectual Property Statement

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

Acknowledgment

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