

ecrit  
Internet-Draft  
Expires: August 19, 2005

B. Rosen  
Emergicom  
N. Abbott  
Telcordia  
February 15, 2005

NENA Requirements for Emergency Call processing  
draft-rosen-nena-ecrit-requirements-00.txt

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [Section 3 of RFC 3667](#). By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with [RFC 3668](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 19, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

The National Emergency Number Association (NENA)'s mission is to foster the technological advancement, availability, and implementation of a universal emergency telephone number system in North America. NENA has an active effort to develop a new architecture for emergency call handling known as "i3" being

Internet-Draft

NENA Requirements

February 2005

developed in its Long Term Definition working group. The following requirements are a subset of the requirements of the i3 work which relate to ecrit work. NENA understands the global nature of the Internet, and is eager to work with the IETF to ensure that emergency call processing meets the needs of users in North America.

## Table of Contents

<a href="#">1.</a>	Requirements notation . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Background on the North American 9-1-1 System . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Functional Requirements . . . . .	<a href="#">7</a>
<a href="#">3.1</a>	Signaling . . . . .	<a href="#">7</a>
<a href="#">3.2</a>	Location . . . . .	<a href="#">7</a>
<a href="#">3.3</a>	Call Back Address . . . . .	<a href="#">8</a>
<a href="#">3.4</a>	Additional Information . . . . .	<a href="#">8</a>
<a href="#">3.5</a>	Validation of Civic Location . . . . .	<a href="#">8</a>
<a href="#">3.6</a>	Routing of Calls . . . . .	<a href="#">9</a>
<a href="#">3.7</a>	Connections to the Emergency Services Network . . . . .	<a href="#">11</a>
<a href="#">3.8</a>	Other . . . . .	<a href="#">11</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">13</a>
<a href="#">5.</a>	References . . . . .	<a href="#">13</a>
	Authors' Addresses . . . . .	<a href="#">13</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">14</a>

## 1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

## 2. Background on the North American 9-1-1 System

The universal emergency number in nearly all of North America is 9-1-1. Wireless or wireline callers to 9-1-1 are routed by the phone system to one of approximately 6,134 Public Safety Answering Points (PSAPs), which are agencies of local government. In North America, there was a very large effort to build what is called the "Enhanced 9-1-1" or E911 system which endeavors to inform the call taker of the location (address) of the caller automatically.

Location based routing of emergency calls is handled by a special purpose tandem switch known as a Selective Router (SR). There are several hundred Selective Routers in North America. PSAPs are connected by dedicated trunks to an SR. The SR has a database that is indexed by a key provided in the signaling to determine which PSAP should receive the call. For wireline callers, the key is the ANI (Automatic Number Identification), typically the calling party number. For wireless callers, the key may be a dynamically assigned number associated with the call.

Automatic delivery of location information to the PSAP is accomplished using a database known as the ALI (Automatic Location Identification) which is also indexed by the ANI (for wireline callers) or by the dynamically assigned key for wireless callers. The ALI contains the location associated with the telephone number of the caller (or determined by the dynamic key for wireless callers). A query to the ALI is made by the PSAP as it answers the call, and the location is displayed to the call taker. To ensure that the location information entered into the ALI conforms to the

civic address space known to the PSAP, there is another database called the "Master Street Address Guide" which contains a listing of all known streets and the known address ranges within those streets. When moves adds or changes are ordered for telephone services, the carriers process service orders for entry into the ALI. Before changes are made, the address information is validated by comparing it to the MSAG. If the address matches an entry in the MSAG, it is considered a valid address, and entered into the ALI.

Each PSAP has a service area, which do not overlap. Nearly all of North America is served by a PSAP, although there remain isolated areas which do not have 9-1-1 service and must rely on direct calls to police, fire or emergency medical services. The boundaries of the services areas often match the boundaries of political subdivisions such as state, county or municipality, but unfortunately, they do not always have such integral boundaries. For historical, political, and practical reasons, some PSAP boundaries are irregular. In some cases, for example, boundaries are a few townships, several unincorporated areas of a county, and a few streets of another

municipality. The boundaries, for civic address purposes, are between specific street addresses. For example, 101 North Main might be served by one PSAP, and 102 North Main may be served by another. As with other areas, sometimes streets are split down the middle, and even numbered houses are in one service area, and odd numbered streets are in another. Although the incidence of irregular boundaries is uncommon, it occurs with sufficient frequency that we must have mechanisms that cope with routing to irregular boundaries.

Validation of addresses, in comparison to the current MSAG, is essential for North America. The accuracy of the location is greatly enhanced by verifying that addresses presented to the PSAP during a call are known to the responders - that is, if a responder is dispatched to 101 North Main, there is a very high probability that there is a 101 North Main. Addresses must be validated before they are used.

The MSAG, like the ALI, is maintained by a designated local 9-1-1 authority, which sometimes has jurisdiction over several PSAPs. This means that there are actually several MSAGs that cover areas corresponding to one or more PSAP service boundaries. This complicates any proposed mechanisms that would maintain global

equivalents of the MSAG because the maintenance of the database must devolve to the service boundaries, which, as has been explained, is irregular. An entry in the MSAG for 101 North Main may be the responsibility of one entity, while the entry that covers 102 North Main may be another entity's responsibility.

In North America, there is a complication with civic addresses that arises because the Post Office does not necessarily follow the changes that evolve over time with municipal boundaries. Specifically, the "Community Name" for the post office is not necessarily the actual (legal) community name. This has been the subject of discussion in geopriv, and there is now agreement that both a postal community name and a legal community name should be carried in a location objects. Routing of emergency calls is always on the legal community name.

In the North American E9-1-1 System, the Selective Router provides default routing arrangements when the specific location information for the caller is not available; this default routing is generally derived based on the local access area from which the call was originated (as identified by a trunk group).

In addition, in the North American E9-1-1 System, the Selective Router supports overload routing arrangements (e.g., to an announcement) in congestion conditions, and contingency routing arrangements when a PSAP is not available to answer emergency calls.

These contingency routing arrangements (e.g., to an alternate answering point) can be invoked automatically (e.g., on a scheduled basis) or in real-time for the PSAP by a designated authority(ies).

The North American E9-1-1 System also provides for congestion control mechanisms that restrict the number of emergency calls that can be offered to a PSAP at any given time.

### [3.](#) Functional Requirements

#### [3.1](#) Signaling

3.1-1: Tracking and Tracing Facilities for all calls must be provided. This include all routing entities as well as all signaling entities.

3.1-2: Each element in the signaling and routing paths solution

- shall maintain call detail records that can be accessed by management systems to develop call statistics in real time.
- 3.1-3: The emergency call routing system must harmonize with international specifications to permit local determination of emergency call number (i.e. 9-1-1, 1-1-2).
  - 3.1-4: Mechanisms must be provided to route emergency calls in areas not served by E9-1-1 to an appropriate PSTN telephone number.
  - 3.1-5: Each element of the signaling and routing paths shall provide congestion controls.
  - 3.1-6: It shall be possible to determine the complete call chain of a call, including the identity of each signaling element in the path, and the reason it received the call (Call History).
  - 3.1-7: Support must be provided to accept calls from end offices and MSCs via the Public Switched Telephone Network, using SS7, CAMA and ISDN interfaces.
  - 3.1-8: Call setup time (dialing of last digit to alerting at the PSAP), under expected peak load shall be less than 2 seconds. If CAMA signaling is in the path, then an additional ? seconds is permitted.

## 3.2 Location

- 3.2-1: Calls using VoIP or subsequent methods are expected to supply location with the call.
- 3.2-2: PSAPs shall accept location as civic and/or geo specified.
- 3.2-3: All representations of location shall include the ability to carry altitude. This requirement does not imply altitude is always used or supplied.
- 3.2-4: The preferred coordinate system for emergency calls is WGS-84.
- 3.2-5: If multiple Location Objects are provided with a call, it should be possible to identify the most accurate, current, appropriate location information to be used for routing emergency calls and dispatching emergency responders.
- 3.2-6: No assumption shall be made that the entity presenting the call to the PSAP has any knowledge of, or control over the provider of location. The location provider may be independent of all other service providers handling the call.

- 3.2-7: PSAPs shall have the ability to requery for a location update.



- 3.2-8: PSAPs shall be able to make use of default location information when measurement based location determination mechanisms fail. Examples include tower/Access Point location, last known fix, etc.
- 3.2-9: PSAPs must be made aware when default location information was used to route a call.

### 3.3 Call Back Address

- 3.3-1: Calls to 9-1-1 shall supply a call back address (URI) with the call

### 3.4 Additional Information

- 3.4-1: In addition to information sent with the call, additional information may be available that is retrieved from internal or external databases using a key to the information included with the call. This key may also include information to identify/address the database.
- 3.4-2: Additional information may be available to the call taker based on the location of the caller.
- 3.4-3: Additional information may be available to the call taker based on the owner of the structure.
- 3.4-4: Additional information may be available to the call taker based on the tenant of the structure.
- 3.4-5: Where a vehicle is involved, additional information may be available.
- 3.4-6: Additional information may be available based on the Address of Record of the caller. In this context, AoR equates to the caller.
- 3.4-7: Consideration should be given to permitting users to have domain independent mechanisms to supply information related to the caller, for example, another datum related to user.

### 3.5 Validation of Civic Location

- 3.5-1: It must be possible to determine, BEFORE an emergency call is placed, if a civic address is "9-1-1 valid".
- 3.5-2: A 9-1-1 Valid Address Database, which contains all valid street addresses within a defined area, should be used as the basis to determine validity of a civic address.
- 3.5-3: A 9-1-1 valid address is defined as an address with a subset of the fields in the NENA XML address format, which when looked up in the 9-1-1 Address Validation database, yields exactly one record.

- 3.5-4: If it is determined that an address is invalid, an error diagnosis should be supplied if appropriate, as well as a contact URI for resolving errors in the database.
- 3.5-5: The 9-1-1 Valid Address Database undergoes slow changes. This must be taken into account when validating civic addresses.
- 3.5-6: The 9-1-1 Valid Address Database defined serving area boundaries may have the same characteristics as routing Req ? and ? below.
- 3.5-7: Validation information must be secured against unauthorized modification. PSAPs (or perhaps a higher level civic authority such as a county, state/province or national body) must be the only entities permitted to make changes to the database.
- 3.5-8: The fields in the 9-1-1 Address Validation database must be used as they are defined in the relevant NENA standard, including use of the Street suffix, pre and post directionals, etc. Only USPS abbreviations will be permitted in suffixes. No abbreviations are permitted in street names or community names. All fields must be populated as appropriate, including the postal community name, county name, and zipcode.
- 3.5-9: PSAPs must have access to the actual (MSAG) community name.
- 3.5-10: A postal address may be a 9-1-1 valid address if, as stated in requirement ?, a query to the 9-1-1 Address Validation Database with the postal address yields exactly one record.
- 3.5-11: The PSAP must have access to all of contents of the 9-1-1 address validation database.
- 3.5-12: The fields in the 9-1-1 Address Validation database must be used as they are defined in the relevant NENA standard, including use of the Street suffix, pre and post directionals, etc. Only USPS abbreviations will be permitted in suffixes. No abbreviations are permitted in street names or community names. All fields must be populated as appropriate, including the postal community name, legal community name, county name, state/province and zipcode.
- 3.5-13: PSAPs must have access to the actual (MSAG) community name.
- 3.5-14: A postal address may be a 9-1-1 valid address if, as stated in requirement ?, a query to the 9-1-1 Address Validation Database with the postal address yields exactly one record.
- 3.5-15: The PSAP must have access to all of the contents of the 9-1-1 address validation database.

### [3.6](#) Routing of Calls

- 3.6-1: Calls must be routed to the correct PSAP based on the location of the caller and the declared service boundary of the PSAP.
- 3.6-2: Routing must be possible on either civic or geo location information.
- 3.6-3: It must be possible to route a call based on either a civic or a geo location without requiring conversion. from one to the other. This requirement does not prohibit an implementation from converting and using the resulting conversion for routing. However, see Req ?.
- 3.6-4: It must be possible for a designated 9-1-1 authority for a PSAP to approve of any geo-coding database used to assist in determining routing of calls to that PSAP. Mechanisms must be provided for the designated 9-1-1 authority for the PSAP to test, and certify a geo-coding database as suitable for routing calls to the PSAP. The PSAP may choose to NOT avail itself of such a mechanism.
- 3.6-5: It must be possible for the designated 9-1-1 authority to supply, maintain, or approve of databases used for civic routing. Mechanisms must be provided for a designated authority for a PSAP to test and certify a civic routing database as suitable for routing calls to that PSAP.
- 3.6-6: It must be possible for the PSAP itself (or a contractor it nominates on its behalf) to provide geocode and reverse geocode data and/or conversion service to be used for routing determination. This implies definition of a standard interchange format for geocode data, and protocols to access it.
- 3.6-7: The PSAP must have a mechanism to declare its serving boundaries (in civic and geo formats) for routing purposes.
- 3.6-8: Boundaries for civic routing must be able to be specific to a street address range, a side of a street (even/odd street addresses), a building within a ôcampusö, or any of the location fields available.
- 3.6-9: It must be possible to use various combined components of the location object for determination of routing. Some areas may only require routing to a country level, others to a state/province, others to a county, or to a municipality, and so on. No assumption should be made on the granularity of

routing boundaries or about the combination of components used.

- 3.6-10: Boundaries mechanisms for geo routing must be able to be specific to a natural political boundary, a natural physical boundary (such as a river), or the boundaries listed in Req ? above

- 3.6-11: Routing databases using 9-1-1 Valid Addresses or lat/lon/altitude as keys must both be available to all entities needing to route 9-1-1 calls.
- 3.6-12: Carriers, enterprises and other entities that route emergency calls must be able to route calls from any location to its appropriate PSAP.
- 3.6-13: It must be possible for a given PSAP to decide where its calls should be routed.
- 3.6-14: It is desirable for higher level civic authorities such as a county or state/province to be able to make common routing decisions for all PSAPs within their jurisdiction. For example, a state may wish to have all emergency calls placed within that state directed to a specific URI. This does NOT imply a single answering point; further routing may occur beyond the common URI.
- 3.6-15: Routing as specified in Req ? may change on short notice due to local conditions, traffic, failures, schedule, etc.
- 3.6-16: Information and mechanisms used to determine routing must be extremely reliable and available, which implies redundancy, protocol stability, and resiliency.
- 3.6-17: Routing information must be secured against unauthorized modification. PSAPs (or perhaps a higher level civic authority such as a county, state/province or national body) or their designated representative must be the only entities permitted to change routing information.
- 3.6-18: It must be possible to supply contingency routing information, for example, an alternate URI or an E.164 to be used when normal routing fails.
- 3.6-19: Multiple types of failures may have different contingency routes.
- 3.6-20: It must be possible to provide more than one contingency route for the same type of failure

- 3.6-21: A procedure must be specified to handle default route capability when no location is available or the location information is corrupted.
- 3.6-22: Location available at the time the call is routed may not be accurate. Updates to location may result in a different route and the system must accommodate this.
- 3.6-23: Default routes must be available when location information is not available.
- 3.6-24: Access Infrastructure providers must provide a location object that is as accurate as possible when location measurement or lookup mechanisms fail.
- 3.6-25: Entities routing emergency calls shall retain information used to choose a route for subsequent error resolution.

- 3.6-26: It should be possible to have updates of location (which may occur when measuring devices provider early, but imprecise first fix location) which can change routing of calls.

### [3.7](#) Connections to the Emergency Services Network

- 3.7-1: If there is network connectivity between the emergency caller and the PSAP, and routing information is available, the call should be completed, even if other parts of the network are not reachable.

### [3.8](#) Other

- 3.8-1: There shall be no single point of failure.
- 3.8-2: Each subsystem in the i3 solution shall be designed such that the system survives major disruption including disaster, deliberate attack, and massive element failure.
- 3.8-3: Special consideration should be given to Distributed Denial of Service attacks
- 3.8-4: The solution shall include mechanisms to test each element and complete call chains from caller end device to internal PSAP systems without interfering with real emergency calls.
- 3.8-5: Mechanisms must be provided to provide constant verification of service availability to the PSAP.
- 3.8-6: Mechanism must be provided to provide automatically generated

misroute and location error reports.

Rosen & Abbott

Expires August 19, 2005

[Page 12]

---

Internet-Draft

NENA Requirements

February 2005

#### [4.](#) Security Considerations

None.

#### [5.](#) References

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

#### Authors' Addresses

Brian Rosen  
Emergicom  
470 Conrad Dr  
Mars, PA 16046  
US

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

Nadine Abbott  
Telcordia  
One Telcordia Drive, Room 4B655  
Piscataway, NJ 08854  
US

Phone: +1-732-699-6109  
Email: nabbott@telcordia.com

#### Intellectual Property Statement

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

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

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

#### Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

#### Copyright Statement

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

#### Acknowledgment

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