NENA i3
Technical Requirements Document

NENA i3 TECHNICAL REQUIREMENTS DOCUMENT
NENA 08-751, Issue 1, September 28, 2006

Prepared by:
National Emergency Number Association (NENA) VoIP/Packet Technical Committee Long Term Definition Working Group

Published by NENA
Printed in USA

NENA
TECHNICAL REQUIREMENTS DOCUMENT

NOTICE

This Technical Requirements Document (TRD) is published by the National Emergency Number Association (NENA), and is intended to be used by Standard Development Organizations (SDO) including NENA, and/or designers and manufacturers of systems that are used for the purpose of processing emergency calls. It should be considered to be a source for identifying the requirements necessary to meet the needs of the emergency services industry as it applies to the subject covered in this TRD. It is not intended to provide complete design specifications or parameters for systems that process emergency calls.

NENA reserves the right to revise this TRD for any reason including, but not limited to, conformity with criteria or standards promulgated by various agencies, utilization of advances in the state of the technical arts or to reflect changes in the design of network interfaces or services described herein. It is possible that certain advances in technology will precede any such revisions. Therefore, this TRD should not be the only source of information used. NENA members are advised to contact their telecommunications carrier representative to ensure compatibility with the 9-1-1 network.

Patents may cover the specifications, techniques or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document is not to be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics. This document is not intended to be used as a specification for the acquisition of products or services. NENA recognizes that the requirements listed here may never be satisfied by products or services from any single source.

This document has been prepared solely for the voluntary use of Standard Development Organizations (SDO) and/or designers and manufacturers of systems that are used for the purpose of processing emergency calls, as well as E9-1-1 Service System Providers, network interface and system vendors, participating telecommunications companies, etc.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Acknowledgments:

This document has been developed by the National Emergency Number Association (NENA) VoIP/Packet Technical Committee Long Term Definition Working Group.

The following industry experts and their companies are recognized for their contributions in development of this document.

Members:	**Company:**
Brian Rosen – WG Leader	NeuStar
Nate Wilcox – Tech Cmte Chair	microDATA GIS, Inc
Robert Sherry	Intrado
Pierre Desjardins	Positron
Marc Linsner	Cisco
Nadine B Abbott	Telcordia
Brian Dupres	Intrado
Roger Marshall	TCS
Henning Schulzrinne	Columbia University
Jeff Frager	Motorola
Patty McCalmont	Intrado
Michael Nelson	Intrado
Guy Roe	Mapinfo

Table of Contents

1 Executive Overview

1.1 Purpose and Scope of Document

This "NENA i3 Technical Requirements Document" is intended to specify the requirements the i3 (Long Term Definition) Standard should meet.

1.2 Reason for Issue

This document is issued to guide the development of the i3 Standard

1.3 Reason for Reissue

NENA reserves the right to modify this document. Whenever it is reissued, the reason(s) will be provided in this paragraph.

Version	Date	Reason For Changes
NENA 08-751	09/28//2006	Initial Document
NENA 08-751.1	05/30/2015	Update web page links

1.4 Recommendation for Standards Development work

This document is intended to be a reference document to guide development of a future Standard. The i3 Standards development is expected to meet the requirements contained herein.

1.5 Cost Factors

Not applicable

1.6 Acronyms/Abbreviations

This is not a glossary!! See NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents.

The following Acronyms are used in this document:	
3GPP	3rd Generation Partnership Project
ACD	Automatic Call Distribution
AES	Advanced Encryption Standard
AoR	Address Of Record
ATIS	Alliance for Telecommunications Industry Solutions
CAMA	Centralized Automatic Message Accounting
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
ECRF	Emergency Call Routing Function

The following Acronyms are used in this document:	
ESInet	Emergency Services IP Network
ESRP	Emergency Services Routing Proxy
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
IP	Internet Protocol
LIS	Location Information Server
LO	Location Object
MSC	Mobile Switching Center
MSAG	Master Street Address Guide
PIDF	Presence Information Data Format
PIDF-LO	Presence Information Data Format for Location Objects
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SONET	Synchronous Optical Network
SR	Selective Router [a.k.a., E9-1-1 Tandem, or E9-1-1 Control Office]
TCP	Transport Control Protocol
TLS	Transport Layer Security
UA	User Agent
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
USPS	United States Postal Service
UTC	Universal Coordinated Time
VF	Validation Function
VoIP	Voice over IP
VPN	Virtual Private Network
XML	eXtensible Markup Language Diffserv NAT IPv4 IPOv6,HIPPA, EPAD, MPLS, RIP, BGP, IS-IS

1.7 Intellectual Property Rights Policy

1.7.1 General Policy Statement

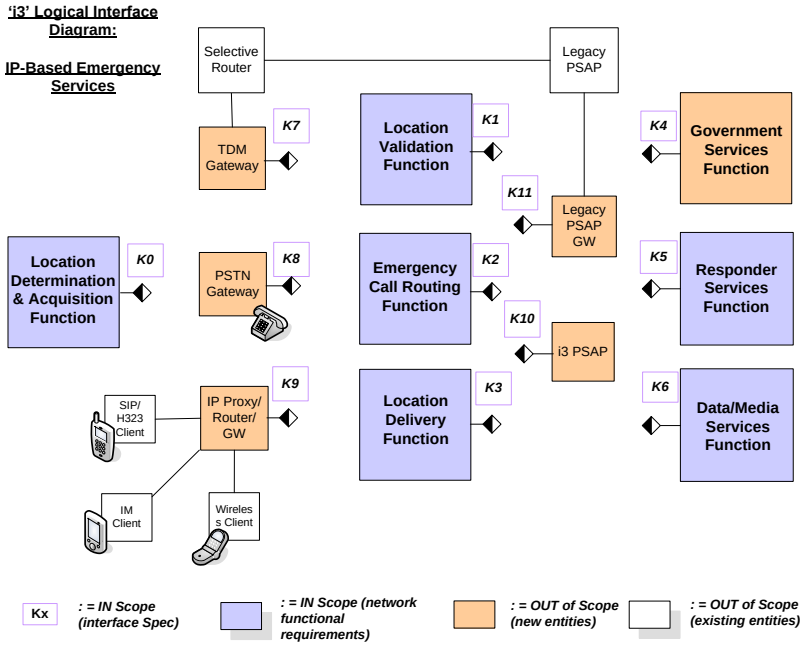
NENA takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

NENA 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:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

2 Scope



The i3 solution encompasses the definition of:

- External Interfaces between PSAPs and public/private networks delivering 9-1-1 calls to the Emergency Service system
- External Interfaces to systems and databases not in the PSAP that supply data and assistance in processing a call
- External Interfaces to systems that handle a call past the point where a call taker has exclusive control over it, such as the handoff to the Computer Aided Dispatch system
- External Interfaces to upper level management systems, such as disaster management systems, as well as peer PSAPs

Explicitly not in scope are interfaces WITHIN an i3 PSAP.

3 Architectural assumptions

For the purposes of developing requirements, we assumed the architecture of the 9-1-1 system would initially be something like:

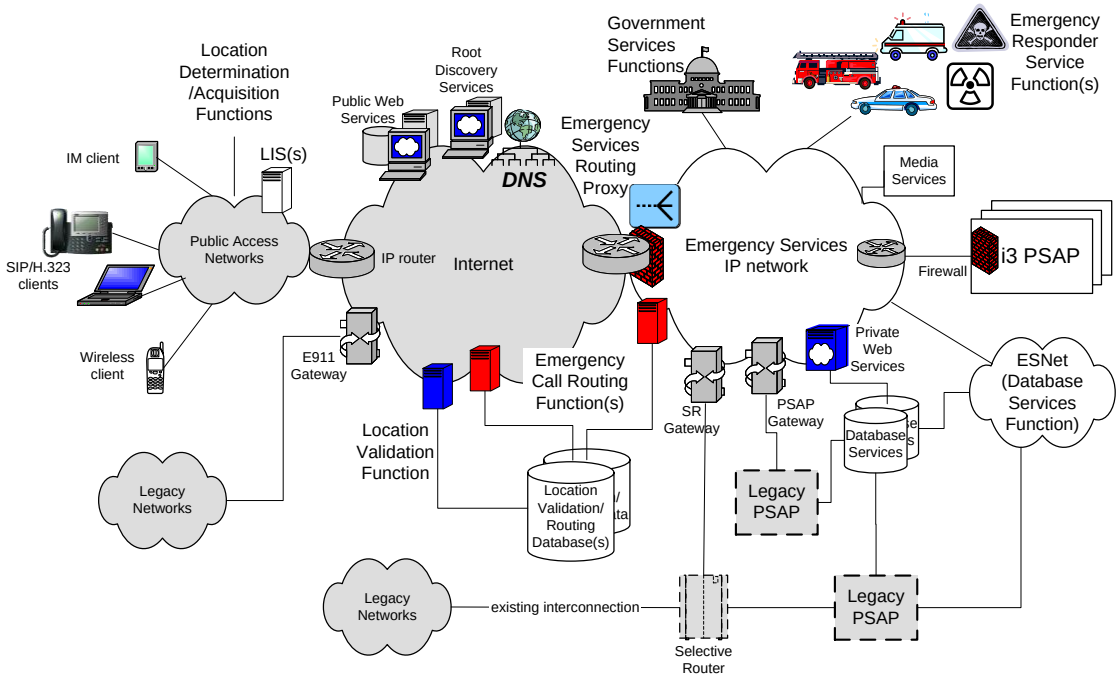


Figure 3 Example i3 Physical Architecture

Other public safety related services might be provided on the Emergency Services IP Network that are not shown on this diagram.

This architectural decomposition is not binding on the solution, but rather is provided to give the reader some help in understanding the requirements.

There is no assumption that a voice or other Communications Service Provider is in the path from the originating end terminal to the PSAP. An enterprise may directly offer calls to the system, and indeed an individual may, if they so choose, route emergency calls to the proper PSAP.

Calls may be placed on the Internet, and the Internet does not respect national boundaries, which means that calls can come from anywhere and be processed by a routing element anywhere else. Furthermore, visitors from other countries roaming into North America must be able to place calls to 9-1-1, and it is expected to be common that equipment purchased outside the U.S. will be used on U.S. originating networks. For these reasons, portions of the conforming i3 implementations (i.e. CPE) must conform to international standards for emergency calls, such as those promulgated by the IETF and others.

3.1 Description of Functional Elements

There are a number of functional elements that are part of the i3 architecture that exist and are specified outside the context of the i3 architecture. These elements are included here to provide a more complete picture of its context.

- IP client – This term is used to refer to the IP endpoint communications equipment or application that is used to originate a voice or text request for emergency services (e.g., by calling 9-1-1). The term IP device or IP endpoint may also be used.
- Routing Proxy – A term used in SIP to describe a SIP server that receives SIP requests and forwards them on behalf of the requestor. A routing proxy determines that next hop for a SIP message and forwards the message.
- User Agent (UA) – Terminology used in the context of SIP to identify the IP device. In SIP, a UA is a network element that is capable of generating SIP requests (e.g., INVITE) and is capable of generating responses for received requests.
- Legacy PSAP – This term is used to PSAPs that are not capable of communicating with VoIP protocols or of supporting the i3-based interfaces specified as part of the i3 Solution.
- PSTN Gateway – This term is used to refer to a signaling and media interconnection point between callers in the PSTN and the i3 architecture, so that i3 PSAPs are able to receive emergency calls from the PSTN and are able to communicate with legacy PSAPs (that are not equipped with a Legacy PSAP Gateway).
- Time Division Multiplexing (TDM) Gateway – This term is used to refer to the signaling and media interconnection/interworking point between the conventional Selective Router and i3 PSAPs.
- Domain Name Server (DNS) –The DNS is used in the Internet today to resolve Domain Names. The input to a DNS is a domain name (e.g., telcordia.com); the response is the IP address of the domain. The DNS allows people to use easy to remember text-based addresses and the DNS translates those names into routable IP addresses.
- Web Services – Web Services identifies an industry standard protocol for exchanges of information. In the i3 architecture, this term is being used as a catch-all for access to the sets of public and private data services to which i3 PSAPs may desire to have access.

The proposed i3 architecture includes functional elements that are specific to the needs and goals of the i3 Solution. This section summarizes these functions.

- Location Determination and Acquisition Functions – Location determination includes the functions to accurately and automatically (without input from the user) determine the position estimate of the IP endpoint device and associate that location information uniquely with that device. Location acquisition refers to the functions necessary to make that location information available to the device on request, or in the case of devices that are not location-aware, to make that location information available to a Proxy acting on behalf of that device so that location information can be used for emergency calling.
- Location Information Server (LIS) – The LIS stores a wiremap of the relationship between a unique identifier for a physical endpoint termination and a location, described as either geo-

coordinates or a civic address). The administrator/owner of the LIS is responsible for creating and maintaining this wiremap, and for ensuring that civic location data is pre-validated by a Validation Function. The LIS may be used during location determination and acquisition. The LIS may also support assignment of a location query key to a particular IP device, and download of this key to the IP device to support subsequent queries for the location from other elements in the IP domain.

- Validation Function (VF) – The VF is used to validate civic location objects against the next generation of the Master Street Address Guide (MSAG). Pre-validation of the civic location information ensures that the calls can be routed to the appropriate PSAP and that emergency services can be dispatched to the correct location.
- Emergency Call Routing Function (ECRF) – The ECRF receives location information (either civic address or geo-coordinates) as input and uses this information to provide a Uniform Resource Identifier (URI) that can be used to route an emergency call toward the appropriate PSAP for the caller's location. Depending on the identity and credentials of the entity requesting the routing information, the response may identify the PSAP, or an Emergency Services Routing Proxy that acts on behalf of the PSAP to provide final routing to the PSAP itself. The same database that is used to route a call to the correct PSAP may also be used to subsequently route the call to the correct responder, e.g., to support selective transfer capabilities.
- Root Discovery Function – The i3 databases are distributed. The Root Discovery Function is used by entities to discover the appropriate Location Validation Function or Emergency Call Routing Function for a given location.
- Emergency Services Routing Proxy (ESRP) – This ESRP is a routing proxy that may act on behalf of a group of PSAPs, to provide final routing to the PSAP, based on the caller's location. This function is not identified explicitly in the i3 functional architecture, but has been discussed in industry presentations and the concept is included in an Internet-draft, draft-schulzrinne-sipping-emergency-arch-02.txt, Emergency Services for Internet Telephony Systems, H. Schulzrinne, B. Rosen. The ESRP function is included in the example physical architecture.
- Emergency Services IP Network – This term is used to refer to a private IP network or IP Virtual Private Network (VPN) that is used for communications between PSAPs and among other entities that support or are supported by PSAPs in providing emergency call handling and response.
- i3 Public Safety Answering Point (PSAP) – The i3 PSAP is a PSAP that is capable of receiving IP-based signaling for delivery of emergency calls and for originating calls. The internal functions are not being specified in the i3 requirements, but the i3 PSAP is expected to be able to use SIP signaling for calls and IP-based data protocols for exchange of other information. It is expected that the CPE Technical Committee will produce a document describing the functionality of IP PSAP equipment.

- Legacy PSAP Gateway – This term is used to refer to the protocol and media interworking functions necessary to allow a Legacy PSAP to interface with i3 PSAPs and other entities on the Emergency Services IP network.
- Responder Services Functions – This term is used to refer to the agencies that provide emergency response in conforming i3 implementations, e.g., Police, Fire, Emergency Medical Service, Poison Control, HazMat (hazardous materials response teams), Coast Guard, etc.
- Database/Media Service Functions – This term is used to refer to the Databases and Database Access Services that provide information requested by PSAPs and other entities on the Emergency Services IP network in support of emergency services handling. Media Service functions might include such things as conference bridge resources, or logging recording services.
- Governments Services Functions – This term is used to refer to government services that might be involved in emergency call handling or escalation. Examples might include: escalation of emergency incidents that require coordination among multiple government agencies, beyond PSAPs; broadcasts; notification services; Homeland Security.
- An Emergency Services IP Network (ESInet) is a unique instance of a communications network dedicated for public safety use. An ESInet delivers emergency requests and corresponding data to emergency services providers and facilitates communication between emergency service providers and other supporting entities. An ESInet is typically deployed to support a set of PSAPs and other public safety agencies on a geographic basis. A given PSAP, or other appropriate entity, may connect to one or more ESInets. ESInets may be interconnected to facilitate emergency event handling and other related interactions.

4 Functional Requirements

4.1 Calls Directed to a PSAP

4.1.1 Signaling

Signaling 0100-0100 Session initiation (call) signaling for IP connected callers shall initially be SIP based. Other protocols are permitted if they are interworked to SIP for presenting to the PSAP. PSAPs shall not be required to accept IP calls using any protocol other than SIP. The architecture shall permit evolution to future protocols.

Signaling 0200-0100 Signaling shall be supportable over UDP and TCP with or without TLS security. PSAP policy shall govern which of these transport mechanisms are acceptable.

Signaling 0300-0100 Abandoned calls shall be captured, with location (if available) and call back information (address or TN as applicable) for presentation to the call taker.

Signaling 0400-0100 Tracking and Tracing Facilities for all calls must be provided. These include all routing entities as well as all signaling entities.

Signaling 0500-0100 Each element in conforming i3 implementations shall maintain call detail records that can be accessed by management systems to develop call statistics in real time.

Signaling 0600-0100 The PSAP shall be able to optionally control disconnect.

Signaling 0700-0100 Conforming i3 implementations must harmonize with international specifications to permit local determination of emergency call number (i.e. 9-1-1, 1-1-2)

Signaling 0800-0100 Mechanisms must be provided to route calls to areas not served by E9-1-1 to an appropriate PSTN telephone number

Signaling 0900-0100 Each element of conforming i3 implementations shall provide congestion controls

Signaling 1000-0100 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, e.g. alternate routed. (This is an existing SIP mechanism, Call History).

Signaling 1100-0100 The Emergency Services IP Network or the PSAP must accept calls from selective routers, including CAMA-like and ISDN interfaces

Signaling 1200-0100 POTS users must be capable of placing emergency calls through gateways to IP based systems.

Signaling 1300-0100 Support must be provided to accept calls from end offices and MSCs where selective routers are no longer provided, including SS7, CAMA and ISDN interfaces

Signaling 1400-0100 Call setup time (dialing of last digit to ring at the PSAP), under expected peak load shall be less than 2 seconds. If CAMA-like signaling is in the path, then an additional 7 seconds is permitted.

Signaling 1500-0100 Voice Activity Detection[1] shall be disabled for emergency calls.

4.1.2 Media

Media 0100-0100 PSAPs shall accept voice, video and text media streams on RTP transport

Media 0200-0100 The Emergency Services IP Network or the PSAP must support existing TTY devices,

Media 0300-0100 PSAPs shall have facilities to detect and react to silent calls

Media 0400-0100 It shall be possible for PSAPs to supply ringback media to callers

Media 0500-0100 It shall be possible for PSAPs to accept additional media (e.g. images) from callers without tearing down the call.

[1] Voice Activity Detection is a feature of some VoIP systems which suppress sending of media packets when audio levels drop below some threshold. In an emergency, background noise may be important, and so Voice Activity Detection should not be used

Media 0600-0100 A minimal (e.g. DiffServe) QoS mechanism shall be specified for use for media presented to or originated from the PSAP.

Media 0700-0100 i3 elements which originate media shall have media loopback mechanisms.

4.1.3 Location

Location 0100-0100 Calls using VoIP or subsequent methods are expected to supply location with the call.

Location 0200-0100 PSAPS shall accept location as civic and/or geo specified

Location 0300-0100 The format for location shall be PIDF-LO

Location 0400-0100 All representations of location shall include the capability to carry altitude and/or floor designation. This requirement does not imply altitude and/or floor designation is always used or supplied

Location 0500-0100 Altitude and/or floor designation shall be provided if available.

Location 0600-0100 The minimum required coordinate basis is WGS-84 or better

Location 0700-0100 The solution shall specify when multiple locations are permitted, what the interpretation of multiple locations shall be, and what the functional elements must do with the locations.

Location 0800-0100 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.

Location 0900-0100 The location source shall be identified and should be Authenticated.

Location 1000-0100 Systems which deploy external LISs that use keys shall provide intermediaries to query the LIS and supply the PSAP with location. The PSAP is not expected to query a LIS with a key in order to determine location.

Location 1100-0100 PSAPs shall have the ability to requery for a location update.

Location 1200-0100 PSAPs shall have the ability to subscribe to an automatic location update event for a particular call

Location 1400-0100 PSAPs shall be able to make use of fall-back location information when measurement based location determination mechanisms fail. Examples include tower/Access Point location, last known fix, etc

Location 1500-0100 PSAPs must be made aware when fall back location information was used to route a call or when it is presented to the call taker as location data.

4.1.4 Call Back Address

CallBack 0100-0100 Calls to 9-1-1 shall supply a call back address (URI, which includes the possibility of an E.164 TN expressed as a tel URI) with the call

CallBack 0200-0100 Calls must provide both a permanent address that reaches the caller and, if different, a temporary address to immediately reconnect to the caller if the call is dropped

Note: The PSAP may not receive a conventional telephone number. In the case of a VoIP caller, the URI may not have a telephone number. This has implications on how and to what extent backwards compatibility can be provided.

4.1.5 Additional Information

In addition to information sent with the call, additional information may be available that is retrieved from internal or external databases using information included with the call as a key. NENA's Future Path Plan (FPP) provides a useful classification of data that may be used to classify such data. It proposes three categories:

- Tier 1 (Essential)
- Tier 2 (Supportive)
- Tier 3 (Supplemental)

Tier 1 information is defined as "data that supports call delivery and adequate response capability." Examples include callback number and caller location. Tier 2 information is defined as information beyond essential data that may support call handling and the dispatch of a call. An example of this type of data may be vehicle information such as "vehicle rolled." Tier 3 information may supplement the call handling and dispatch, but is not necessary to complete the handling of the situation. An example may be personal medical information. Generally, we expect Tier 1 data, or a reference to it, to be delivered with the call, and Tier 2/Tier 3 data be available within the Emergency Services IP Network, or elsewhere, to be subscribed to or queried by the PSAP when needed. Such additional (Tier 2 & 3) data may also be made available to the PSAP proactively by other entities via the ESInet, meaning that the PSAP may not need to ask for it, although they would always have the ability to disregard or refuse to receive it.

AddInfo 0100-0100 Additional information may be available to the call taker based on the location of the caller, see section 4.2.1

AddInfo 0200-0100 Additional information may be available to the call taker based on the owner of the structure, see section 4.2.1

AddInfo 0300-0100 Additional information may be available to the call taker based on the tenant of the structure, see section 4.2.1

AddInfo 0400-0100 Where a vehicle is involved, additional information may be available, see section 4.2.1

AddInfo 0500-0100 Additional information may be available based on the Address of Record (AoR) of the caller. In this context, AoR equates to the caller

AddInfo 0600-0100 Consideration should be given to permitting callers to have domain independent [2] mechanisms to supply information or the scene of the incident about themselves

4.1.6 Calls placed by a third party

Calls may be originated by an entity, typically a call center on behalf of a caller. Examples include telematics, central alarm monitoring, text or video relay, and satellite systems. 3rd party call origination requires that the call be routed based on the location of the caller, and not the location of the 3rd party. Not all callers, or all 3rd parties may be VoIP capable, and some calling mechanisms (such as some Telematics systems) do not have the capability for direct call back. Thus the originator may not be able to support all of the capabilities described here.

3rdParty 0100-0100 3rd party originated calls shall be fully supported in conforming i3 implementations

3rdParty 0200-0100 PSAPs should receive an indication with the call that it is a 3rd party call

3rdParty 0300-0100 PSAPs should receive the identities of all other parties in the call. This may need to be specific to an operator in a 3rd party call center.

3rdParty 0400-0100 The call should include callback information for both the caller and the 3rd party such that the PSAP can recreate the call if it is dropped.

3rdParty 0500-0100 The 3rd party shall be able to provide supplemental information, either with the call directly, or a reference to it.

3rdParty 0600-0100 Location of the caller may come from access network of the caller or from the 3rd party

3rdParty 0700-0100 3rd parties may need authorization through an administrative process before they can place 9-1-1 calls

4.1.7 Validation of Civic Location

Validation 0100-0100 It must be possible to determine, BEFORE an emergency call is placed, if a civic address is valid.

Validation 0200-0100 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

[2] Domain independent in this context means that the entity providing information about the caller may be independent of the entity providing telephony services, and in fact that entity may provide such information regardless of which of several telephony services (home, wireless, enterprise) the caller may subscribe to provide such information regardless of which of several telephony services (home, wireless, enterprise) the caller may subscribe to.

Validation 0300-0100 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. This requirement does not preclude the validation mechanism from returning multiple 9-1-1 valid locations.

Validation 0400-0100 If it is determined that an address is invalid; an error diagnosis should be supplied to the querier if appropriate, as well as a contact URI for resolving errors in the database.

Validation 0500-0100 Methods must be provided to revalidate locations to accommodate changes to the 9-1-1 valid address data.

Validation 0600-0100 The 9-1-1 Valid Address Database defined area boundaries may have the same characteristics as Routing 0800-0100, Routing 0900-0100 and Routing 1000-0100 below.

Validation 0700-0100 Validation information must be secured against unauthorized modification. 9-1-1 Authority[3] (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.

Validation 0800-0100 The fields in the 9-1-1 Valid Address Database must be used as they are defined in the relevant NENA Standard, including use of the Street suffix, pre and post directional's, 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 zip code.

Validation 0900-0100 PSAPs must have access to the actual (MSAG) community name

Validation 1000-0100 i3 must define a process to evolve from the current MSAG to the 9-1-1 Address Validation database

Validation 1100-0100 A postal address may be a 9-1-1 valid address if, as stated in Validation 0800-0100, a query to the 9-1-1 Address Validation Database with the postal address yields exactly one record. This requirement does not preclude the validation mechanism from returning multiple 9-1-1 valid locations.

Validation 1200-0100 A current MSAG address may be a 9-1-1 valid address if the fields are fully populated as described in Validation 0800-0100 (with respect to, for example, mandatory use of street suffix and pre/post directional's, only standard USPS abbreviations permitted, etc.)

Validation 1300-0100 The PSAP must have access to all of contents of the 9-1-1 address validation database.

[3] The government agency responsible for 9-1-1 databases within a jurisdiction. There are often several PSAPs under one 9-1-1 Authority.

4.1.8 Routing of Calls

Routing 0100-0100 Calls must be routed to the correct PSAP based on the location of the caller known at the time of the call and the declared service boundary of the PSAP

Routing 0200-0100 Routing must be possible on either civic or geo

Routing 0300-0100 It must be possible to route a call from either a civic or a geo without requiring conversion. This requirement does not prohibit an implementation from converting and using the resulting conversion for routing. However, see Req 0600-0100

Routing 0400-0100 It must be possible for a designated 9-1-1 authority to approve of a geocoding database used to convert civic to geo as part of determining how to route calls to it. Mechanisms must be provided for a PSAP to test, and certify a geocoding database as suitable for routing calls to it. The PSAP may choose to NOT avail itself of such a mechanism.

Routing 0500-0100 It must be possible for the designated 9-1-1 authority to supply, maintain, or approve of databases used for civic routing including geocode data if civic routing is achieved by geocoding a civic address. Mechanisms must be provided for a PSAP to test and certify a civic routing database as suitable for routing calls to it.

Routing 0600-0100 There must be a database (K6) interface defined so that the PSAP itself (or a contractor it nominates on its behalf) may provide geocode and reverse geocode data (off line, not in real time). This implies definition of a standard interchange format for geocode data, and protocols to access it.[4]

Routing 0700-0100 There must be a mechanism to declare PSAP serving boundaries (in civic and geo formats) for routing purposes (e.g. to the administrative interface of the call routing mechanism).

Routing 0800-0100 Boundaries for civic routing must be specific to a street address range, a side of a street (even/odd street addresses), a building within a "campus", or any of the location fields available.

Routing 0900-0100 It must be possible to use various 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, and so on. No assumption should be made on the granularity of routing boundaries.

Routing 1000-0100 Boundary mechanisms for geo routing must be able to be specific to a political boundary, a natural physical boundary (such as a river), or the boundaries listed in Req 0900-0100 above

[4] Errors are likely if it is possible that two conversions of data are made. For example, if conversion is made from civic to geo for routing, and the resulting geo is converted back to civic for dispatch, an "off-by-one" error can occur. These errors can be mitigated by using the same database for each conversion. By making the PSAP's database available for conversion, such an approach could be used.

Routing 1100-0100 Routing databases using 9-1-1 Valid Addresses or lat/lon/altitude as keys must be available to all entities needing to route 9-1-1 calls

Routing 1200-0100 Carriers, enterprises and other entities that route emergency calls must be able to route calls to the appropriate Emergency Services Network based on available location information. There must be no restrictions on call originators.

Routing 1300-0100 It must be possible for any given 9-1-1 Authority to decide where its calls should be routed, and make changes to its routing policy dynamically.

Routing 1400-0100 It shall be possible 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.

Routing 1400-200 It shall be possible that certain routing information only be accessible by authorized entities

Routing 1500-0100 It shall be possible to change routing may change on short notice due to local conditions, traffic, failures, schedule, etc.

Routing 1600-0100 This requirement has been deleted

Routing 1700-0100 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) must be the only entities who can authorize a change to routing information

Routing 1800-0100 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.

Routing 1900-0100 Multiple types of failures may have different contingency routes

Routing 2000-0100 It must be possible to provide more than one contingency route for the same type of failure

Routing 2100-0100 A procedure must be specified to handle “default route” capability when no location is available or the location information is corrupted

Routing 2200-0100 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. If the call has not been answered before the update is available, the system may reroute the call automatically. After the call is answered, the PSAP may request the call be rerouted as part of a transfer operation.

Routing 2300-0100 This requirement has been deleted

Routing 2400-0100 Access Infrastructure providers must provide a location object that is as accurate as possible when location measurement or lookup mechanisms fail.

Routing 2500-0100 Entities routing emergency calls shall retain information used to choose a route for subsequent error resolution

Routing 2600-0100 It should be possible to have updates of location (which may occur when measuring devices provider early, but imprecise "first fix" location) change routing of calls. See Routing 2200-0100.

Routing 2700-0100 There shall be mechanisms to route calls to one or more alternate PSAPs when a PSAP receives a very large number of calls (which is an instance of alternate-routing)

Routing 2800-0100 Alternate-routing shall be able to be initiated by an authority designated by the PSAP

Routing 2900-0100 There shall be mechanisms to allow PSAPs to accept or refuse such alternate-routed calls. No calls shall be alternate routed to another PSAP where the destination PSAP does not accept such routing

Routing 3000-0100 Prior arrangements for alternate-routing calls shall be possible, but provisions must be made for dynamically changing such arrangements

Routing 3100-0100 Alternate-routed calls shall be capable of being bridged back to the original destination PSAP if appropriate

Routing 3200-0100 Alternate-routed calls shall be recognizable as alternate-routed before they are answered at a PSAP

Routing 3300-0100 Alternate-routing mechanisms should be designed to function well in disaster situations where loss of connectivity will be common

Routing 3400-0100 There shall be mechanisms to carry the reason for alternate routing (differentiating for example on incoming call queue busy from failure of an element) and make different routing decisions based on the reason.

Routing 3500-0100 PSAPs shall be able to specify treatment of its calls in all abnormal situations, where treatment includes return of busy indication, answering at an alternate PSAP, connection to an Interactive Voice Response Unit, etc.

Routing 3600-0100 PSAPs shall be able to accept non emergency calls placed to, for example 3-1-1[5]

4.1.9 Connections to the Emergency Services IP Network

Connections 0100-0100 If there is network connectivity between the emergency caller and a PSAP, and routing information is available, the call should go through, even if other parts of the network are not reachable.

[5] Some PSAPs are used to answer non emergency calls, sometimes only in overflow situations.

Connections 0200-0100 PSAPs shall have functions to determine the status of the Emergency Services IP Network

Connections 0300-0100 It must be possible to connect directly, via IP, to the Emergency Services IP Network, or indirectly via the Internet

4.1.10 Support of existing wireline and wireless callers

Existing 0100-0100 Backwards compatibility of existing wireline and wireless callers must be implemented

Existing 0200-0100 Support mechanisms for backwards compatibility may evolve, but at all times it must be possible to accommodate existing originating offices and mobile switching centers without requiring changes to such switches.

4.2 Databases and Services available to the PSAP to handle Calls

i3 includes interfaces that permit authorized access to information and services that are available to the PSAP through the Emergency Services IP Network. It also allows other authorized agencies and contractors[6] who need information or services that reside in the PSAP to access such data or services. These interfaces are concerned primarily with information and services pertaining to a specific call or event.

Information access by the PSAP
A variety of databases may be available to the PSAP. These databases are characterized by being associated with some key which is obtained directly or indirectly from the call, and where the response of the database is to return information that it associates with that key. An example would be retrieval of information associated with a location (c.f. Requirement 4.2.11)

Services access by the PSAP
A variety of services may be available to the PSAP. These services are characterized by actions to be taken on the PSAPs behalf, initiated by request of the PSAP, as well as notification of asynchronous events by the service to the PSAP. An example would be accessing a logging service to play back previously recorded media.

Information Access from the PSAP
Other authorized agencies or contractors may need access to data that resides in the PSAP. As with database access by the PSAP, a request may include a "key" and the response is to return information associated with the key. Other data, e.g. administrative information, may also be accessed.

[6] A contractor as used in this document is a service provider providing a service to a PSAP or other agency on the Emergency Services Network instead of the PSAP or agency providing the service itself

Service access from the PSAP
A PSAP may provide a service to other agencies or contractors connected to the Emergency Services IP Network. As with services provided to the PSAP, actions will be taken upon request of the external entity. The PSAP may also provide asynchronous event notifications.

Note: This description does not imply that there is a fundamental difference between Databases and Services. It is often the case that side effects occur resulting from a database query, e.g. invoking additional services. It is also the case that databases are often accessed and updated in performing a service. The distinction here is merely to make sure all requirements are captured.

There are a wide variety of services and databases that may be made available to PSAPs which are not specifiable by NENA. Thus, while we present requirements here, we recognize that if a PSAP desires to use a database or service defined elsewhere, it should be permitted to do so without involvement of any layer or adapter that forces the service or database to fit a single model. PSAPs should use these requirements as a guide to evaluate such services to see how compatible they may be with other, NENA-defined, databases and services.

The Emergency Services IP Network may be shared with many public safety agencies and contractors, and as such, we must define our interfaces to conform to standards agreed upon among all such agencies.

4.2.1 Information Access and Services Awareness

For a database or service to be used, it must be known to the PSAP (for databases or services accessed by the PSAP) or advertised by it (for databases or services it offers to the network). Services are provided by a domain, which we define here as a set of addressable entities under common administrative control (which might be the local Emergency Services IP Network itself, or a service provider within it. The PSAP should be able to discover services and become aware of new services as they are introduced as well as the removal existing services.

ServiceBasic 0100-0100 Databases and services shall have globally unique identifiers

ServiceBasic 0200-0100 Mechanisms for discovery of, and connection to services which MAY be used by services provided shall be specified.

ServiceBasic 0300-0100 Where there are multiple instances of the same service (same id), there must be a mechanism to identify each instance.

ServiceBasic 0400-0100 There shall be a mechanism by which an entity can determine if a particular database or service is provided, and if so, how to contact the database or service within a domain.

ServiceBasic 0500-0100 There should be a mechanism by which multiple service providers providing the same service but differentiated by a qualifier can be selected based on a specific value of the qualifier.

ServiceBasic 0600-0100 It should be possible to have the exact same service offered by multiple, competing service providers.

ServiceBasic 0700-0100 PSAPs must always opt-in to services provided on the network. No services shall be provided which a PSAP does not explicitly request, regardless of whether or not the service is free or has a cost associated with it

ServiceBasic 0800-0100 Services must inform PSAPs of its availability or non availability, both planned and unplanned.

ServiceBasic 0800-0100 Provisioning of new services to a PSAP must be graceful and not require non-related services to be affected

4.2.2 Incidents

In order that multiple databases and services may be utilized by multiple agencies in handling of calls, there needs to be ways to relate elements in some way so that correlations are possible. We use the following definitions:

Agency: an organization that is a client of a database or service.

Agent: a person employed by or contracted by an agency.

Call Request: a single communication to a PSAP that results in a defined action by a call taker. A call does not have to be a literal phone call. It could be an Instant message, a SMS text message, an Automatic Crash Alert, etc.

Incident: a defined public safety event that incurs a response within the domain of a PSAP. Examples include a traffic accident (including subsequent secondary crashes), a hazardous material spill, etc. Multiple Call Requests may be associated with an Incident

Interagency Incident: One or more incidents that span multiple PSAPs and involve multiple response agencies. A disaster involving a wide region is an example, but any incident involving more than one primary PSAP is an Interagency Incident. Multiple incidents within a PSAP may be associated with an Interagency Incident.

The life cycle of a Call Request includes: call origination, call abandonment or completion, call duration, call clearing, and post-call processing of indefinite duration.

Incident.0100-0100 It shall be possible to uniquely identify an agency within the national Emergency Services IP Network

Incident.0200-0100 It shall be possible to uniquely identify an agent within an agency

Incident.0300-0100 It shall be possible to uniquely identify a Call Request throughout its life cycle, across multiple transfers of the call among agencies

Incident.0400-0100 A PSAP or a service on the ESInet may declare an Incident

Incident.0500-0100 It shall be possible to uniquely identify an Incident throughout its life cycle.

Incident.0600-0100 It shall be possible to associate multiple calls with an Incident

Incident 0700-0100 Incidents may be declared to be within a hierarchy of incidents, where one incident has a number of subsidiary incidents associated with it. There can be an unlimited number of levels.

Incident.0800-0100 All databases and services shall make use of Agent, Agency, Call Request, Incident and Interagency Incident identifiers to uniquely associate data and events with the proper identifiers.

Incident.0900-0100 Wherever practical, database entries, accesses and updates, as well as service invocations and events shall be correlated to the appropriate call, incident or interagency incident as appropriate

Incident 1000-0100 It shall be possible to interleave messages for multiple active incidents in any order.

Incident 1100-0100 Call Requests and Incidents can be active or inactive at a specific agency. An active Call Request corresponds to an emergency service request undergoing processing by a call-taker.

Incident 1200-0100 A Call Request becomes inactive at the agency when it is declared as such by the agency, possibly causing disengagement from associated services.

4.2.3 Bridge Services

Bridge 0100-0100 Bridge services may be provided as a service on the ESInet, or may be provided internal to the PSAP.

Bridge 0200-0100 All participants in the bridge must have access to the call identifier of the original call.

Bridge 0300-0100 Information gathered by one agency on the call request must be available to other agencies being bridged. It must be possible for the bridged agency to be made aware such information exists.

Bridge 0400-0100 Any agency on the call must be made aware of any other agencies (or external participant) bridged to the call.

Bridge 0500-0100 Provision for bridging agencies that are only accessible via Selective Router or PSTN must be defined

Bridge 0600-0100 An i3 PSAP must be able to transfer or bridge a call to or from any PSAP, including internationally, with all data that accompanied the call (e.g. location)

Bridge 0700-0100 The call-taker must be able to control what the caller hears while bridge/transfer operations are completed.

4.2.4 Information Discrepancy Service

In any service or database there is the potential for a discrepancy noted by the user of the data or service. This includes a misroute of a Call Request. An information discrepancy service allows this discrepancy to be sent to the appropriate administrative agency for correction. The agency then may return a tracking ticket and notify the using agency of the disposition.

Discrepancy 0100-0100 Databases and services should include a mechanism for an agency using the database or service to report any discrepancy it noted, specifically inclusive of misrouted information.

Discrepancy 0200-0100 A method for including free form text must be included in a discrepancy report.

Discrepancy 0300-0100 Once the receiving agency receives the information discrepancy report it shall return an identifier for the discrepancy to the using agency.

Discrepancy 0400-0100 Once the information discrepancy is resolved by the managing agency a status report shall be sent to the using agency.

Discrepancy 0500-0100 i3 shall define a standardized mechanism for this purpose which should be used by databases and services that do not have a valid reason for using another method

Discrepancy 0600-0100 Discrepancy reports and status reports should have at least one free text field

4.2.5 Report and Status Services

Report 0100-0100 Where a response to a request may take significant time to complete, databases and services should provide status reporting mechanisms to allow the requestor to determine the status of an outstanding request

Report 0200-0100 Where appropriate, services should provide mechanisms to request historical reports

Report 0300-0100 Where appropriate, services should provide mechanisms to request configuration reports

Report 0400-0100 Where appropriate, services should provide mechanisms to request reports by type of incident, location of incident (Geo or civic) and date range to allow authorities to map incidents by geographic area.

4.2.6 Network Requirements

The Emergency Services IP Network is expected to be an internetwork (network of networks) of IP networks joined by routers. Logically, the local Emergency Services IP Network joins all public safety agencies in a jurisdiction, and that local network is interconnected, perhaps to neighboring jurisdictions. Physically, the Emergency Services IP Network will consist of several networks, with different layer 2 mechanisms, including wireline, wireless, government owned facilities, leased private facilities, virtual private networks, etc. The network should be managed to be as secure as practical. However, no element of the network should assume that it is secure. The network between the PSAP and the ESInet will be a private or virtual private network based upon TCP/IP. It will have scalable bandwidth to support new enhanced services. The network must be robust to support all categories of media, including text, graphics and video based upon the applications that are supported. The Emergency Services Network is connected to the Internet through firewalls.

Network.0100-0100 The Network connectivity between the PSAP and the ESInet shall be a private or virtual private network based upon TCP/IP.

Network.0200-0100 The protocols and the corresponding networks shall be capable of supporting the transmission of images, video, high resolution graphics, non real time voice, and other capabilities.

Network.0300-0100 Connections between the PSAP and ESInet shall be secured TCP/IP connections such that advanced authorization, authentication and security features can be implemented.

Network.0400-0100 DiffServ Code Points to be used for PSAP needs shall be specified

Network.0500-0100 NAT may be required in some jurisdictions between the Emergency Services IP Network and the Internet, so all services intending to use Internet connections must assume NAT.

Network.0600-0100 i3 defined service applications must be capable of operating on IPv4 and IPv6 network infrastructures.

4.2.7 Protocol Requirements

The protocols between the PSAP and ESInet will be bi-directional to support the new services that will be implemented. The protocols should allow end points to discover each other. Where standards exist, they should be used instead of special-purpose protocol specifications, wherever possible. This does not preclude 3GPP, ESIF or NENA-specified application protocol interfaces for services and data exchanges.

Protocol.0100-0100 Domain names (DNS) should be used in preference to IP addresses

Protocol.0200-0100 Application interfaces should have versions, and versions should be negotiable.

Protocol.0300-0100 Mechanisms used in failure and recovery situations shall be capable of being exercised to ensure they are operating properly.

Protocol.0400-0100 Services should be designed such that making a service available or unavailable shall not affect any other service not dependent on it. This may be an obligation on both the client and the server.

Protocol 0500-0100 Reliable services should be designed such that failure of a server shall not affect the service.

Protocol.0600-0100 Redundancy mechanism specification of a service must include what granularity of transaction integrity is provided. Database access systems might use two phase commit with rollback. SIP might use a paradigm where calls that are signaled complete stay up, calls that initiate after failure go through, calls in the middle of signaling establishment fail and must be retried.

4.2.8 Security/Privacy

Databases and Services should require authentication before use. Authentication may be by agency, for databases and services that are not specific to a person within the agency, or by person, which are specific to a person. Authentication requires credentials. Authorization specifies what actions or access is permitted and is subject to policy of both ends. Integrity protection insures messages sent across the network cannot be forged or modified without detection. Privacy prohibits reading messages when not authorized to do so.

Databases containing sensitive information and Services which provide sensitive functionality require suitable authentication and access restrictions for use. Authentication may take several forms and may apply on a personal level or agency level. Person-based authentication schemes may incorporate such mechanisms as passwords, smartcards or tokens. Agency based authentication schemes may employ such mechanisms as system-to-system authentication via x.509 digital certificates.

Access rules and restrictions must be employed by sensitive databases and services to ensure that actions taken within the system are limited to only authorized personnel and agencies. It is the responsibility of database and service operators to ensure that personnel and/or agencies have been authenticated and access controls are applied to a level of satisfaction appropriate to the sensitivity of the database or service.

Security.0100-0100 Elements connected to the ESInet which provide access to sensitive data or services shall require users and/or their agencies to be authenticated prior to being granted access to such element.

Security 0200-0100 Authentication shall be by agency or by person, depending on the nature of the database or service provided. Person authentication is preferred in order to provide accountability for actions taken by personnel in the network.

Security 0300-0100 The specific authentication mechanisms for the Emergency Services IP Network should be that agreed to among public safety agencies. The specific credentialing mechanisms employed should be as agreed to.

Security 0400-0100 i3 shall define credentialing mechanisms for agencies and employees/contractors within those agencies

Security 0500-0100 Credentials issued per Security 0400-0100 should be used for database access and service authentication

Security 0600-0100 Person-based authentication mechanisms shall be provided to support password-only (weak) or two-factor (strong) user authentication between a PSAP CPE and ESInet based on the configuration of the ESInet.

Security 0700-0200 Password based authentication mechanisms shall protect the password such that it is possible for the user to prove knowledge of the password without transmitting the password.

Security 0800-0100 It must be possible for security-sensitive actions taken within the network to be associated with a person or agency in a manner that provides non-repudiation by the responsible party. Such actions must be historically traceable back to the responsible party in a manner that provides non-repudiation by the responsible party of the accuracy of the historical information.

Security 0900-0100 Proxy authentication should be used so that "Single Sign On" can be achieved.

Security 1000-0100 All sensitive communications over the Emergency Services IP Network that directly relate to emergency databases and services shall be protected by suitable Integrity Protection mechanisms.

Security 1100-0100 All sensitive communications over the Emergency Services IP Network that directly relate to emergency databases and services shall be protected by suitable Privacy mechanisms.

Security 1200-0100 The mechanisms chosen for Security requirements above shall use multiagency standards wherever possible

Security 2100-0100 i3 implementations should adhere to existing national standards and best practices in security.

Security 2100-0200 Signaling and control elements of i3 implementations should conform to the standards and practices set forth in Generic Signaling and Control Plane Security Requirements for Evolving Networks Standard [American National Standard ATIS-1000007].

Security 2100-0300 Management systems and network elements of i3 implementations should conform to the standards and practices set forth in Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane [American National Standard T1.276-2003]

4.2.9 Maintenance

External interfaces between the PSAP and databases and services should incorporate best practices to maintain maximum system availability. Hardware elements should be able to come into service and go out of service without impacting the overall service availability.

Maintenance 0100-0100 Mechanisms in protocols and services must incorporate methods for each end to monitor the health of the other. .Specific services may be designated as non critical and thus exempt from this requirement

Maintenance 0200-0100 Any device with an external interface, or any database or service available via an external interface shall be capable of being brought into or out of service without affecting other databases or services not dependent on it.

Maintenance 0300-0100 Hardware elements of high availability services shall be capable of being brought into or out of service without affecting the overall service availability

Maintenance 0400-0100 A mechanism shall be defined to advise management and/or users of impending maintenance service activities for non-high availability services.

Maintenance 0500-0100 Integrity and authenticity of data in databases accessible to any party must be capable of being verified by that party

Maintenance 0600-0100 Any device or database service must be capable of having its software upgraded without affecting the availability of the device or service.

4.2.10 Additional Data

Information will be available to PSAPs that is not necessarily delivered with the call, but is associated with the location, caller or call.

AdditionalData 0100-0100 Mechanisms for providing additional data must be made available to the PSAP

AdditionalData 0200-0100 PSAPs must request such data, either at the time it wishes to get the data, or as part of service enrollment

AdditionalData 0300-0100 Additional Data may be located within the Emergency Services IP Network, or in public networks

AdditionalData 0400-0100 Mechanisms must be provided to require authentication prior to being authorized to access additional data

AdditionalData 0500-0100 Mechanisms must be provided to protect additional data privacy.

AdditionalData 0600-0100 Where additional data is not stored in the PSAP, and the data is relatively static, mechanisms must be provided that allow a PSAP to cache the data for fast retrieval under times of system stress (such as disasters).

AdditionalData 0700-0100 Processes must be established to standardize representation of additional data, which must involve the owners/creators of that data

AdditionalData 0800-0100 Information provided on the call must be sufficient to locate information associated with the location, caller or call.

AdditionalData 0900-0100 Additional Data may be provided by other agencies or services in the Emergency Services IP Network

4.2.11 Additional Data associated with a location

AdditionalLocationData 0100-0100 Distinction must be made between data associated with a building or campus and a tenant of such a building or tenant. Each source may have different additional data

AdditionalLocationData 0200-0100 There must be a mechanism to determine the tenant from the building owner/manager for a call in order to correctly query for tenant specific additional data

4.2.12 Additional Data associated with a caller

AdditionalCallerData 0100-0100 Mechanisms must be provided to support additional data associated with the Address of Record of the caller

AdditionalCallerData 0200-0100 Information associated with a caller must be opt-in by the caller only

AdditionalCallerData 0300-0100 Information associated with a caller may include Private Health Information as defined in the HIPAA and mechanisms must be provided to protect that data according to that rule <ref, abbbr>

4.2.13 Additional Data associated with a call

AdditionalCallData 0100-0100 Mechanisms must be provided to support additional data associated with the call

4.2.14 Other

OtherData 0100-0100 Mechanisms must be provided to implement NCIC queries from call takers (PSAP policy controller).

OtherData 0200-0100 Mechanisms must be provided to support external services not directly tied to a call

4.3 Connections to Downstream Systems

4.3.1 Choosing a Responder

ChooseResponder 0100-0100 The i3 PSAP shall be capable of associating an indefinite number of responders with a location

ChooseResponder 0200-0100 The service boundaries of responders shall be specifiable in polygon and/or civic address forms.

ChooseResponder 0300-0100 There shall be no assumptions made concerning alignment of responder service boundaries to PSAP service boundaries, any political boundary or the service boundary of any other responder.

ChooseResponder 0400-0100 Responders shall be classified into a list maintained by NENA. Examples of classifications would be police, fire, EMS, poison control, animal control

ChooseResponder 0500-0100 It shall be possible for more than one responder to provide the same classification of service to the same location.

ChooseResponder 0600-0100 It should be possible to have specialties within a classification based on specific capabilities of a responder

ChooseResponder 0700-0100 The PSAP shall be able to determine the Display Name (English Language Translation), classification, for a responder

ChooseResponder 0800-0100 The i3 PSAP shall be capable of bridging/transferring a call to any responder(s) associated with the call without placing the call requester on hold

ChooseResponder 0900-0100 The i3 PSAP shall be capable of bridging/transferring a call to any PSTN or VoIP address

ChooseResponder 1000-0100 For responders that are connected to the PSAP via VoIP, all information received with the call shall be sent with the transfer/bridge

ChooseResponder 1100-0100 Any information entered/created by the call taker shall be made available to the responder.

ChooseResponder 1200-0100 For responders that are connected to the PSAP via the Selective Router introduction of i3 must not cause them to lose functionality they have now.

ChooseResponder 1300-0100 Responders must have access (subject to appropriate authentication and access controls) to data associated with a location, caller or call.

ChooseResponder 1400-0100 Responder selection shall be capable of working independently of the type of originating network. This implies the i3 responder selection mechanisms should work on calls to the PSAP arriving via a selective router. This requirement does not preclude an implementation from also supporting ALI based ESN selection of responders.

ChooseResponder 1500-0100 Any media stream (voice, video, text or image) received by the PSAP shall be bridgeable/forwardable to responders if it is capable of receiving them.

ChooseResponder 1600-0100 Call takers shall be able to communicate with dispatchers of any responder via voice, video or text if the responder is capable of it.

4.3.2 Other disposition of calls

OtherDisposition 0100-0100 A PSAP must be able to control disposition of calls not answered by a call taker. Such dispositions include queuing a call, returning a busy indication, connecting the call to an Interactive Voice/Text Response Unit, or routing the call to an alternate PSAP.

OtherDisposition 0200-0100 Treatment of calls as per OtherDisposition 0100-0100 may be dependent on the media request of the caller

OtherDisposition 0300-0100 PSAPs shall be notified of abandoned calls, and be able to obtain location and call back information included for such calls

OtherDisposition 0400-0100 Sessions to PSAPs shall have mechanisms to determine if a call is dropped without normal termination messaging

OtherDisposition 0500-0100 PSAPs shall be able to accept non emergency calls placed to, for example 3-1-1

OtherDisposition 0600-0100 Non emergency calls shall be capable of being differentiated from emergency calls

OtherDisposition 0700-0100 PSAPs shall have the capability to apply different call treatments (per OtherDisposition 0100-0100) to non emergency calls, specifically, where queuing services are provided, non emergency calls may require separate queues.

OtherDisposition 0800-0100 PSAPs shall be provided mechanisms to deal with large volumes of fraudulent calls as part of a deliberate attack on the PSAP.

OtherDisposition 0900-0100 Mechanisms shall be provided to recognize non emergency calls marked with priority (for example, the SIP Resource Priority Header), and provide different disposition of such calls from unmarked calls

4.3.3 Computer Aided Dispatch

CAD 0100-0100 Support for existing NENA CAD interfaces must be provided

CAD 0200-0100 A new CAD interface providing facilities commensurate with the data and signaling requirements presented herein shall be specified.

4.4 Connections to Local, Regional, State and Federal Authorities and peer connections

Exterior 0100-0100 It shall be possible for authorities superior to a PSAP to have visibility into events occurring within the PSAP, such as unusual call volume, significant failures, etc.

Exterior 0200-0100 It shall be possible for Incident information as defined in Section 4.2.2 to be made available to higher level authorities.

Exterior 0300-0101 0100 It shall be possible for a PSAP to provide or receive Incident information as defined above to/from other PSAPs

Exterior 0400-0100 Services available from other authorities (e.g. NCIC queries) should be available to PSAPs on the Emergency Services IP Network as any other service described herein

4.4.1 Disaster Management

Disaster 0100-0100 PSAPs shall have interfaces to EPAD (and similar event notification systems) to both accept and generate events.

Disaster 0200-0100 Routing of calls in a disaster shall be one of the cases of alternate routing detailed in Section 4.1.8

4.4.2 PSAP Backup/Failover

BackUp/Failover 0100-0100 When a PSAP fails, calls intended to route to it shall route to one or more designated PSAP(s)

BackUp/Failover 0200-0100 There must be a mechanism to allow PSAPs to designate its backup PSAP(s), and such PSAP(s) must agree to provide backup service

BackUp/Failover 0300-0100 Calls arriving from a failed PSAP must be identifiable by the backup PSAP as being failover calls

BackUp/Failover 0400-0100 When a failed PSAP with backup arrangements activated comes back in service, a graceful transition to the revived PSAP must occur

BackUp/Failover 0500-0100 It must be possible to have a redundant (duplicate) PSAP that is capable of immediately taking over responsibility for a failed PSAP

BackUp/Failover 0600-0100 Security mechanisms designed to assure identity of PSAPs must work reasonably well when backup PSAPs are processing calls for a failed PSAP[7].

BackUp/Failover 0700-0100 It must be possible for the backup PSAP to transfer calls and data associated with calls to any of the dispatch functions the failed PSAP could. Capabilities at the backup PSAP may limit the functionality the backup can provide.

BackUp/Failover 0800-0100 No assumptions should be made on where the backup PSAP is located, Specifically, the backup PSAP may not be on the same Emergency Services IP Network as the failed PSAP.

[7] For example, a secret key, such as the private key of a public key cryptosystem would have to be shared with a backup PSAP.

4.5 Other

Other 0100-0100 An Intra/Inter PSAP Instant Messaging system shall be specified with connections to similar systems available to responder dispatcher/management

Other 0200-0100 There shall be no single point of failure in conforming i3 implementations. Specific services could be designated as non critical and thus exempt from this requirement

Other 0300-0100 Each subsystem in conforming i3 implementations shall be designed such that the system survives major disruption including disaster, deliberate attack, and massive element failure.

Other 0400-0100 Mechanisms to mitigate "Distributed Denial of Service" attacks or similar malicious situations shall be specified

Other 0500-0100 All databases used by conforming i3 implementations shall support manual query (under PSAP policy control and within any local or state law) to the call taker or management systems.

Other 0600-0100 A service must be defined to log all media and all events with timestamps such that a complete picture of a call can be reconstructed from the log after the call.

Other 0700-0100 Mechanisms to test each element and complete call chains from caller end device to internal PSAP systems without interfering with real emergency calls shall be specified

Other 0800-0100 A mechanism must be specified to achieve synchronized time across multiple devices, services and agencies.

5 References

[1] IETF RFC 1032, *Establishing a Domain – Guidelines for Administrators*, M. Stahl, November 1987.

[2] IETF RFC 1033, *Domain Administrators Operations Guide*, M. Lottor, November 1987.

[3] IETF RFC 1035, *Domain Names – Implementation and Specification*, P. Mockapetris, November 1987.

[4] IETF RFC 2131, *Dynamic Host Configuration Protocol*, R. Droms, March 1997.

[5] IETF RFC 3261, *SIP: Session Initiation Protocol*, June 2002.

[6] IETF RFC 3825, *Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information, July 2004*

[7] Internet draft, *DHCP Option for Civil Addresses*, Henning Schulzrinne, July 2004, draft-ietf-geopriv-dhcp-civil-02

[8] Internet draft, *A Presence-based GEOPRIV Location Object Format*, J. Peterson, May 2004, draft-ietf-geopriv-pidf-lo-02

[9] Internet draft, *Emergency Services for Internet Telephony Systems*, H. Schulzrinne, B. Rosen, July 18, 2004, draft-schulzrinne-sipping-emergency-arch-01, Section 14.2.

[10] Generic Signaling and Control Plane Security Requirements for Evolving Networks Standard, American National Standard ATIS-1000007

[11] Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane, American National Standard T1.276-2003

[12] 3GPP TS 23.167, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions

6 Appendix A Recommendations for designing Emergency Services IP Networks

Although NENA will not specify how an ESInet should be built, it will provide guidance to 9-1-1 authorities who will be specifying their own networks. This section details requirements for such guidance.

Network.0600-0100 The Emergency Services IP Network shall be a conventional routed IP network (use of MPLS or other "SubIP" mechanisms is permitted as appropriate)

Network.0700-0100 The PSAP should use redundant local area networks for reliability

Network.0800-0100 The connection from the PSAP Local Area Network to the Emergency Services IP Network must be redundant, physically diverse, and logically separate.

Network.0900-0100 It is recommended that the PSAP have at least two entirely different physical connections, which use diverse facilities. For example, an ideal arrangement would be to have the PSAP directly connected to a SONET ring, and to also have an independent fiber or other high bandwidth connection to an entirely separate network with no facilities shared between the SONET ring and the backup facility; for example, a fiber connection from the local cable company or a government owned multimegabit microwave system.

Network.1000-0100 The Emergency Services IP Network shall be engineered to sustain real time traffic, including data, audio and video. <merge them>

Network.1100-0100 The Emergency Services IP Network shall implement DiffServ (RFC2474 & 2475) and may implement IntServ (RFC2205)

Network.1300-0100 The Routers between the PSAP and the Emergency Services IP Network shall support at least RIP (RFC?)

Network.1400-0100 The Routers between the PSAP and the Emergency Services IP Network should support BGP and ISIS

Network.1400-0100 No NAT should be used between the PSAP and the rest of the Emergency Services IP Network.