ECRIT
Internet-Draft
Expires: September 7, 2006

H. Schulzrinne
Columbia U.
R. Marshall, Ed.
TCS

March 6, 2006

Requirements for Emergency Context Resolution with Internet Technologies
draft-ietf-ecrit-requirements-06.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 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 correct location.

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

ascertain whether 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 that building exists at that spot. 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].

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.

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: The numerical and/or text identifier which is supplied by a user or a user device, which identifies the call as an emergency call. A universal emergency identifier is an example of an emergency identifier.

Emergency Service Routing Proxy (ESRP): An ESRP is an emergency call routing support entity that invokes the location-to-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 a universal 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 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) which identify a PSAP, or intermediary which knows about a PSAP that is designated as responsible to serve that location.

Mapping client: A mapping client interacts with the Mapping Server to learn one or more 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 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.

Universal emergency identifier: An emergency identifier which is recognized by any compatible endpoint, from any geographic location. A general approach to using universal emergency identifiers is outlined in the service URN draft (I-D.ietf-ecrit-service-urn [5]).

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.

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 (ASPs or 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.

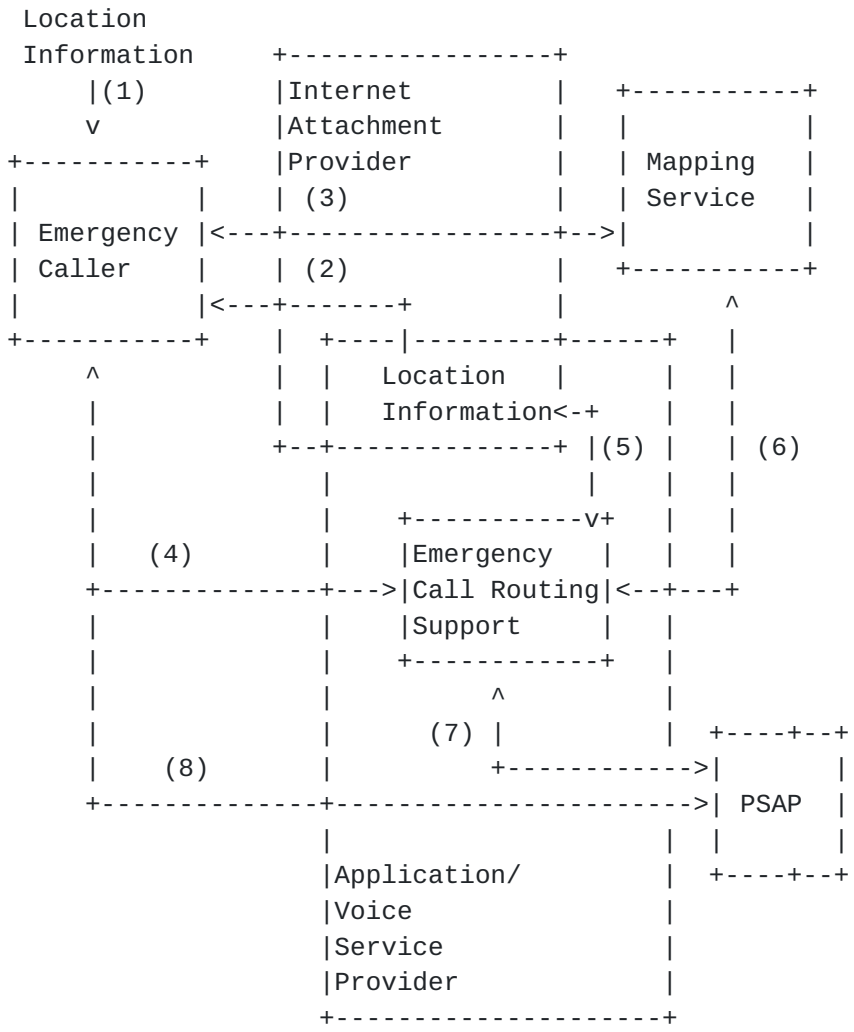

Figure 1: Framework for emergency call routing

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 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 to determine the appropriate PSAP.

(6) Individual 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: The existence of an Application/Voice Service Provider (ASP/VSP) 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 MUST be supported (i.e., implemented in the protocol, though not necessarily used in all calls).

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 [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. Differences of currency in mapping sources: For alternate mapping, differences in currency between mapping data contained within mapping sources SHOULD be minimized.

Motivation: Alternative sources of mapping data may not have been created or updated with the same set of information within the same timeframe.

Re7. Mapping result usability: The ECRIT mapping protocol MUST return a URI (or URIs) that are usable within a standard signaling protocol (i.e., without special emergency extensions).

Motivation: For example, a SIP specific URI returned by the mapping protocol, needs to be usable within any SIP capable phone in 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 accessibility: 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 servers, may be used for multiple purposes and applications beyond emergency service mapping.

5. Identifying the Caller's Location

Location can either be provided direct, 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 server MUST implement support for the WGS-84 coordinate reference system and MAY support other coordinate reference systems.

Lo2. 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 needs to receive the caller's location.

6. Emergency Identifier

Id1. Universal emergency 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. An example of this might be "urn:service:sos".

Id2. Emergency identifier resolution: Where multiple emergency identifiers exist, there MUST be a mechanism to differentiate each emergency identifier used, 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: 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. Prevention of fraud: A call MUST be routed to a PSAP if it is identified as an emergency call.

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

Id5. Extensibility of emergency identifiers: The list of defined emergency identifiers MUST be extensible, and it is not necessary to provide mapping for every possible service.

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

Id6. Discovery of emergency dial strings: The protocol MUST support a mechanism to discover existing location-dependent emergency dial strings, (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. Local emergency dial string translation: An end device (i.e., SIP UA), SHOULD translate home emergency dial strings into universal emergency identifiers. The UA would most likely be pre-provisioned with the appropriate information in order to make such a translation.

Id8. Emergency dial string replacement: For each signaling protocol that can be used in an emergency call, reserved universal emergency identifiers SHOULD be allowed to replace the original emergency dial strings, 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.

Id9. Universal emergency identifier recognition: A universal emergency identifier MUST be recognized by any network element which supports the mapping protocol.

Id10. Emergency identifier not recognized: A call MUST be recognized as an 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.

Id11. Discovery 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 (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 local emergency dial string.

7. Mapping Protocol

Given the requirement from the previous section, one of having a universal emergency identifier that is independent of the caller's location, and since each PSAP only serves 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 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: Calls MUST be routed to the PSAP responsible for a 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. 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.

Ma3. 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.

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

Ma5. URI alternate 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 additional information 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 (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.

Ma9. Resilience against 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.

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. 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 an ESRP, may not necessarily be anywhere close to the caller or the appropriate PSAP, but must still be able to obtain a mapping.

Ma12. 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]).

Ma13. 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 mapping servers for the same city or county may handle different streets within that city or county.

Ma14. Any time 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 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.

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 (i.e., implement, though not necessarily use), a method to be able to return multiple URIs for different PSAPs that cover the same area.

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.

Ma18. Anonymous 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 (RFC 3693 [9]).

Ma19. Location delivery by-value: The mapping protocol MUST support (i.e., implement, though not necessarily use) 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.

Ma20. 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.

Ma21. Ubiquitous triggering: The mapping protocol MUST implement, but 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.

Ma22. Validation of civic location: The mapping protocol MUST implement a method via a mapping request, that makes it possible for a mapping 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.

Ma23. Validation resolution: The mapping protocol MUST support (i.e., required to implement, but 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.

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.

Ma24. Indication of non-existent location: The protocol MUST support 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 includes a way to identify a separate mechanism to resolve any such 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.

Ma25. 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 signaling path to the PSAP.

Ma26. 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.

8. Security Considerations

Security considerations are discussed in the ECRIT security document I-D.taylor-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] Schulzrinne, H., "Security Threats and Requirements for Emergency Call Marking and Mapping", draft-taylor-ecrit-security-threats-03 (work in progress), March 2006.

[5] Schulzrinne, H., "A Uniform Resource Name (URN) for Services", draft-ietf-ecrit-service-urn-00 (work in progress), February 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 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

Copyright Statement

Acknowledgment

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