Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)

NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)
NENA 08-001, Issue 1 December 6, 2005

Prepared by:
National Emergency Number Association (NENA) VoIP-Packet Technical Committee

Published by NENA
Printed in USA

NENA STANDARD

NOTICE

This NENA STANDARD is published by National Emergency Number Association **(NENA)** as a guide for the designers and manufacturers of systems that are used for the purpose of processing emergency calls. It is not intended to provide complete design specifications or parameters nor to assure the quality of performance of such equipment.

NENA reserves the right to revise this NENA STANDARD 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 equipment or services described herein.

It is possible that certain advances in technology will precede these revisions. Therefore, this NENA STANDARD 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 has been prepared solely for the voluntary use of E9-1-1 Service System Providers, network interface and system vendors, participating telephone 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 Technical Committee has developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
4350 N Fairfax Dr, Suite 750
Arlington, VA 22203-1695
800-332-3911
or: techdoccomments@nena.org

Acknowledgments:

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

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

Members:	**Company**
Anand Akundi – Co-Work Group Leader and Technical Editor	Telcordia Technologies
Mark Lewis – Co-Work Group Leader	Nortel Networks
Nate Wilcox – VoIP/Packet Technical Chair	State of Vermont 9-1-1
Nadine Abbott	Telcordia Technologies
Delaine Arnold	Arnold 9-1-1 Consulting
Ric Atkins	Tarrant County 9-1-1 District
Erica Aubut	State of Vermont 9-1-1
Tim Barry	AT&T
Marc Berryman	Greater Harris County 9-1-1
Paul Binder	T-Mobile
Patty Bluhm	HBF Group
Dean Bordens	SBC
Tom Breen	Bellsouth
Tom Browne	HBF Group
Guy Caron	Bell Canada
Larry Ciesla	Intrado
Martin Dawson	Nortel Networks
Carol DeFazio	Telcordia Technologies
Martin Dolly	ATT
Jerry Eisner	Intrado
Tom Hicks	Intrado
Bill Horne	Tarrant County 9-1-1
Dick Khan	SBC
Marc Linsner	Cisco
Bill Marczac	Bellsouth
Roger Marshall	TCS
Jeff Martin	TCS
Ken Maynard	Bexar Metro 9-1-1 Metro District
Paul Mallett	CSEC
Patti McCalmont	Intrado
Dave Morris	Verizon
Theresa Reese	Telcordia Technologies

Brian Rosen	Emericom
John Rosenberg	Lucent
John Savaglio	SBC
Carl Smith	Intrado
Paul Stoffels	SBC
Chuck Thompson	C.P. Thompson Limited
Larry Truesdale	Nortel Networks
Greg Welenson	Vonage
James Winterbottom	Nortel Networks

TABLE OF CONTENTS

1 Executive Overview

Voice over Internet Protocol (VoIP) is poised to become the predominant technology used in the telecommunications industry. As the public adopts VoIP, E9-1-1 calls will increasingly originate from VoIP users. Some VoIP telecommunications service provider networks, however, are not natively compatible with the existing E9-1-1 infrastructure. This document was developed to outline an interim architecture to connect callers in the IP domain with Public Safety Answering Points (PSAPs) supported by the existing E9-1-1 Service Provider network.

1.1 Purpose and Scope of Document

This document is the NENA recommended standard for the i2 architecture to support the interconnection of VoIP domains with the existing Emergency Services Network infrastructure in support of the migration toward end-to-end emergency calling over the VoIP networks between callers and PSAPs.

This document provides an overview of the VoIP architecture, functional elements, and interfaces, as well as the interface specifications necessary for interconnection with the existing Emergency Services Network infrastructure.

This document does not include specifications for the methods used to determine location nor how the endpoint actually receives location.

1.2 Reason to Implement

VoIP is being introduced into the North American environment by VoIP Service Providers (VSPs). NENA and a number of the VSP's acting through the Voice on the Net (VON) Coalition reached agreement to support current NENA and industry work towards long-term solutions that include (a) delivery of 9-1-1 calls to the proper PSAP; (b) providing callback number/contact information to the PSAP; (c) providing the location of the caller; and (d) PSAPs having direct IP connectivity. The initial standards development work of the NENA VoIP/Packet Committee was to be completed by the end of 1Q05. This architecture embodies that initial work.

This recommended standard is being provided to facilitate the development and implementation of interoperable, standard equipment and processes to support VoIP emergency services calling throughout North America.

1.3 Benefits

Use of this document will:

- Ensure that equipment and service providers that conform to these recommendations will have a solution that is interoperable,
- Foster development of network elements and processes that can be reused in the architecture that supports end-to-end IP calling to the PSAP.

1.4 Operational Impacts Summary

Operational impacts include:

- Additional data provided to the PSAP. In order to differentiate VoIP emergency calling, VoIP calls will be distinguishable and new data elements pertinent to VoIP calls will be provided to call takers. This may impact both call taking procedures and training of call takers.
- New processes required. Call routing will be based on the caller's location which will be matched to routing information contained in routing databases. With this architecture, VoIP caller addresses may not be stored in Automatic Location Identification (ALI) databases, but must still be Master Street Address Guide (MSAG) valid. This will require comparison with information contained in new validation databases. New processes to populate and maintain these routing and validation databases must be developed and implemented.
- Default Routing. Some calls will be placed without location information available, making location-based routing virtually impossible. Some form of default routing for those calls will have to be implemented. Handling of those calls will have operational implications for the PSAPs receiving the calls.

1.5 Document Terminology

The terms "shall ", "must " and "required" are used throughout this document to indicate required parameters and to differentiate from those parameters that are recommendations. Recommendations are identified by the words "desirable" or "preferably."

1.6 Reason for Issue

This document is issued to identify the minimum requirements and desirable network elements for VSP interconnection with the E9-1-1 Service Provider infrastructure for delivery of emergency calls and associated callback, location, and service provider information, equivalent to conventional wireline and wireless callers.

1.7 Reason for Reissue

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

1.8 Date Compliance

All systems that are associated with the 9-1-1 process shall be designed and engineered to ensure that no detrimental, or other noticeable impact of any kind, will occur as a result of a date/time change up to 30 years subsequent to the manufacture of the system. This shall include embedded application, computer-based or any other type application.

To ensure true compliance the manufacturer shall upon request provide verifiable test results to an industry acceptable test plan such as Telcordia GR-2945-CORE or equivalent.

1.9 Anticipated Timeline

This architecture is intended to be implemented in the near term. It provides the technological approach required to meet the objectives agreed to by NENA and the VON Coalition. Prior to implementation, further agreement must be reached on roles and responsibilities for developing, operating and maintaining the network elements called for in the architecture.

1.10 Costs Factors

Implementation of the architecture outlined in this document will require the deployment of a number of new network elements. Each of the new elements must be provisioned, operated, and maintained. In addition new databases are required, which will further require the development and maintenance of new supporting processes.

1.11 Cost Recovery Considerations

Traditionally, much of the cost of the existing E9-1-1 Service Provider infrastructure has been supported through the collection of fees and surcharges on wireline and wireless telephone service. New network elements in the IP Domain will need to be paid for in some manner. Additionally, as VoIP service replaces traditional voice services that currently support the E9-1-1 Service Provider infrastructure, existing fee collections will decline and must be replaced.

1.12 Acronyms/Abbreviations

This is not a glossary. See NENA 01-002 - 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:	
ALI DB	Automatic Location Identification Database
ANI	Automatic Number Identification
CRN	Contingency Routing Number
DHCP	Dynamic Host Configuration Protocol
ERDB	ESZ Routing Data Base
ESGW	Emergency Services Gateway
ESN	Emergency Service Number
ESQK	Emergency Services Query Key
ESRN	Emergency Services Routing Number/Name
ESZ	Emergency Services Zone
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
IP	Internet Protocol
LIE	Location Information Element
LIS	Location Information Server

The following Acronyms are used in this document:	
LIS-ID	Location Information Server Identifier
LK	Location Key
LO	Location Object
LRO	Last Routing Option
MPC	Mobile Positioning Center
MSAG	Master Street Address Guide
PIDF	Presence Information Data Format
PIDF-LO	Presence Information Data Format - Location Objects
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RDO	Route Discovery Operator
RFC	Request for Comments
RPC	Remote Procedure Call
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SR	Selective Router [a.k.a., E9-1-1 Tandem, or E9-1-1 Control Office]
SRDB	Selective Routing Database
TDM	Time Division Multiplexing
TLS	Transport Layer Security
UA	User Agent
UDDI	Universal Description, Discovery and Integration
URI	Uniform Resource Identifier
USPS	United States Postal Service
UTC	Universal Coordinated Time
VDB	Validation Data Base
VEP	VoIP End Point
VESA	Valid Emergency Services Authority
VoIP	Voice over IP
VPC	VoIP Positioning Center
VSP	VoIP Service Provider
WSDL	Web Service Definition Language
XML	eXtensible Markup Language

2 Architecture

This section provides an overview of the i2 migratory solution architecture recommended by NENA for supporting emergency calls originated in the IP domain and terminated using the PSTN emergency services infrastructure.

2.1 General Assumptions

1. It is assumed that one goal of the i2 solution architecture is to make no changes that will affect the PSAP.
2. It is assumed that one goal of the i2 solution architecture is to minimize changes in the existing Emergency Services Provider infrastructure, although the i2 architecture does not preclude Emergency Services Providers from providing additional services in the IP domain.
3. It is assumed that existing processes used for wireless carriers can be used to cause the Selective Routing Databases (SRDBs) and ALI DBs to be populated with the appropriate shell records for the Emergency Services Query Keys (ESQKs) used in this architecture.
4. The i2 solution supports the receipt of both civic and geodetic location information as input to emergency call routing decisions. This enables the solution to route calls regardless of the format of the location provided by the source. It is expected that the location provided by the originating network and chosen for routing purposes by the VPC will be the location that is provided to the PSAP. The location provided to the PSAP will be in the same form (civic or geo) that was received.
5. The call setup signaling in the IP domain described in this document uses Session Initiation Protocol (SIP) as specified in IETF Request For Comments (RFC) 3261[5] (plus other supporting work in IETF), and additional requirements described or identified in this standard. Where IP domains use other protocols (e.g., ITU-T H.323), it is assumed that they will support emergency parameters (e.g. location) for inter-working with various interfaces and with SIP when required.
6. A Valid Emergency Services Authority (VESA) registry will be used to provide certification of entities that are authorized to query for and view location information for any given emergency call instance it is requested to process.
7. The various agencies that are needed to play a role for this solution to work will step up to their roles and responsibilities.
8. Location information may, in general, be presented by the VoIP end point by one of two methods: Civic or geo. **However, civic location is required for non-wireless fixed and nomadic types of service, with geodetic location optionally sent as supplemental information in addition to the civic location for these service types.** Civic location presented to the PSAP is expected to be MSAG Validated.

Refer to next section for additional assumptions about the Phase i2 solution architecture and relationships between entities in the architecture.

2.2 Overview of Interconnection to Conventional E9-1-1 Systems

This section provides an overview of the interconnection between the IP domains and the existing E9-1-1 Emergency Services Provider infrastructure.

Figure 2-1 illustrates the functional elements and signaling interfaces used to support the i2 solution. The acronyms used to label elements in the diagram are defined in the NENA Master Glossary and in Section 1.12 of this standard. On the left of the figure are the functional elements of the IP domain. Some of these represent functional elements used in the SIP architecture and are defined in IETF RFC 3261[5].

Several new functions are introduced in the i2 solution that assist in:

- determination and validation of location information,
- routing emergency calls to the appropriate interconnection point with the existing infrastructure,
- providing the interconnection for the IP domain with the existing network elements and databases needed to support delivery of location information to the PSAP.

Brief descriptions of these new functional elements are provided in Section 2.3, along with definitions of some of the SIP elements from RFC 3261[5] for convenience.

The IP domain “cloud” in the figure represents the collective set of IP domains, including multiple private and public service provider domains, from which emergency calls might originate, and through which emergency calls are interconnected with the existing emergency services infrastructure that is shown on the right-hand side of the diagram.

In this document, all the call control interfaces are described using SIP as the example protocol. This does not preclude providers from using other call control protocols as long as the functionality described in this document is provided by the other protocol. For example, H.323 is a protocol that could be used instead of SIP. If other protocols have to be used then it is important that the same functionality be provided

The logical SIP signaling interfaces between functional elements used for call setup signaling in the IP domain are represented by dashed lines in the figure. The logical interfaces for the exchange of location-related data between and among functional elements in the IP domain are represented by solid lines. The interfaces defined in this standard are labeled (Vx) for convenience in referencing individual interface descriptions. The physical and logical signaling and data exchange interfaces among existing E9-1-1 network and database elements are defined in other documents.

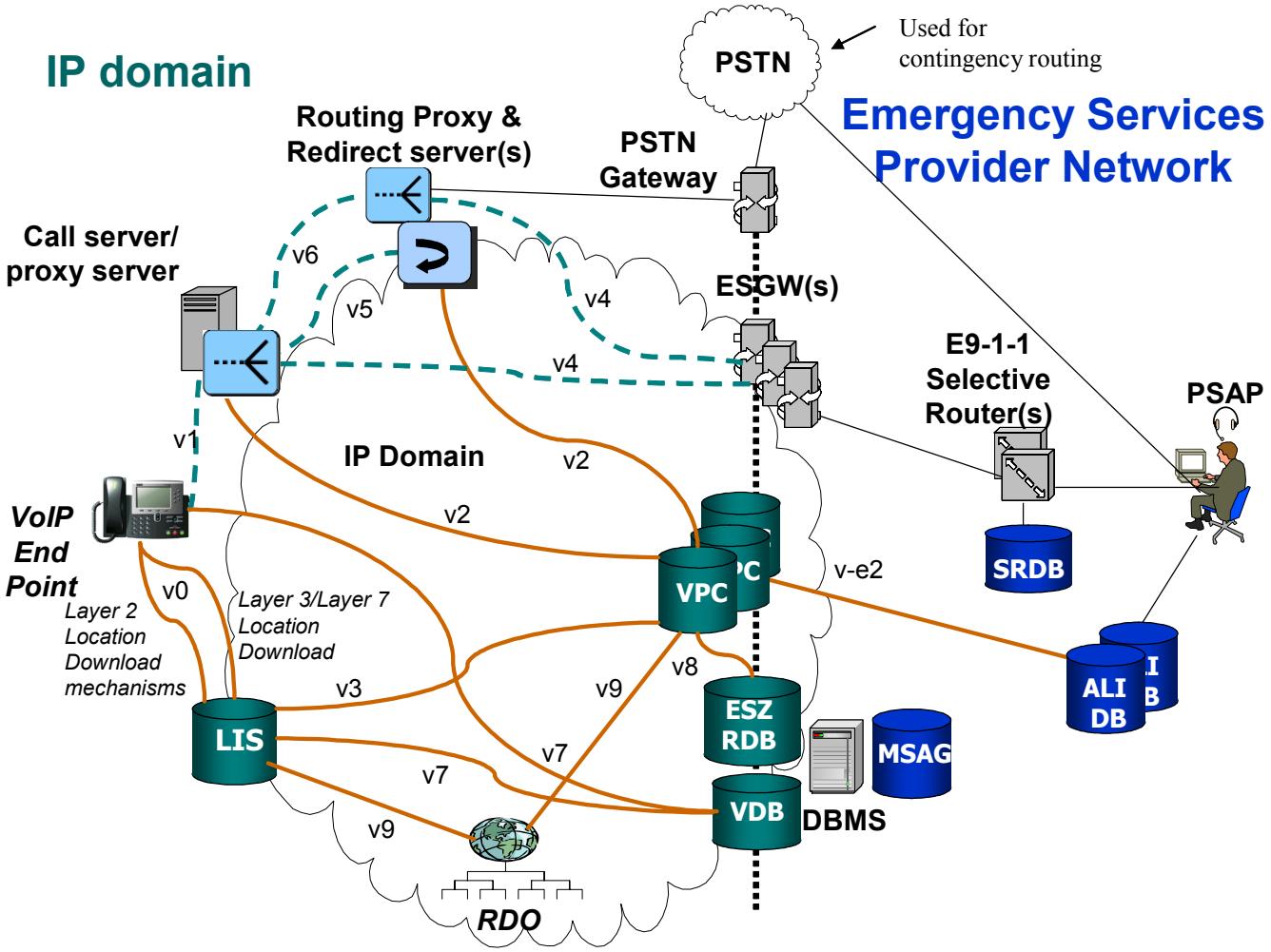


Figure 2-1 VoIP Domain Interconnection with Emergency Services Provider Network

This figure is simplified for illustrative purposes, not showing all the interconnection of multiple entities or mirrored E9-1-1 Selective Routers (SRs), ALI DBs, or new MSAG-based databases used for VoIP emergency call routing or validation of location. The PSTN cloud is part of the diagram because the i2 solution allows for contingency routing using the PSTN. In cases of failures, it may be possible for emergency calls to be routed to the appropriate PSAP using the PSTN. It should be noted that:

- There may be multiple VoIP Positioning Centers (VPCs) in any given serving area. The Call Server/Proxy Server/Redirect Server chooses the VPC for interconnection.
- A given VPC may have interfaces to one or more ALI DBs. One or more VPCs may have interfaces to any given ALI DB.

- The Emergency Service Zone (ESZ) Routing Database (ERDB) may be distributed across multiple data base repositories in North America, but there is one authoritative source for the routing data for any given geographic serving area. When the ERDB is implemented apart from the VPC, it may support routing queries from VESA-certified VPCs in the i2 solution.
- The Validation Database (VDB) may be distributed across multiple data base repositories in North America, but there is one authoritative source for the location validation data for any given geographic serving area.
- There will be at least one Emergency Services Gateway (ESGW) interconnected with any given E9-1-1 SR.
- Any given ESGW may be interconnected with one or more E9-1-1 SRs.
- Each VoIP endpoint/User Agent is served by only one Location Information Server (LIS) at any given time.
- A Call Server is operated by a VSP. A Call Server is typically configured to contact contracted VPC(s) for emergency calls.
- ESGW operators can be regional similar to SR operators today.
- Each VSP operator may contract with one or multiple ESGW operators and a single ESGW can be reached from multiple VSP operators.

The interfaces shown in Figure 2-1 are described in greater detail in subsequent sections of this document.

2.3 Description of Functional Elements

This section provides brief high-level descriptions of the functional elements in the IP domain used to support validation and management of location information, routing of emergency calls, and delivery of location-related information to network elements and data bases in the existing E9-1-1 service provider infrastructure.

2.3.1 User Agent (UA)

As defined for SIP in IETF RFC 3261[5], the User Agent represents an endpoint in the IP domain, a logical entity that can act as both a user agent client (UAC) that sends requests, and as user agent server (UAS) responding to requests.

2.3.2 VoIP Endpoint (VEP)

In this document, the term VoIP endpoint is used to refer to the endpoint IP Device that is used to originate an emergency call.

2.3.3 Server

A server is a network element that receives requests in order to service them and sends back responses to those requests. Examples of servers used in SIP domains are proxies, user agent servers, redirect servers, and registrars.

2.3.4 Call Server

The term Call Server in this document is used to refer to the entity in a private or public IP domain that provides service to endpoints in an emergency caller's home domain and that interworks with the SIP servers and other elements in the IP domain used to support emergency services call routing in the i2 solution. The Call Server may use SIP or some other VoIP signaling protocol within its own serving domain.

2.3.5 Proxy or Proxy Server/Policy and Routing Server

"A policy and routing server in the context of SIP is a proxy server, an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it." (Refer to IETF RFC 3261[5].) It can be a policy/routing element in other protocols

2.3.6 Redirect Server/Call Relay Server

In the context of SIP, a call relay server is a redirect server UA server that generates (3xx) redirect responses to requests it receives, redirecting the client to contact an alternate set of Uniform Resource Identifiers (URIs). (Refer to IETF RFC 3261[5].) This may be an H.323 Gatekeeper for implementations that use ITU H.323 architectures.

2.3.7 Dynamic Host Configuration Protocol (DHCP) Server

The DHCP server is capable of providing configuration information to IP Devices/endpoints. For example, the DHCP server is used to allocate dynamically assigned IP addresses to an IP Device. In the i2 solution, the DHCP server may be used as a Layer 2 mechanism to download location-related information to the IP device from a wiremap stored in a Location Information Server (refer to Section 2.6). (Refer also to IETF RFC 2131[4].) Bearing in mind that the definition of the V0 interface is outside the scope of this document, it is important to state that there are multiple approaches currently under study for this interface. They are primarily broken down into L2 approaches (e.g. DHCP, LLDP) and L3/L7 approaches that are L2 independent. The detailed specification of this interface is out of scope of this document, and DHCP is used only as an example of how such functionality may be accomplished in an i2 compliant solution.

2.3.8 Location Information Server (LIS)

In some implementations, a LIS serves as a repository for location information. Location information is in the form of civic address or geo-spatial location attributes correlated with a particular physical location. The LIS is configured with mappings between individual location information and a logical representation of the physical locations with which they are associated. This set of associations is called a "wiremap."

The wiremap in the LIS is assumed to be configured and maintained by the entity that provides/maintains the physical or logical access facility for endpoint equipment. For examples, this might be an IT administrator for an enterprise, or an Internet Service Provider (ISP) or access provider in non-enterprise/residential VoIP markets. The administrator/owner of the LIS is responsible for creating and maintaining this wiremap, and for ensuring that the civic location data is MSAG-validated.

A given endpoint can be associated with a physical location that is mapped to a particular civic address or geo coordinates, and this information is downloaded from the LIS to the endpoint as described in Section 2.6.1.

The LIS may also support assignment of a location query key, to a particular instance of an address, to support subsequent queries for the address, as described in Section 2.6.2.

2.3.9 Validation Data Base (VDB)

The VDB contains information that describes the current, valid civic address space defined by the Emergency Services Network Provider's MSAG. The structure of the database is beyond the scope of this standard. However, the VDB should have the capability to receive a validation request containing a civic address consisting of data elements included in the civic Location Object being defined in IETF Internet drafts and as described in NENA 02-010[11], and be able to determine if this civic address is a valid address. The VDB will return a response indicating that a given location is a valid address or an error response. This process ensures that the address is a real address (i.e., the address exists) but does not ensure that it is the location of the caller.

The VDB may be distributed across multiple databases, for example, with different VDBs serving different regional areas; however, there will be one primary source of validation data for any given geographic area or address.

2.3.10 Emergency Service Zone (ESZ) Routing Data Base (ERDB)

The ERDB contains routing information associated with each ESZ in a serving area. It supports the boundary definitions for ESZs and the mapping of civic address or geo-spatial coordinate location information to a particular ESZ.

For each ESZ, the ERDB contains one Emergency Services Routing Number (ESRN) associated with the primary Selective Router (SR) that serves the ESZ and one routing Emergency Services Number (ESN) that uniquely identifies the ESZ in the context of that SR. The ERDB may contain a Contingency Routing Number (i.e., a 10-digit 24x7 PSAP number) associated with the ESZ. The ERDB may also contain an Administrative ESN for the ESZ, when applicable. Section 4.5.1 provides more details on Administrative ESNs.

When an emergency call is originated, and location information is received from the VPC, the ERDB will identify the ESZ and routing information associated with the received location information, and will provide the ESRN, the routing ESN, the CRN (if available) and optionally the administrative ESN to the VPC.

The ERDB supports an interface from one or more VESA certified VPCs in the i2 solution. The ERDB may be distributed across multiple data base repositories, but there is one authoritative source for the routing data for any given geographic serving area. Civic location-based routing data in the ERDB is expected to be based on the same MSAG data used to provide location validation in the VDB, and also from existing SR network configuration information. The ERDB may support an interface to the Database Management Systems that manage the MSAG data (to receive updates), but this interface is not specified in this document.

2.3.11 VoIP Positioning Center (VPC)

The VoIP Positioning Center (VPC) is the element that provides routing information to support the routing of VoIP emergency calls, and cooperates in delivering location information to the PSAP over the existing ALI DB infrastructure.

The VPC supports access to the routing data in the ERDB.

The VPC receives queries over the V2 interface, described later in this document that includes call and location-related information.

The information provided in a query over the V2 interface includes Callback information, when available (to be provided to the PSAP so that a call-taker can call back an emergency caller), and a PIDF-LO or Location Key. The VPC may also receive other information about the call, such as Voice Server Provider (VSP) identification information.

If the VPC receives a Location Key, the VPC obtains the location information from the identified LIS.

The VPC uses the received location information with other locally stored information that enables it to determine the appropriate ERDB to query for the routing instructions.

The VPC uses the received location information to request routing information from the ERDB that is associated with the caller's location. .

The VPC may also obtain information from the ERDB to assist in contingency routing.

Using the routing data received from the ERDB, the VPC temporarily allocates an ESQK to a particular call instance and stores information associated with that call with the ESQK pending a subsequent query from an ALI DB.

The VPC passes the ESRN, ESQK, and the Last Routing Option (LRO) to the Call Server/Routing Proxy/Redirect Proxy in the response to a request for routing information associated with the emergency call.

The VPC de-allocates the ESQK when it receives an indication that the call has ended or when the guard timer associated with the ESQK assignment expires, whichever occurs first.

2.3.12 Emergency Services Gateway (ESGW)

The Emergency Services Gateway (ESGW) is the signaling and media interworking point between the IP domain and conventional trunks to the E9-1-1 SR that use either Multi-Frequency [MF] or Signaling System #7 [SS7] signaling. The ESGW uses the routing information provided in the received call setup signaling to select the appropriate trunk (group) and proceeds to signal call setup toward the SR using the ESQK to represent the Calling Party Number/Automatic Number Identification (ANI) information.

2.4 Description of 9-1-1 Data Objects

This section identifies 9-1-1 data objects defined in the i2 solution architecture. These data objects are needed to support routing of emergency calls and delivery of location information to PSAPs. The use of the data objects and the protocols defined to carry them are described in detail in the specification of the various interfaces in the i2 solution architecture.

Emergency Services Routing Number (ESRN) – The ESRN is used by the Call Server/Routing Proxy to route an emergency call to the correct ESGW, and by the ESGW to select the desired path to the appropriate SR for the call. The ESRN is expected to be a ten-digit North American Numbering Plan Number.

Emergency Services Query Key (ESQK) – The ESQK identifies a call instance at a VPC, and is associated with a particular SR/ESN combination. The ESQK is delivered to the E9-1-1 SR and as the calling number/ANI for the call to the PSAP. The ESQK is used by the SR as the key to the Selective Routing data associated with the call. The ESQK is delivered by the SR to the PSAP as the calling number/ANI for the call, and is subsequently used by the PSAP to request ALI information for the call. The ALI database includes the ESQK in location requests sent to the VPC. The ESQK is used by the VPC as a key to look up the location object and other call information associated with an emergency call instance. The ESQK is expected to be a ten-digit North American Numbering Plan Number.

Last Routing Option (LRO) – The LRO is sent by the VPC to the Call Server/Routing Proxy and provides the Call Server/Routing Proxy with a "last chance" destination for the call. The LRO may be the Contingency Routing Number (CRN), which is a 24x7 PSAP emergency number, or it may contain a routing number associated with a national or default call center. The content of the LRO will depend on the condition that resulted in the providing of the LRO. Ultimately the usage of LRO routing data for call delivery is based on logic internal to the Call Server/Routing Proxy.

Contingency Routing Number (CRN) – A 10-digit 24x7 number that could be used, when available, to route emergency calls to the PSAP in scenarios where a network (i.e., trunk or SR) failure results in the ESGW being unable to route the emergency call over the desired path to the SR. The CRN is expected to be a 10-digit North American Numbering Plan Number.

Location Object (LO) – In the context of this document, the LO is used to refer to the current position of a VoIP endpoint that originates an emergency call. The LO is expected to be formatted as a Presence Information Document Format – Location Object (PIDF-LO) as defined by the IETF in draft-ietf-geopriv-pidf-lo-03[8]. The PIDF-LO may be:

Geo location – latitude, longitude, elevation, and the datum which identifies the coordinate system used. For the i2 solution it is expected that geo location information will be formatted using the World Geodetic System 1984 (WGS84[1]) datum.

Civic location – a set of elements that describe detailed street address information.

Location Key (LK) – an object that uniquely identifies an instance of a LO that is stored/managed by a LIS on behalf of a VoIP endpoint. The Location Key must contain:

LIS-ID – an identifier for the LIS in which the LO is stored.

Client ID – an identifier for an instance of a LO (Geo Location, Civic Location or both) that is stored in a LIS.

Location Information Element (LIE) – a protocol container for either or both of:

one LK.

one PIDF document.

Callback Number – an identifier for an emergency caller that can be used by the PSAP to reach an emergency caller subsequent to the release of an emergency call. In the i2 solution, the Callback Number is an E.164 number, but may be represented in VoIP signaling by a uniform resource indentifier (uri), for example.

Postal Address - A Postal Address includes the following data elements in the validateAddress request and response:

- HouseNum
- PrefixDirectional (not included in all addresses – e.g. **N** 7TH)
- StreetName
- StreetSuffix (not included in all addresses – e.g. CONGRESS **AVE**)
- PostDirectional (not included in all addresses e.g. ACADEMY DR **E**)
- PostalCommunity
- CountyName
- StateProvince
- PostalCode
- Country

An address is considered Postal valid if it exists in the U.S. Postal Service (USPS) or Canadian Postal Service data. A valid Postal Address will conform to USPS abbreviations as specified in USPS Standard Publication No. 28 or the Canadian Postal Guide. The VDB may use a database or service based on USPS data to determine whether an address is a valid postal address.

[1] The required coordinate system for the i2 solution is WGS84 using EPSG 4326 format, defined in GML defined with a position->Point->pos. Where an altitude is reported WGS84 using EPSG 4979 is required. Locations MUST be described as one of a point, a circle, or a polygon as defined draft-winterbottom-geopriv-pdif-lo-profile-00.txt.

MSAG Address - An MSAG Address includes the following data elements in the validateAddress request and response:

- HouseNum
- HouseNumSuffix
- PrefixDirectional (not included in all addresses – e.g. **N** 7TH)
- StreetName
- StreetSuffix (not included in all addresses – e.g. CONGRESS **AVE**)
- PostDirectional (not included in all addresses e.g. ACADEMY DR **E**)
- MSAGCommunity
- CountyID (not used by all MSAG addresses)
- StateProvince

An address is considered MSAG valid if it exists in the MSAG database. The MSAG database is created by the Addressing Authority for a region. It contains entries for valid Address Ranges for the Streets (within the Communities, Counties, and State) for which the Addressing Authority is responsible. The Abbreviations, Street Names and Community Names may not be the same as the valid Postal Address for the same address (in fact they will most probably be different – see Appendix C. An MSAG address may also require a County ID to be specified. The County ID may be an abbreviation of County Name or it may be the TAR Code for the County.

2.5 Interface Definitions

This section provides brief definitions of the VoIP and data exchange interfaces included in the i2 Solution.

2.5.1 V0 – LIS to VoIP Endpoint

The V0 interface is used to provide a means for a VoIP endpoint to receive information corresponding to a pre-determined location. The information provided may be in the form of a LK including Client-ID and LIS-ID, or it can be a PIDF-LO containing the actual location, as described in Section 2.5.2. In the i2 timeframe, it is expected that the PIDF-LO may include either or both Geo and Civic information, to enable routing of the emergency call, and a Civic Location, e.g. addresses for non-wireless IP devices (wireless IP endpoints are not specifically addressed), for display to the PSAP.

How the IP network actually determines the location and the protocol between the LIS and IP device is outside the scope of this document.

This interface should be defined by standards organizations such as TIA/IETF. NENA recommendation for this interface are currently under development.

2.5.2 V1 – VoIP Endpoint to Call Server/Proxy

The V1 interface is between the VoIP Endpoint and the Call Server within the VSP's network. It is used to initiate an emergency call which will ultimately be answered by the correct PSAP and is also used to communicate the location information to the Call Server when an emergency call is initiated.

The interfaces must:

a. Transport emergency call notifications
b. Support transport of the location information (containing either or both of an PIDF-LO and LK)
c. Support the other requirements listed in this document

This interface should be defined by standards organizations such as TIA/IETF.

2.5.3 V2 – Call Server/Proxy to VPC

The V2 interface is used to request emergency call routing information when the Call Server/Routing Proxy/Redirect Server is a separate element from the VPC. The Call Server can invoke the V2 interface directly or utilize a Routing Proxy/Redirect Server, which requires forwarding the LIE, or sufficient information to construct the LIE to the Routing Proxy/Redirect Server. It is expected that the VSP/Routing Proxy Operator will have a business relationship in place which would allow the Call Server/Proxy to route the call to the appropriate VPC.

The V2 interface is an eXtensible Markup Language (XML) query/response interface. It provides a means for the Call-Server/Routing Proxy/Redirect Server to request emergency services routing information from the VPC based on the location of the caller. The Call Server/Routing Proxy/Redirect Server sends a request containing location information (LO or LK), callback information and if available a VSP identifier to the VPC. The VPC uses the location information to interact with an ERDB to determine an ESRN for routing and an ESRN/ESN combination associated with a pool of ESQKs from which an ESQK can be allocated for the call. The ESRN and ESQK are returned over the V2 interface in the response to a request for routing information associated with an emergency call. The VPC will return an LRO, if one is available.

2.5.4 V3 – LIS to VPC (Optional)

The V3 interface provides a means for the VPC to obtain the emergency caller's location. This is used when the LIE, provided to the VPC via the V2 interface, contains an LK. The LK is used in obtaining the location from the LIS. The VPC uses the returned location information to obtain routing information from the ERDB.

2.5.5 V4 – Call Server/Routing Proxy to ESGW

The V4 interface is used to forward the call to the appropriate ESGW. The Call Server/Routing Proxy uses the ESRN returned from the VPC to forward calls to the appropriate ESGW and inserts the ESRN and ESQK into the signaling message.

2.5.6 V5 – Call Server to Redirect Server

The V5 interface is defined as a SIP interface to a Redirect Server so it supports a subset of the SIP specification. The Call Server sends a SIP INVITE containing callback information, the PIDF-LO/LK, and the VSP identifier to the Redirect Server. The Redirect Server interfaces to the VPC to obtain routing instructions for the emergency call based on the location of the caller. The VPC

provides the ESRN and ESQK to the Redirect Server. The Redirect Server responds to the Call Server with a 300 response with a Contact header containing the ESRN and a PAI (described in more detail in Section 5.6) containing the ESQK. The Redirect Server will also include a Contact header including the LRO, if a LRO was included in the response from the VPC. The Call Server then selects an ESGW based on the ESRN and forwards the call to it via the V4 interface.

To facilitate release of the ESQK allocated to the call, the Redirect Server will need to inform the VPC when the call has terminated. To enable termination reporting using existing SIP methods, the Redirect Server will need to send a SUBSCRIBE method to the Call Server via the V5 interface to make the Call Server aware that notification should be sent upon termination of the call. When the Call Server detects that the call has terminated, the Call Server will send a NOTIFY method via the V5 interface to the Redirect Server. Upon receiving the NOTIFY method, the Redirect Server will inform the VPC so that it can release the ESQK.

2.5.7 V6 – Call Server to Routing Proxy

The V6 interface is defined as a SIP interface to a Routing Proxy. The Routing Proxy supports the full SIP specification. The Routing Proxy interfaces to the VPC via V2. The VPC provides the ESRN and ESQK, and the LRO, in a response defined by V2. The Routing Proxy then sends an INVITE with the ESRN and ESQK to the ESGW over the V4.

2.5.8 V7 – Location Validation Interface

The V7 interface is used by the LIS provider to request validation of a given Civic Location as compared with the MSAG-based data stored in the VDB. The VSP may also use this interface, when acting on behalf of its customers in the function of location provider/verifier.

A location validation request includes at least the civic location. The response includes an indication of whether or not the Civic Location is a valid address recognized by the MSAG, and may include error/diagnostic information to assist in resolving problems.

The interface should be able to support individual location validation requests sent one at a time for validation processing.

2.5.9 V-E2 – VPC to ALI DB

The V-E2 interface uses the E2+ protocol as defined in NENA Standards 05-001[13], with modifications required for support of i2. The ESQK is sent over the V-E2 interface. The VPC responds with the emergency caller's location, callback number, and VoIP Provider identifier/information it received in the VSP and/or source element.

The ALI DB will need to steer ESQK queries to the VPC provider. The ESQK may need to be identified with a VoIP Class of Service to separate the logic that is in place for Wireless. B

2.5.10 V8 -- VPC to ERDB

The V8 interface supports queries from the VPC to the ERDB. The VPC sends location information for the emergency caller to the ERDB to obtain routing information (ESRN), and other information to help in selection of an appropriate ESQK for the call and to support the delivery of call/location information in response to ALI database requests.

2.5.11 V9 – LIS/VPC to Root Discovery Operator

The V9 interface allows a VEP/LIS or VPC to discover the appropriate VDB/ERDB. Several mechanisms have been defined to allow for the discovery of the VDB/ERDB and these mechanisms are described in Section 2.10.

2.5.12 Web Services

A number of the new Vx interfaces described in this document use Web Services. This section is intended to serve as a high-level tutorial of Web Services.

"A web service is a software application identified by a URI, whose interface and bindings are capable of being identified, described and discovered by XML artifacts and supports direct interactions with other software application using XML based messages via Internet-based protocols."
(World Wide Web Consortium)

A **web service** is a collection of protocols and standards used for exchanging data between applications. Software applications written in various programming languages and running on various platforms can use web services to exchange data over the internet in a manner similar to inter-process communications on a single computer.

2.5.12.1 Standards used

- XML: All data to be exchanged is formatted with XML tags. This encoding can be performed by Simple Object Access Protocol (SOAP) or XML-Remote Procedure Call (RPC) (note: industry standards for security, interoperability, etc. are based on SOAP).
- Common protocols: XML data can be transported between applications using common protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).
- Web Services Description Language (WSDL): The public interface to the web service is described by WSDL. This is an XML-based service description on how to communicate using the web service. It describes the operations the service has available, the messages the service will accept, and the protocol of the service.
- Universal Description, Discovery, and Integration (UDDI): The web service information is published using this protocol. It enables applications to look up web services information in order to determine whether to use them.
- SOAP: The service messaging layer of a web service. The messages are XML based. The protocol consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of

application-defined datatypes, and a convention for representing remote procedure calls and responses.

2.5.12.2 Key Points regarding Web Services

The key points to web services in providing emergency services are:

- Web services are programming language and platform neutral. A web service can be written in Microsoft's .NET on a Window's platform and accessed via a UNIX Java platform or other common development platforms.
- Web services are industry standard. They were developed by the World Wide Web Consortium and the standards are freely available.

For more information on WSDL see the following link:

http://www.w3schools.com/wsdl/default.asp

2.5.12.3 Substitution of Special Characters

The Web Services interfaces are XML-based and certain text characters have special meanings to XML and HTML. As a result, these characters cannot be passed through the interface directly. Instead, the client must substitute standard HTML character codes for these characters. The following table lists the characters and the codes used to replace them.

Character	HTML Code
&	&amp;
' (apostrophe)	&apos;
<	&lt;
>	&gt;
" (double quote)	&quot;

Table 2-1 HTML Code Table

2.6 Location Information Storage Scenarios

There may be a variety of technologies and solutions for determining the location of an individual caller, but after the location has been determined and validated (refer to Section 2.9), location information must be made available for routing an emergency call to the appropriate interconnection point and for delivery to the PSAP. This section provides a high-level overview of two basic scenarios for storing location information for support of emergency calling from the IP domain.

2.6.1 Endpoint Stores Location

The approach being developed in the IETF is based on the premise that the VoIP endpoint[2] (User Agent) is the entity most qualified to store and manage its own location information. This activity takes place on the V0 interface shown in Figure 2-1. There are multiple approaches currently under study for this interface. They are primarily broken down into L2 approaches (e.g. DHCP, LLDP with appropriate references) and L3/L7 approaches that are L2 independent. The detailed specification of this interface is out of scope of this document. This activity takes place on the V0 interface shown in Figure 2-1.

To convey geographical location information within an object that includes a user's privacy and disclosure preferences and which is protected by strong cryptographic security, IETF has defined an XML-based Presence Information Data Format - Location Object (PIDF-LO) that allows for encapsulation of location information within a presence document. The PIDF-LO defines an object suitable for both identifying and encapsulating pre-existing location information formats and for providing adequate security and policy controls to regulate the distribution of that location information. To provide its location to another entity (e.g., for originating an emergency call among many other potential applications), the VoIP endpoint constructs a PIDF-LO that encapsulates it's locations, as well as policy documents that describe how and to what entities that location information can be presented. Note that the emergency services architecture being developed in IETF requires that the UA Client must include location information on emergency calls. The PIDF-LO can be used independently of any 'using protocol' (e.g., SIP); any protocol that can carry XML or MIME document types can carry the PIDF-LO.

In the endpoint-stored location scenario, using SIP signaling, the UA includes this PIDF-LO in the message body of the INVITE message over the *V1* interface shown in Figure 2-1. The PIDF-LO may be carried over the V5 or V6 interface to a redirect or routing proxy, depending on the call routing scenario (refer to Section 2.7), and is carried in a LIE over the *V2* interface to the VPC for routing determination and for subsequent delivery to the PSAP.

2.6.2 LIS Stored – Location Key

An optional approach to supporting location for emergency services calling is allowed in the i2 solution, where completely specified in other standards bodies. This method allows for the LIS to store the location information for a given endpoint and to download to that VoIP endpoint a Location Key, in addition to, or instead of, the location information itself. Then, the VoIP endpoint stores the LK and provides it, instead of or in addition to the location information, over the V1 interface on emergency call originations. The location information/Location Key may be carried in call setup signaling over the V5 or V6 interface to a redirect or routing proxy, depending on the call routing scenario (refer to Section 2.7), and it will be included over the V2 interface to the VPC. When the VPC receives the LK in an LIE, it uses the LIS-ID in the LK to route a query for location to the appropriate LIS over the *V3* interface, including the Client-ID, the electronic signature of the

[2] There are currently work efforts that are discussing the feasibility of having a network element store location instead of the endpoint. This scenario may be added to a future issue of this document.

LIS, and its own authentication information in the query. The LIS authenticates the VPC, and then returns the PIDF-LO to the VPC for routing determination and for subsequent delivery to the PSAP.

2.7 Call Routing Scenarios

The definition of Call Server, Redirect Server, and Routing Proxy permits a variety of business relationships and responsibilities to be established. The variations considered in this document include (but are not limited to):

- VSP contracts for VPC and ESGW services from one or more providers, and retains maximum control over the processing of emergency calls. The VSP's Call Server implements the V2 interface, directly queries the VPC for ESRN/ESQK, selects the proper ESGW given the ESRN and routes calls via the PSTN using the LRO if routing fails.
- VSP contracts separately for VPC and ESGW services but desires a SIP interface to access routing data. The Redirect Server Operator implements a Redirect Server which accepts 9-1-1 calls from the VSP's Call Server. The Redirect Server obtains the ESRN and ESQK from the VPC. It returns the call to the VSP's Call Server with the ESRN and ESQK in the SIP Request URI. The Call Server selects the proper ESGW based on the ESRN. The Call Server handles alternate routing using the LRO.
- VSP contracts for a single 9-1-1 call termination service from a Routing Proxy provider and uses the V6 SIP interface to route emergency calls to the Routing Proxy provider. The Routing Proxy Service Provider receives all 9-1-1 calls at its Routing Proxy. The Routing Proxy provider implements the V2 interface, queries the VPC for ESRN/ESQK, selects the proper ESGW given the ESRN, and routes calls via the PSTN using the LRO if routing fails.

The remainder of this section describes these three different example call routing scenarios which will be able to be supported in the i2 solution. These solutions differ in terms of the element that is responsible for interacting with the VPC to obtain the routing information and the query key for the call, and in subsequently routing the call to the appropriate gateway (i.e., ESGW). In the first scenario, it is assumed that a Call Server is responsible for detecting that an emergency call origination has been requested, and interacting with a VPC to obtain the necessary routing information and query key. The Call Server is then responsible for routing the call to the appropriate ESGW. The second scenario includes a Redirect Proxy, which is responsible for accessing the VPC, but subsequently returns control of the call back to the Call Server for subsequent routing/processing. In the third scenario, a Routing Proxy Server in the call path is responsible for querying the VPC and routing the call forward to the ESGW. Each of these scenarios is illustrated with a diagram showing the relevant interfaces and a high-level description of the associated information flow.

These scenarios also describe a contingency routing capability, to address scenarios in which the ESGW is unable to route an emergency call to the E9-1-1 SR over the desired path because of a failure condition associated with the interconnecting trunk group or SR.

Each scenario also includes providing an indication of call release to the VPC so that it can release the allocated ESQK for use in routing other calls.

2.7.1 Basic Call Routing of VoIP Emergency Calls to ESGW

Figure 2-2 illustrates a basic call routing scenario for a VoIP emergency call origination. In this scenario, a Call Server queries the VPC for routing information, and routes the call directly to the ESGW. Before the emergency call is originated, the civic location is validated in steps A and B (refer to Section 2.9).

Step 1. The endpoint is populated with a PIDF-LO and/or LK. The figure illustrates the method whereby a PIDF-LO/LK is downloaded from the LIS to the endpoint by the DHCP server, using the ***V0*** interface. **Depending on the originating service provider(s) other methods may apply, DHCP is used in these call flows as an example**.

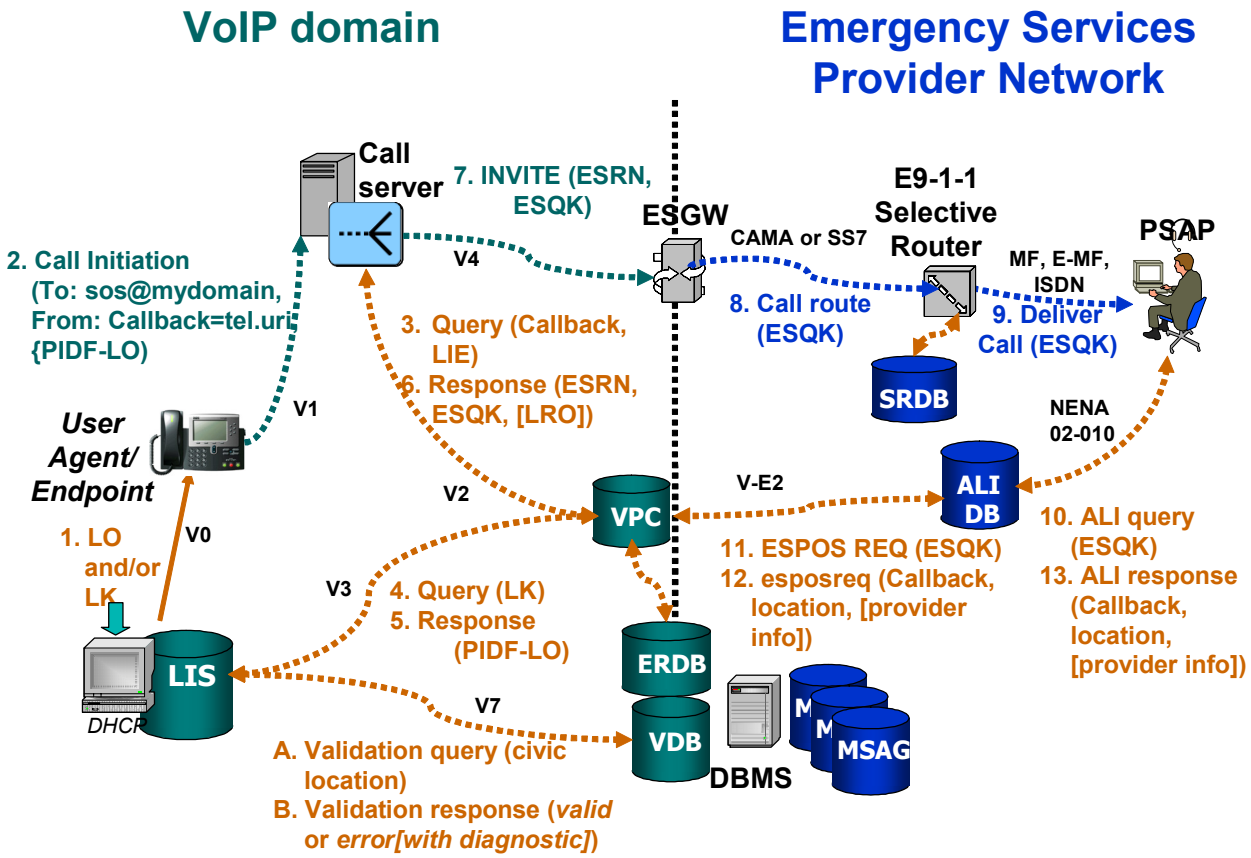


Figure 2-2 Basic Call Routing of VoIP Emergency Calls

Step 2. The VoIP endpoint originates an emergency call by sending a call initiation request, designating sos@local.domain.name as the target destination, and including Callback information, and the PIDF-LO. Using SIP as the example, the User Agent would send an INVITE, including sos@local.domain.name in the Request URI header, a tel-uri in the From header to indicate the Callback to be used, and including the PIDF-LO member-body in the INVITE.

Step 3. The Call Server receives the call initiation request and sends a routing request to the VPC using the information received in the call request. The VPC receives the routing request containing the following:

- An identifier for the emergency caller that can be mapped to an E.164 telephony number (e.g., a tel URI)
- LIE.

Step 4. If a LK is received, based on the LIS-ID in the LK, the VPC may determine the address of the LIS by querying a DNS, or it may determine it based on information stored at the VPC. The VPC queries the identified LIS over the ***V3*** interface, including the received location key.

Step 5. The LIS returns to the VPC the location it has associated with the Client-ID, over the ***V3*** interface.

Step 6. The VPC uses the location (received from the Call Server or queried from the LIS) to obtain the ESZ-related routing information from the ERDB. The ERDB identifies the ESRN, ESN, and CRN that will facilitate routing via the appropriate ESGW to the SR that serves this ESZ. The VPC uses the received routing information to allocate an available ESQK from the pool of ESQKs appropriate for the SR/ESN associated with the caller's location/ESZ and sends a response to the routing request for this call, including the allocated ESQK and ESRN, as well as the appropriate LRO.

The VPC also determines the VSP either from the routing request contents or from the originator of the request. The VPC maps the caller's Callback tel.uri, VSP, and the contents of the location into the appropriate fields necessary to populate the response to an Emergency Services Positioning Request (ESPOSREQ) and stores this information pending a subsequent query.

Step 7. The Call Server will take the ESRN received in the response and use it as the basis for selecting the appropriate ESGW toward which to route the emergency call. The Call Server will also include in outgoing signaling the ESQK (as the calling number for the call). The Call Server routes the call to the ESGW, including the ESRN routing information provided by the VPC and the ESQK.

The LRO will be retained at the Call Server and only used for emergency call routing if the ESGW detects a failure condition that makes routing based on the ESRN impossible.

Step 8. The ESGW uses the received ESRN to select an outgoing route (i.e., trunk group) to the appropriate E9-1-1 SR. If the trunk group is available, the ESGW seizes a trunk and signals an emergency call origination to the E9-1-1 SR, using outgoing (SS7 or MF) signaling that includes the digits "9-1-1" as the called number and the ESQK as the calling number/ANI.

If the ESGW determines that it cannot route the call over the route associated with the ESRN due to a failure condition, it shall inform the Call Server that a failure has occurred.

Step 9. The SR receives the emergency call, uses the ESQK to query the SRDB for the associated Emergency Service Number (ESN), and uses the ESN to identify the appropriate PSAP for the call. The SR then delivers the call to the appropriate PSAP, signaling the ESQK as the Automatic Number Identification (ANI) information.

Step 10. The PSAP ANI/ALI controller receives the call setup signaling, and sends an ALI query to its serving ALI DB, using the ESQK as the query key.

Step 11. The ALI DB sends an ESPOSREQ to the VPC (identified in the shell record for the ESQK in the ALI DB), and includes the ESQK as the query key in the request.

Step 12. The VPC receives the ESPOSREQ from the ALI DB, and uses the ESQK to retrieve the ALI record information it stored previously (in Step 4). The VPC returns an Emergency Services Positioning Request response (esposreq) to the ALI DB to provide the Callback Number, the location information, and the VSP provided information that can be supported by the V-E2 interface.

Step 13. The ALI DB receives the esposreq from the VPC. It may also extract additional information from the shell record for the ESQK. The ALI DB returns an ALI response to the PSAP, following requirements in NENA 02-010.

Step 14. (not shown) When the VPC receives an indication that a particular instance of an emergency call is being cleared, the VPC de-allocates the associated ESQK and makes it available for subsequent emergency calls. Note that release of the ESQK may occur as a result of an indication of call release over the V2 interface from the Call Server/Routing Proxy, or the expiration of the ESQK guard timer, whichever occurs first.

2.7.2 Proxy Redirect Server

Figure 2-3 illustrates an example of an emergency call setup using SIP signaling to perform a proxy redirect server. In this scenario, the Call Server uses a Redirect Server to obtain routing information, and then routes the call to the ESGW. The SIP Redirect Server performs a routing query to the VPC.

Before the emergency call is originated, the location is validated in steps A and B (refer to Section 2.9).

Steps 1 and 2 are the same as in the basic scenario described in Section 2.7.1.

Step 3. The Call Server/SIP Proxy Server sends an INVITE over the ***V5*** interface to a SIP Redirect Proxy.

Step 4. The SIP Redirect Server queries the VPC over the V2 interface (or an internal interface if the VPC is implemented with the Redirect Server), providing:

- An identifier for the emergency caller that can be mapped to an E.164 telephony number (e.g., a tel URI)
- LIE

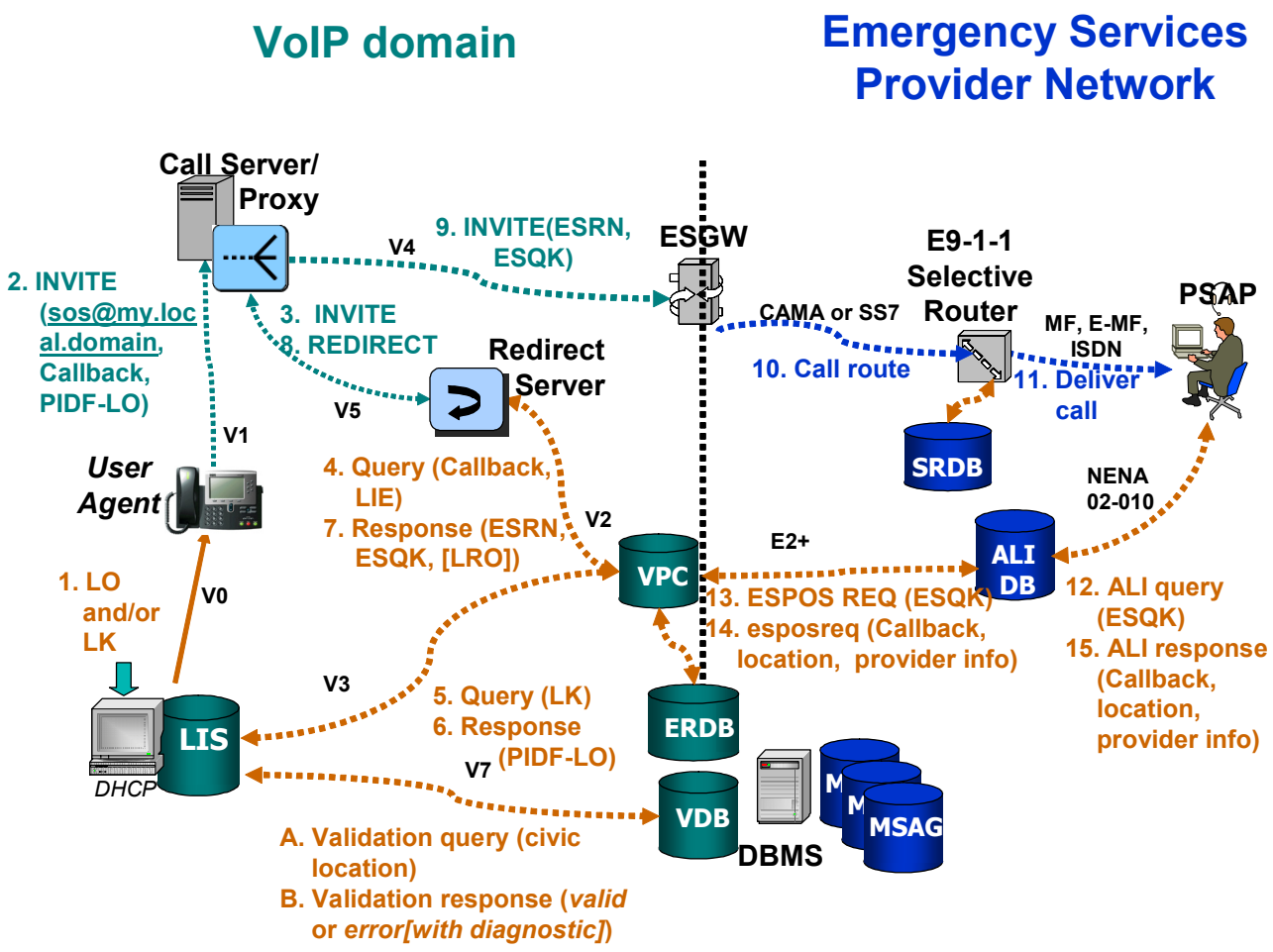


Figure 2-3 SIP Proxy Redirect

Steps 5 through 7 are the same as Steps 4 through 6 in the basic scenario described in Section 2.7.1.

Step 8. The Redirect Server returns a SIP REDIRECT message to the SIP Proxy, including the ESQK and the ESRN provided by the VPC. It may also include a LRO, if provided by the VPC.

Step 9. The Call Server/SIP Proxy routes the call to the ESGW over the ***V4*** interface, including the ESRN provided by the VPC and the ESQK.

Steps10-15 are the same as Steps 8-14 in the basic scenario described in Section 2.7.1

2.7.3 Routing Proxy Routing Scenario

Figure 2-4 illustrates an example of emergency call routing via a routing proxy. In this scenario, the emergency call is routed via a routing proxy which performs the routing query to the VPC, and then routes the call directly on to the ESGW.

Before the emergency call is originated, the LO is validated in steps A and B (refer to Section 2.9

Steps 1 and 2 are the same as in the basic scenario described in Section 2.7.1.

Step 3. The Call Server/SIP proxy sends an INVITE over the ***V5*** interface to a SIP Routing Proxy.

Step 4. The SIP Routing Proxy queries the VPC over the ***V2*** interface, providing:

- An identifier for the emergency caller that can be mapped to an E.164 telephony number (e.g., a tel URI)
- LIE.

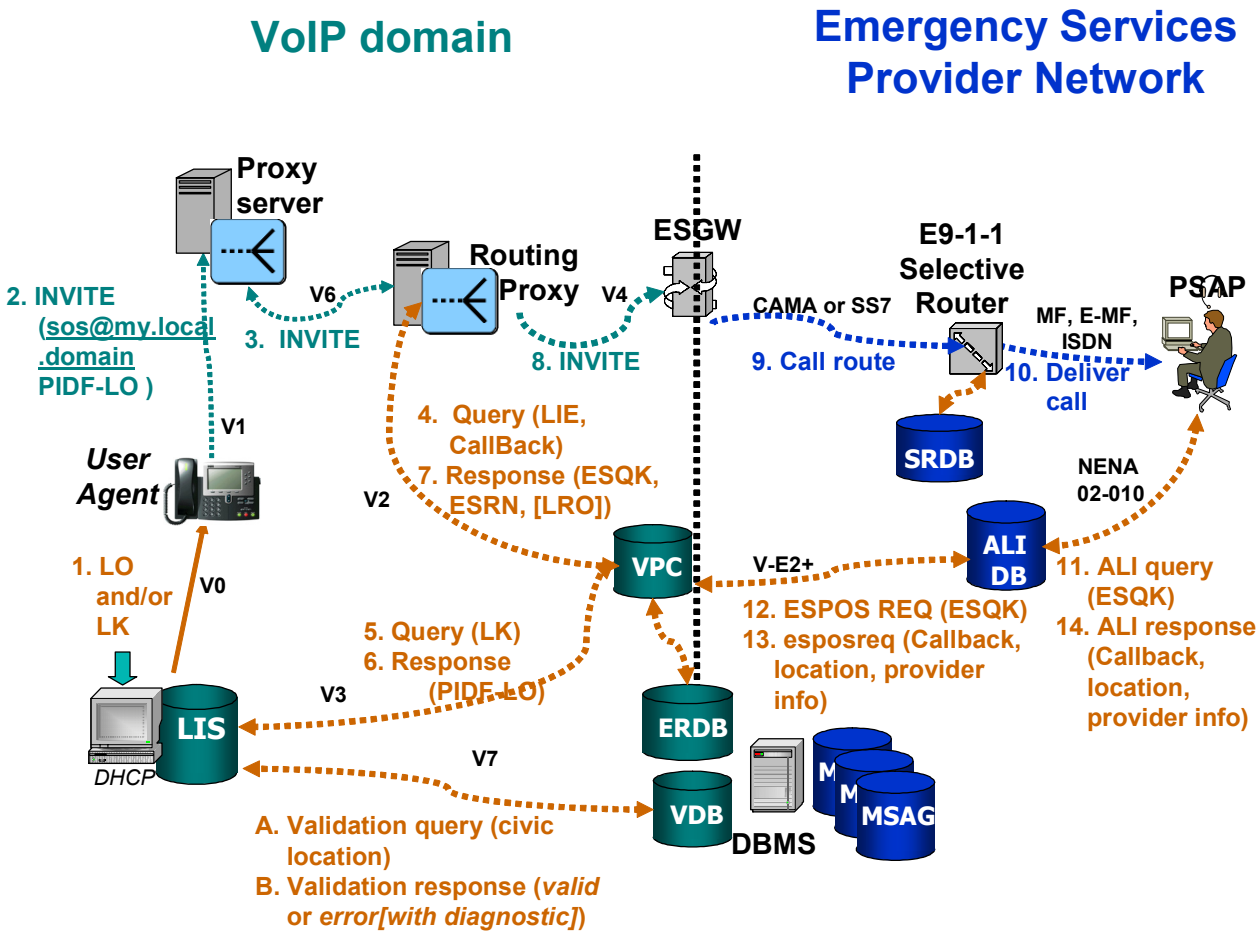


Figure 2-4 SIP Proxy Routing – Proxy Performs Query and Route

Steps 5 and 6 are the same as Steps 4 and 5 in the basic scenario described in Section 2.7.1.

Step 7. The VPC uses the received PIDF-LO to request routing information from the ERDB. The ERDB uses the received location to determine the ESRN, ESN, and CRN for the call. The VPC uses

the ESRN and ESN to determine the ESQK associated with the ESZ of the caller, and allocates an available ESQK for the call. The VPC sends a response to the routing request for this call over the ***V2*** interface to the Routing Proxy, including the allocated ESQK and ESRN. A LRO may also expected to be included in the routing response.

The VPC also determines the VSP either from the routing request contents or from the originator of the request. The VPC maps the caller's Callback tel.uri, VSP, and the contents of the location into the appropriate fields necessary to populate the response to a subsequent ESPOSREQ from the ALI DB and stores this information pending a subsequent query.

Step 8. The SIP Routing Proxy routes the call to the ESGW over the ***V4*** interface, including the ESRN and the ESQK provided by the VPC.

Steps 9-15ff in the Emergency Services Provider Network are the same as Steps 8-14ff in the basic routing scenario described in Section 2.7.1.

2.7.4 ESRN Routing Tables

To route calls to the correct ESGW, the routing entity must translate an ESRN to the URI of the ESGW. For this purpose, the ESGW operator maintains a table which maps ESRN to ESGW. The routing data for this table is provided in a standardized form, and may be retrieved using HTTPS. The table is an XML representation:

```
<route-table xmlns="urn:nena:xml:ns:es:rt"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:nena:xml:ns:es:rt rt.xsd">

      <ESGW>

            <organization-name>Brian's ESGW Service</organization-name>

            <expiration>2006-12-01T09:28:43+10:00</expiration>

      </ESGW>

      <Routes>

            <Route ESRN=2127113345 hostname="LowerManttanNY.example.com"/>

            <Route ESRN=2127113346 hostname="LowerManttanNY.example.com"/>

      ...

            <Route ESRN=4047113345 hostname="RaritanNJ.example.com"/>

      ...

      </Routes>

</route-table>
```

The ESGW operator shall supply the URI of this document to the routing entity.

2.7.5 Call Performance Section

The following diagram provides the estimated setup times to deliver a call to the PSAP. The number directly under each entity, e.g. Call Server, represents the processing time. The number given on each line is the time required to pass the information through the network.

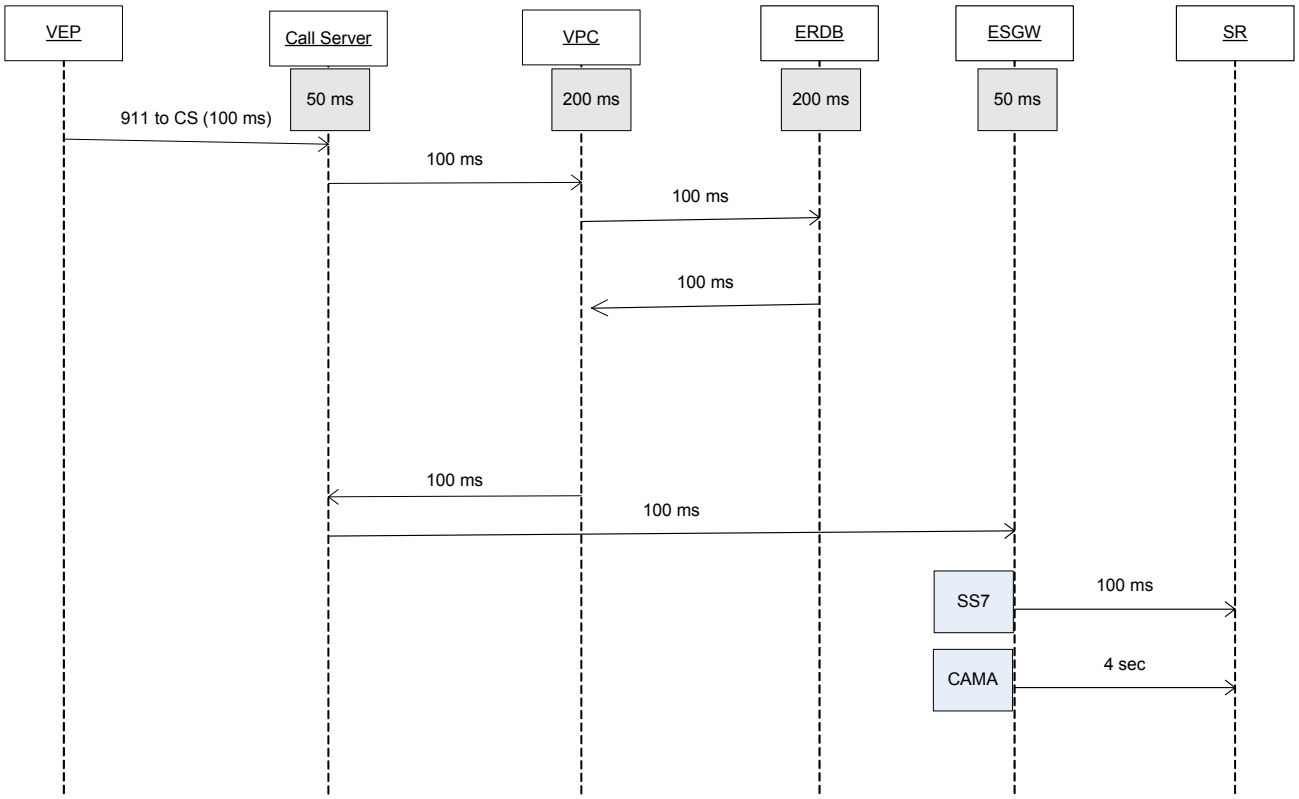


Figure 2-5 - Call Routing Performance

ASSUMPTIONS:

1. Congestion encountered using internet access is not considered in the performance. No assumption is made that the Internet provides separate priority queues for voice calls.
2. Network connections assume WANs.
3. Network time between the VPC and ERDB can be eliminated if VPC has access to the information locally.
4. It is assumed that the VPC is preloaded with the information needed to determine the appropriate ERDB. It is also assumed that the chosen ERDB has the routing information that is being requested.
5. Delivery to the SR is expected to be either SS7 ISUP or traditional CAMA.
6. Aligning with PSTN requirements, the maximum wait time for call setup is 10 seconds. So once the CS receives the call from the IP endpoint the call should be set up within that timeframe or torn down. This over-rides SIP specified timers that allow up to 32 seconds.

7. Authentication/authorization at the ERDB is assumed in the processing time.
8. ESGW assumes no special software for logic specific to handling emergency calls, i.e., an off the shelf gateway box can be used.
9. No authentication/authorization processing time is included in this figure. It is assumed agreements between the Call Server/Routing Proxy exist.
10. IP Network latency can not be quantified so an additional 1 second is added to each configuration.
11. Processing times shown indicate the total processing time required to process each call.

Overall timers applicable to the set up:

- Call Server – 10 seconds, call set up
- CS to VPC – 5 seconds, maximum wait for response from VPC
- VPC to ERDB – 1.5 seconds, maximum wait for each ERDB query
- VPC – 4.5 seconds, maximum overall wait time for any interactive responses between a VPC and ERDB(s).

Average Expected Call Setup Times:

- 2 to 2.5 Seconds with SS7 to the SR
- 6 to 6.5 Seconds with CAMA to the SR

Call Setup times for the various configurations:

1. VEP->CS->VPC-> ERDB-> VPC->CS->ESGW->SS7 SR+IPL = 2200ms
2. VEP->CS->VPC-> ERDB-> VPC->CS->ESGW->CAMA SR+IPL =6050ms
3. VEP->CS-> Max Wait to VPC->(ERDB interaction) ->CS->ESGW->SS7 SR+IPL =6100ms
4. VEP->CS-> Max Wait to VPC->(ERDB interaction) ->CS->ESGW->CAMA SR+ IPL =10000ms
5. Overall Maximum call setup time from time CS receives call – 10 seconds

2.8 Call Routing Failure Scenarios

There are a number of errors or abnormal conditions (e.g., network failures) that may occur in the process of routing emergency calls originated by VoIP users to the appropriate E9-1-1 SR in the Emergency Service Provider's network. This section identifies different error scenarios that may occur in the course of routing an emergency call to the appropriate SR in an i2 environment, and identifies the contingency/default routing mechanisms that should be invoked at the various VoIP elements that are impacted by the abnormal condition or event.

2.8.1 Abnormal Conditions Detected at the Call Server/Proxy

There are several classes of error/failure conditions that may be detected at the Call Server/Proxy. One class of abnormal conditions is related to the request for routing information that the Call Server/Proxy is expected to generate for emergency calls and send to the appropriate VPC, and the processing of the associated response message from the VoIP Positioning Center (VPC). This class of error/failure scenarios includes the following:

- The Call Server/Proxy cannot identify the VPC (or its network address) to which the routing request associated with the emergency call should be directed.
- The Call Server/Proxy has lost connectivity to the VPC.
- The Call Server/Proxy receives an error response containing no routing information from the VPC.
- The Call Server/Proxy does not receive any response from the VPC within a pre-determined period of time.

In all of these scenarios, the Call Server/Proxy does not receive any routing data from the VPC. If the problem is a loss of connectivity to the (primary) VPC, and the Call Server/Proxy is connected to multiple VPCs, the Call Server/Proxy may attempt to send the routing request to a secondary VPC, provided that the appropriate agreements exist between the VSP and the VPC providers. Should one of the other error scenarios described above occur, the Call Server/Proxy is expected to use a default routing number or URI that has been pre-defined by the VSP to route the call to an agent at a 24x7 call center. The callback number will be treated as the calling number/Automatic Number Identification (ANI) for the call.

In another set of scenarios, the Call Server/Proxy receives some routing information from the VPC, but this information does not include an ESRN or ESQK. In this case, the Call Server/Proxy receives a default routing number in an LRO from the VPC, without an ESRN or an ESQK. This could occur if the VPC does not successfully receive routing information from the ERDB in response to a routing query.

If the Call Server/Proxy receives routing information consisting of only an LRO, the Call Server/Proxy will either use the LRO or the default routing number provisioned at the Call Server/Proxy, depending on the precedence pre-defined by the VSP, as the routing number for the emergency call. The callback number will be signaled as the calling number/ANI for the call.

Another class of abnormal conditions results from network failures that make routing the emergency call over the desired primary route impossible. These include the following scenarios:

- The Call Server/Proxy receives an ESRN (along with ESQK and LRO) from the VPC, but there is no available outgoing route to an ESGW associated with the ESRN.
- The Call Server/Proxy receives a failure indication from the ESGW (as described in Section 2.8.3).

Under both of these scenarios, the Call Server/Proxy is expected to use the LRO received in the routing response from the VPC as the routing number for the call, and the callback number as the calling number/ANI for the call.

2.8.2 Abnormal Conditions Detected at the VPC

One class of errors that might be detected at the VPC involves problems with the structure or content of the routing request from the Call Server/Proxy to the VPC, or queries from the VPC to the

Emergency Service Zone (ESZ) Routing Database (ERDB) or Location Information Server (LIS). This class includes the following scenarios:

- The VPC receives a badly structured routing request from the Call Server/Proxy (i.e., request message cannot be parsed or is malformed.)
- The routing request from the Call Server/Proxy contains neither a Location Key nor a PIDF-LO.
- The VPC receives a PIDF-LO in the routing request from the Call Server/Proxy, but it cannot determine, based on the received location, which ERDB to query for the routing data.
- The VPC receives a PIDF-LO in the routing request from the Call Server/Proxy, but when it uses it to query the ERDB for routing data, it receives either an error response or no response from the ERDB.
- The VPC receives a Location Key in the routing request from the Call Server/Proxy, but it cannot determine where to send the location query (i.e., it cannot determine the appropriate LIS).
- The VPC receives a Location Key in the routing request from the Call Server/Proxy, but has lost connectivity to the desired LIS.
- The VPC receives a Location Key in the routing request from the Call Server/Proxy, and is unable to successfully retrieve a PIDF-LO from the LIS (i.e., it receives an error response or no response from the LIS).

In all of these scenarios, the VPC is unable to successfully obtain routing data from the ERDB and provide it in a response to the Call Server/Proxy. If the VPC is unable to obtain the necessary routing data from the ERDB, the VPC will be expected to send a response message to the Call Server/Proxy that either indicates the nature of the error that occurred, or that provides a default routing number as determined based on prior agreements between the VPC provider, the VSP, and the call center to which calls are to be default-routed.

Another type of abnormal condition that might be encountered at the VPC is related to a lack of resources at the VPC. Specifically, the VPC successfully receives routing data from the ERDB, but there are no ESQKs available from the applicable pool to associate with the specific call instance. In this case, the VPC is expected to return a default ESQK value in the response message to the Call Server/Proxy along with an ESRN and an LRO containing a CRN, if available, or a default routing number.

2.8.3 Abnormal Conditions Detected at the ESGW

It is possible that an emergency call gets successfully routed to an ESGW, with the expected information communicated in call setup signaling (i.e., the ESRN and ESQK), and that the ESGW can identify the appropriate outgoing trunk group to the SR associated with the received ESRN, but a trunk failure or SR failure makes it impossible for the ESGW to deliver the call to the desired SR over the primary route. In such a scenario, it is expected that the ESGW will attempt to select a

secondary route for the emergency call, assuming one has been provisioned. However, if there is no way for the ESGW to route the call forward, it is expected that the ESGW will inform the Call Server/Proxy of the failure condition using the appropriate SIP signaling mechanism. The Call Server/Proxy will then follow the procedures described in Section 2.8.1.

2.8.4 Default Routing at the Selective Router

If the SR receives an emergency call from an ESGW, but the incoming call setup signaling associated with that call does not include sufficient information to allow the SR to successfully invoke the selective routing process, the SR will route the call to a pre-defined default PSAP based on the incoming trunk group over which the call was delivered by the ESGW.

2.8.5 Summary of Contingency/Default Routing

The following table summarizes the contingency/default routing scenarios described above, and the associated routing procedures.

Table 2-2 Contingency/Default Routing Summary

Element	*Scenario*	*Procedure*
Call Server/Proxy	• The Call Server/Proxy has lost connectivity to the VPC (and is not connected in primary/secondary arrangement to multiple VPCs). • The Call Server/Proxy receives an error response (with no routing information) from any of the VPCs. • The Call Server/Proxy does not receive any response from the VPC within a pre-defined period of time. • The Call Server/Proxy cannot determine which VPC to which to send the routing request.	Call Server/Proxy uses pre-defined default routing number or URI to route call to 24x7 call center with which VSP has an arrangement. Call Server/Proxy signals callback number as calling number/ANI for the call.
	• The Call Server/Proxy has lost connectivity to the VPC, and the Call Server/Proxy is connected to multiple VPCs in primary/secondary arrangement.	Call Server/Proxy may attempt to send the routing query to a secondary VPC, if supported by agreements between the VSP and VPC providers.
	• Call Server/Proxy receives ESRN (along with ESQK and LRO) from VPC, but there is no available outgoing route associated with ESRN. • Call Server/Proxy receives failure indication from ESGW.	Call Server/Proxy uses LRO as routing number for the call, and callback number as calling number/ANI for the call.
	• Call Server/Proxy receives a default routing number from VPC.	Call Server/Proxy uses default number provided by VPC or pre-defined -default routing number/URI provisioned at Call Server/Proxy as routing number for the call, depending on precedence defined by VSP. Callback number is calling

		number/ANI for the call.
VPC	• VPC receives a badly structured routing request from the Call Server/Proxy. • Routing request contains neither a Location Key nor a PIDF-LO. • VPC cannot determine which ERDB to query based on received location. • VPC receives either an error response or no response from the ERDB. • VPC receives Location Key in routing request from Call Server/Proxy but cannot determine which LIS to query for location. • VPC receives Location Key in routing request, but has lost connectivity to the desired LIS. • VPC receives an error response or no response from LIS when querying for location.	VPC sends a response message to the Call Server/Proxy that either indicates the nature of the error condition, or that provides a default routing number, depending on the arrangements made between the VPC provider and the VSP.
	• Lack of resources at VPC (i.e., no ESQKs available for assignment to specific emergency call.	VPC returns a default ESQK along with an ESRN and LRO to the Call Server/Proxy in response to its routing request.
ESGW	• Trunk failure or SR failure makes routing call over primary route associated with ESRN impossible.	ESGW selects a secondary route for the call, if one has been provisioned.
	• No outgoing routes associated with the received ESRN are available.	ESGW returns a failure indication to the Call Server/Proxy.
Selective Router	• Incoming signaling associated with emergency call does not contain sufficient information to allow SR to successfully invoke selective routing process.	SR routes call to pre-defined default PSAP associated with incoming trunk group from ESGW.

2.9 Location Validation

It is important that civic location information be pre-validated by comparison with validation data based on the MSAG data maintained by the Emergency Services Provider and/or their designated E9-1-1 Database provider(s).

In the i2 Solution, location validation is performed by the LIS provider or by the VSP provider on behalf of the VoIP caller. The VDB provides a mechanism to perform validation on civic location information.

Location validation takes place before a call is originated. The purpose of location validation is to ensure that the location information can be used to properly route an emergency call to the desired PSAP, and also that the location information provided to the PSAP can be used for dispatch of responders.

The location validation architecture in the i2 Solution supports a mechanism for the entity seeking validation of location information (e.g., the LIS) to discover the appropriate VDB for any given serving area. This mechanism is described in Section 2.10.1.

After the appropriate VDB has been identified, the location validation request is sent using the interface described in Section 5.9. The location validation request may include as input a postal or jurisdictional address[3]. The end result of location validation shall result in location information that includes sufficient information to support mapping to a specific record in the MSAG.

2.10 Root Discovery Mechanism

The root discovery mechanism is defined to allow

- Location validation clients (e.g., LISs or VSP customers) to identify the appropriate serving VDB(s) for any given geographic location
- VPCs to identify the appropriate serving ERDB(s) for any given geographic location.

2.10.1 Assumptions

The following assumptions relate to the two applications for the root discovery mechanism.

2.10.1.1 VDB Discovery Assumptions

The prescribed approach to VDB discovery is defined with the following criteria in mind.

- There is no assumption that only one provider of validation services exists for a given location. There may be competition for validation services in the future and the architecture shall not preclude the ability for more than one VDB provider to validate a given location. However, if there are competing providers, they must all have validation data that is based on one authoritative source (the MSAG) designated by the local 9-1-1 jurisdictional authorities.

[3] Jurisdictional Address: An MSAG valid address for the physical location of a subscriber access line, which has been assigned by the jurisdiction's local addressing authority; i.e., planning department, zoning department, etc. and is used for 9-1-1 emergency dispatching purposes.

- A local 9-1-1 authority may certify VDB provider(s) to assure quality of the data.
- There is no assumption that access to the validation service shall be charged for or provided free of charge or have open access or require authenticated access.
- It is not assumed that discovery will be able to occur fully automatically or whether it will need manual transcribing of location information and/or network addresses.
- It is not assumed that the service will or will not be available to members of the general public; this being a matter of individual provider policy and/or any legislative or other constraints which may emerge in the future.
- There is an assumption that a single well-known URL will be available to operate as the root of discovery for VDB services. There is an assumption that the overall guidelines of operation and technical information associated with the use of VoIP services to access E9-1-1 will be publicly available on an Internet accessible web site.

2.10.1.2 ERDB Discovery Assumptions

The prescribed approach to ERDB discovery is defined with the following criteria in mind.

- There is no assumption that only one provider of ERDB services may identify itself as the routing service provider for a given geographic coverage area. This is because the MSAGs on which the routing data is based may have irregular boundaries that do not conform exactly to jurisdictional boundaries. Therefore, more than one provider may be identified for a given geographic location
- A local 9-1-1 authority may certify ERDB provider(s) to assure the quality of the data.
- There is no assumption about whether access to the ERDB shall be charged for or provided free of charge.
- It is assumed that the ERDB will require authenticated access. It is assumed that discovery of the ERDB's coverage areas will also require authenticated access.
- It is not assumed that discovery will be able to occur fully automatically or whether it will need manual transcribing of location information and/or network addresses.
- It is assumed that the ERDB will generally not be available to members of the general public; although this may be a matter of individual provider or PSAP policy and/or any legislative or other constraints which may emerge in the future.
- There is an assumption that a single well-known URL will be available to operate as the root of discovery for ERDB services. This may or may not be the same URL as used for VDB location validation services. There is an assumption that the overall guidelines of operation and technical information associated with the use of VoIP services to access E9-1-1 will be publicly available on an Internet accessible web site.

2.10.2 Root Discovery

2.10.2.1 Service provider data consolidation

Providers of ERDB/VDB services shall be responsible for communicating the identity, URL, and coverage of their service area(s) to the host of the root discovery service. It is expected that the root discovery service operator will publish a mechanism by which such information may be communicated to it. The host of the root discovery shall also publish a mechanism by which a 9-1-1

authority shall inform it of the certification status of the VDB operator in its area. No mechanism is defined to facilitate the root service operator being able to seek out and determine the identity of ERDB/VDB service providers who do not make themselves known to them.

2.10.2.2 Basic Discovery

In its most basic form the root discovery URL shall consist of a human readable list of ERDB/VDB service providers as a table keyed against jurisdictional descriptions of the area of coverage of their validation service. The table should be presented in alphabetical order by state/province and, if further breakdown is required, by county (if applicable) in alphabetical order and if necessary, by municipality in alphabetical order. For each row in the table, a list of ERDB/VDB service provider URLs shall be provided. A facility to download this table in CSV (Comma Separated Values) format shall also be supported.[4]

The root discovery service provider shall provide a database query mechanism to discover the ERDB or VDB. VPC operators would use this mechanism to obtain information about ERDBs; location validation clients (e.g., LIS operators or VSP customers) would use the same mechanism to obtain information about VDBs. In this case, the user shall be able to key in a civic address, or fragment of a civic address (e.g., using a form), and have those providers offering the appropriate services for this location returned as a list. A provided fragment may be ambiguous. That is, the discovery database may be able to find multiple separate regions and associated ERDB or VDB entities that match that fragment; the implication being that greater precision is required in the fragment to identify the actual ERDB or VDB required. Where the fragment of the civic address is ambiguous, the result shall highlight this with the address fields leading to ambiguity highlighted.

[4] Other ways of getting at the data might be supported. For example, navigation by clicking through graphical images of country and regional maps may also be supported at the discretion of the root service provider. The extent to which such enhancements are useful will depend on considerations such as the number and geographical interleaving of the area of coverage of ERDB/VDB service providers.

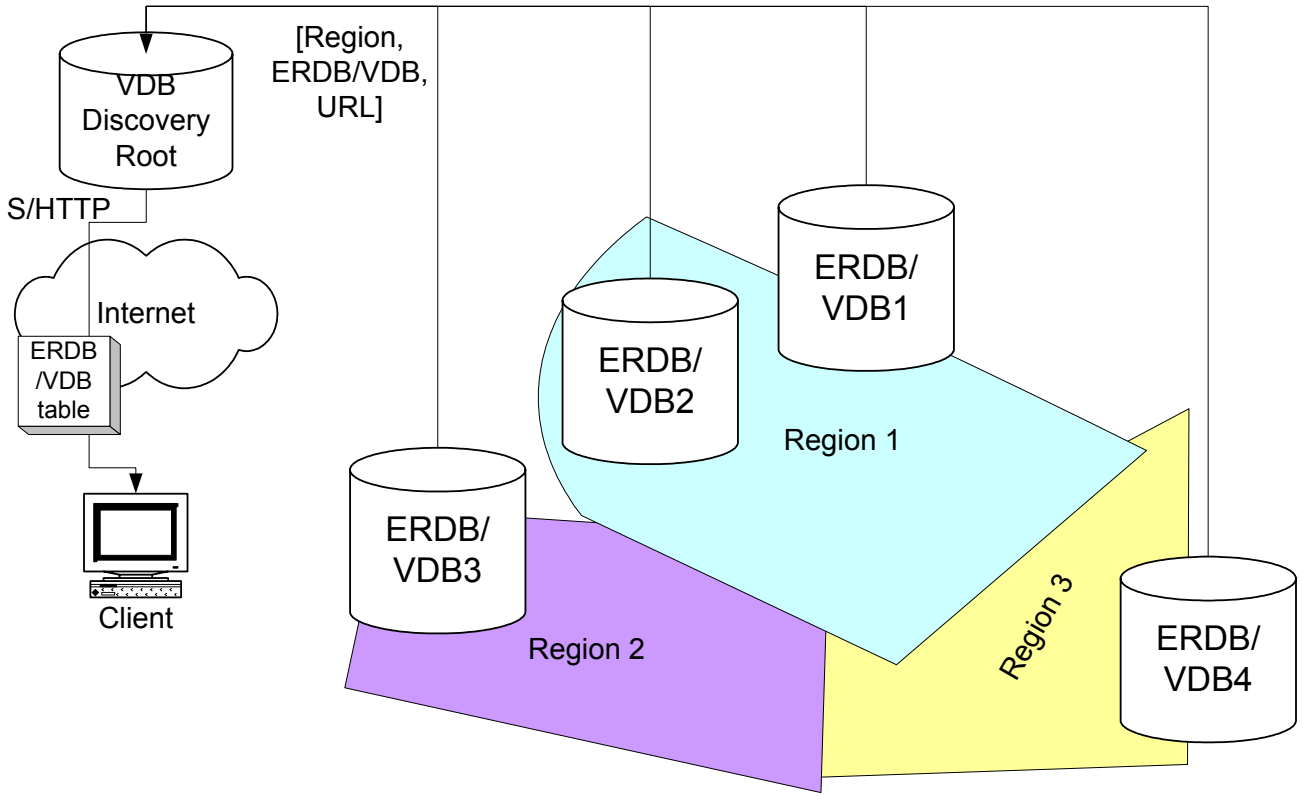


Figure 2-6 Basic ERDB/VDB discovery

2.10.2.3 Automated discovery

The root discovery service provider shall also support an automated discovery mechanism such that the available ERDB orVDB service providers for a given location can be determined via an XML-based web query. This interface is implemented using web services. This interface can support both a machine to machine and a human to machine interface. For identifying the VDB, the semantics of this query shall be:

```
<vdb-identity-request
  xmlns="urn:nena:xml:ns:es:vdbdiscover"
  xmlns:xsi=http://www.w3c.org/2001/XMLSchema-instance
  xsi:schemaLocation="urn:nena:xml:ns:es:vdbdiscover vdbdiscover.xsd">

    <vlocation>
      <…geopriv cl:civicAddress coded location…>
    </vlocation>

</vdb-identity-request>
```

and the response shall be similarly formatted to provide a status of

- Found
- NotFound, or
- Ambiguous

Similarly, for identifying the ERDB, the semantics of the query shall be:

```
<erdb-identity-request
  xmlns="urn:nena:xml:ns:es:erdbdiscover"
  xmlns:xsi=http://www.w3c.org/2001/XMLSchema-instance
  xsi:schemaLocation="urn:nena:xml:ns:es:erdbdiscover erdbdiscover.xsd">

    <vlocation>
      <…geopriv cl:civicAddress coded location…>
    </vlocation>

</erdb-identity-request>
```

and the response shall be similarly formatted to provide a status of

- Found
- NotFound, or
- Ambiguous

For a status of Found, depending on the type of query, the response shall include a list of URLs for ERDB providers that offer routing determination for that location or a list of VDB providers who offer validation services for that location. For NotFound, there are no other response parameters provided. For Ambiguous, those cl:CivicAddress fields which need to be resolved before a definitive list of providers can be returned shall be provided.

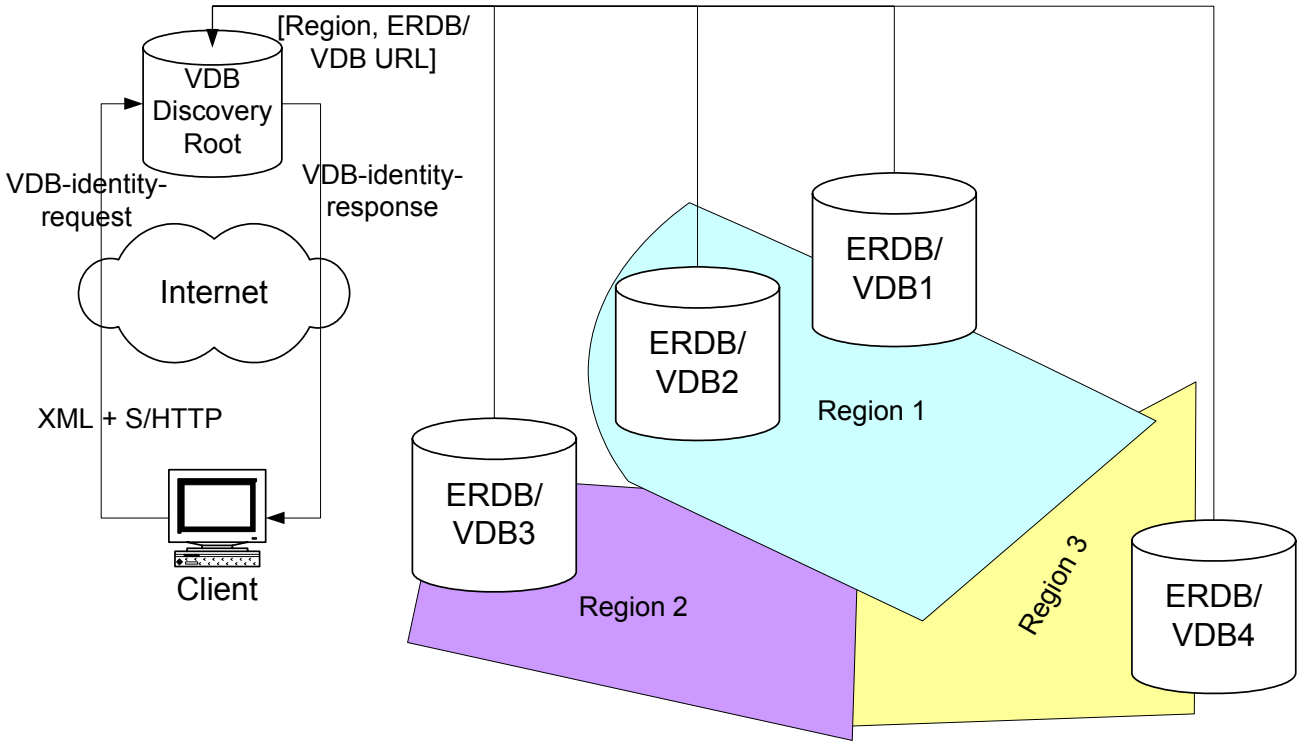


Figure 2-7 Automated ERDB/VDB Discovery

2.10.2.4 ERDB/VDB steering – deferred discovery

This functionality is actually part of the ERDB/VDB query semantics but is pertinent to the discovery function.

It is possible that a request for routing determination/validation is sent to an ERDB/VDB which does not provide coverage for the location being presented. However, based on an analysis of the submitted civic address fields, it may determine through ancillary data that this location can be routed/validated by an alternative ERDB/VDB. This situation may occur where the root discovery data does not cover the degree of granularity or geographical interleaving that two ERDB/VDB operators actually share. For example two ERDB/VDB operators may cover discrete sections of the same municipality and even streets within the same municipality.

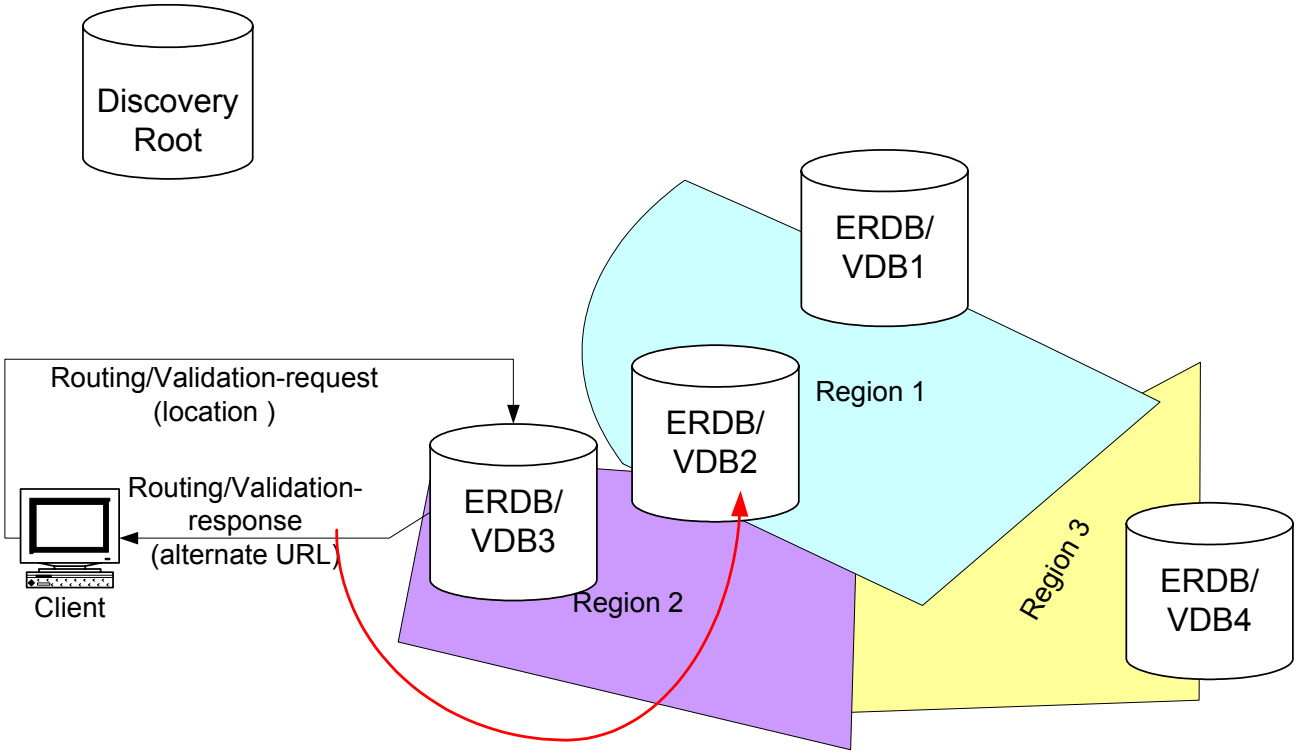


Figure 2-8 Deferred ERDB/VDB Discovery

When multiple responses are provided and the query originator makes the wrong choice, the ERDB/VDB query semantics provide for a response that indicates an inability to validate the proffered location but with an additional parameter to indicate an alternative ERDB/VDB provider URL. Alternatively, co-operating adjacent ERDB/VDB operators may choose to automatically steer validation requests between each other, which would be transparent to the requesting client. This function may also be used by commercial location validation brokers who may add value to the validation process while back-ending queries to the actual VDB providers.

2.10.2.5 Load Balancing

Where a client is provided with multiple VDB/ERDB addresses the client may choose to round robin the results to ensure even distribution.

2.10.3 VDB Directory File Format

The VDB directory file shall consist of a header identifying the following:

- Special file identifier tag string including format version
- Applicable country
- URL of source of file
- Date and time of creation of the file

- Expiry date and time of the file (by which the source URL must have a new version of the file with potential changes)

Each of the above pieces of information will be on a new line in the file and be provided in order. Formats for each of the items will be as follows.

The special identifier string and version line shall be the first line of the file and shall have the form:

%!VDB-Directory-file V<version>

Where <version> is a decimal integer of one or more digits and is greater than or equal to one (1).

The applicable country is a string representing the country of coverage. The strings **USA** or **Canada** shall be used for these countries.

The URL of the source file will be a standard dot delimited URL of the entity which generated the data file. Nominally this is the VDB root discovery URL.

The date and time of creation of the file shall be in the form:

Created <time>

Where <time> indicates when the file content was generated by the source and is of the form

YYYY:MM:DD HH:MM:SS

Where YYYY is the four digits representing the year, MM is the zero leading two digits representing the month, and DD is the zero leading two digits representing the day number of the month. HH is the zero leading hour of day, from 00 to 23. MM is the zero leading integer minutes of the hour and SS is the zero leading integer seconds of the minute, both from 00 to 59. The date and time of file creation date shall be provided in the universal time system (UTS) and not be specific to a particular time zone.

The date and time of effect for the file shall be in the form

TakesEffect <time>

The effect date and time of the file shall be expressed using the same specification, in UTS, as the creation date and time. This will be a date and time at which the contents of the file may be regarded as valid. It shall be no earlier than the creation time and will supersede the contents of any previous file at that time even if the expiry time of the previous file is after the effect time.

The date and time of expiry for the file shall be in the form

Expires <time>

The expiry date and time of the file shall be expressed using the same specification, in UTS, as the creation date and time. This will be a date and time no earlier than the effect time. The contents of the file must be considered invalid at this time and a file with a later effect time than the effect time of this file must have been retrieved and its contents available to replace the current contents at least by the time of expiry.

The rest of the file shall consist of the data representing VDB URLs which service indicated locations. It will be provided as an alphabetically ordered comma separated set of values which each data record commencing on a new line. Each line will have the following format:

<State>, <County>, <Municipality>, <VDB URL list>

The <State> value will have any one of the standard country specific (e.g.,USPS) 2 character state/province abbreviations (e.g. CA, WA, TX,…).

The <County> value will correspond to the country specific (e.g.,USPS) spelling of the county name (e.g. Collin as in Collin County, Texas).

The <Municipality> value will correspond to the country specific (e.g., USPS) spelling of the municipality name of interest (e.g. Plano, as in Plano, Collin County, Texas).

The VDB URL list shall be a semicolon separated list of URLs identifying the address of VDB services that provide validation for the location indicated by the State-County-Municipality values preceding this value. A URL list may be blank.

Records shall be provided in alphabetical order by row with each state/county grouping according to the following convention.

State, *, *, <urls for all counties of this state not listed>
State, County, *, <urls for all municipalities of this county not listed>
State, County, Municipality, <urls for the specific municipality>

Note – Where no record is provided for a particular state, this shall be equivalent to the situation where a **State,** record with an empty URL list. That is, it shall be interpreted that there are no VDB facilities for that state.

Information in the file is order dependent by line. Lines may be blank and blank lines may be ignored. End of line may be DOS or UNIX format and indicated by either a <CR><LF> or just a <CR>. All other whitespace characters may be ignored except where it forms part of a state, county, or municipality name they may be interpreted as a single space character where they occur in these names. State, county, and municipality names shall not include a comma or asterisk and should be limited to alphabetical, space, and hyphen characters.

2.10.3.1 Example directory file

```
%!VDB-Directory-file V1
USA
vdbroot.nena.org

Created         2005:06:22 14:35:26
TakesEffect     2005:06:26 00:01:00
Expires         2005:07:27 00:00:00

AL, *, *, vdbse.sbc.com
AL, Autauga, *, vdbse.sbc.com
AL, Autauga, Montgomery, vdb.rnopco.com;vdbse.sbc.com
AL, Autauga, Pratville, vdb.rnopco.com
AK, *, *, vdbak.bpac.com
AS,*,*, americansamoa-territorialauthority-vdb.asta.gov
:
: denotes actual contents not shown for brevity
:
FM,*,*,    (comment – example of blank list; e.g. no VDB for Federated States of Micronesia at this stage)
:
: denotes actual contents not shown for brevity
:
TX, *, *, vdbsw.sbc.com
:
: denotes actual contents not shown for brevity
:
WY, *, *, vdbwy.bigsky911.com;vdbnc.bpac.com
<eof>
```

2.10.4 ERDB directory file format

The ERDB directory file shall consist of a header identifying the following:

- Special file identifier tag string including format version
- Applicable country
- URL of source of file
- Date and time of creation of the file
- Expiry date and time of the file (by which the source URL must have a new version of the file with potential changes)

Each of the above pieces of information will be on a new line in the file and be provided in order. Formats for each of the items will be as follows.

The special identifier string and version line shall be the first line of the file and shall have the form:

%!ERDB-Directory-file V<version>

Where <version> is a decimal integer of one or more digits and is greater than or equal to one (1).

The applicable country is a string representing the country of coverage. The strings **USA** or **Canada** shall be used for these countries.

The URL of the source file will be a standard dot delimited URL of the entity which generated the data file. Nominally this is the ERDB root discovery URL.

The date and time of creation of the file shall be in the form:

Created <time>

Where <time> indicates when the file content was generated by the source and is of the form

YYYY:MM:DD HH:MM:SS

Where YYYY is the four digits representing the year, MM is the zero leading two digits representing the month, and DD is the zero leading two digits representing the day number of the month. HH is the zero leading hour of day, from 00 to 23. MM is the zero leading integer minutes of the hour and SS is the zero leading integer seconds of the minute, both from 00 to 59. The date and time of file creation date shall be provided in the universal time system (UTS) and not be specific to a particular time zone.

The date and time of effect for the file shall be in the form

TakesEffect <time>

The effect date and time of the file shall be expressed using the same specification, in UTS, as the creation date and time. This will be a date and time at which the contents of the file may be regarded as valid. It shall be no earlier than the creation time and will supersede the contents of any previous file at that time even if the expiry time of the previous file is after the effect time.

The date and time of expiry for the file shall be in the form

Expires <time>

The expiry date and time of the file shall be expressed using the same specification, in UTS, as the creation date and time. This will be a date and time no earlier than the effect time. The contents of the file must be considered invalid at this time and a file with a later effect time than the effect time

of this file must have been retrieved and its contents available to replace the current contents at least by the time of expiry.

The rest of the file shall consist of the data representing ERDB URLs which service indicated locations. It will be provided as an alphabetically ordered comma separated set of values which each data record commencing on a new line. Each line will have the following format:

<State>, <County>, <Municipality>, <ERDB URL list>

The <State> value will have any one of the standard country specific (e.g.,USPS) 2 character state/province abbreviations (e.g. CA, WA, TX,…).

The <County> value will correspond to the country specific (e.g.,USPS) spelling of the county name (e.g. Collin as in Collin County, Texas).

The <Municipality> value will correspond to the country specific (e.g., USPS) spelling of the municipality name of interest (e.g. Plano, as in Plano, Collin County, Texas).

The ERDB URL list shall be a semicolon separated list of URLs identifying the address of ERDB services that provide routing and translation for the location indicated by the State-County-Municipality values preceding this value. A URL list may be blank.

Records shall be provided in alphabetical order by row with each state/county grouping according to the following convention.

State, *, *, <urls for all counties of this state not listed>
State, County, *, <urls for all municipalities of this county not listed>
State, County, Municipality, <urls for the specific municipality>

Note – Where no record is provided for a particular state, this shall be equivalent to the situation where a **State,** record is provided with an empty URL list. That is, it shall be interpreted that there are no ERDB facilities for that state.

Information in the file is order dependent by line. Lines may be blank and blank lines may be ignored. End of line may be DOS or UNIX format and indicated by either a <CR><LF> or just a <CR>. All other whitespace characters may be ignored except where it forms part of a state, county, or municipality name they may be interpreted as a single space character where they occur in these names. State, county, and municipality names shall not include a comma or asterisk and should be limited to alphabetical, space, and hyphen characters.

2.10.4.1 Example directory file

```
%!ERDB-Directory-file V1
USA
```

```
erdbroot.nena.org

Created         2005:06:22 14:35:26
TakesEffect     2005:06:26 00:01:00
Expires         2005:07:27 00:00:00

AL, *, *, erdbse.sbc.com
AL, Autauga, *, erdbse.sbc.com
AL, Autauga, Montgomery, erdb.rnopco.com;erdbse.sbc.com
AL, Autauga, Pratville, erdb.rnopco.com
AK, *, *, erdbak.bpac.com
AS,*,*, americansamoa-territorialauthority-erdb.asta.gov
:
: denotes actual contents not shown for brevity
:
FM,*,*,    (comment – example of blank list; e.g. no ERDB for Federated States of
Micronesia at this stage)
:
: denotes actual contents not shown for brevity
:
TX, *, *, erdbsw.sbc.com
:
: denotes actual contents not shown for brevity
:
WY, *, *, erdbwy.bigsky911.com;erdbnc.bpac.com
<eof>
```

3 Security

The critical nature of the E9-1-1 Emergency Services Network makes it essential to ensure that the E9-1-1 network is properly protected. The i2 solution introduces new network elements, new underlying transport networks and protocols to the E9-1-1 Emergency Services network. Note that a number of protocol interfaces are outside the scope of the 9-1-1 system (V0/V1/V5/V6) and several that are between elements that are considered to be within the 9-1-1 system (V2, V3, V4, V7). The former are specified by other standards organizations, such as the IETF. The latter are defined in this document. For the interfaces within the scope of this document, the security mechanisms are dependent on the specifics of the underlying network joining the various i2 solution network elements.

Specifically, if the network that joins the network elements is private, secured, and managed such that there is no reasonable possibility that anyone not specifically authorized to see E9-1-1 data (and specifically location data) has access to any systems on that network, it will not be required to deploy additional security measures. It should be noted that it is extremely difficult to guarantee that

a network is completely private, secured and managed with no reasonable possibility of unauthorized access, therefore it is not recommended that such "walled gardens" be the only security provided. It is recommended that if even if private networks are used to implement the i2 interfaces, additional security mechanisms described in this section be used.

The following sections provide recommendations on the steps that can be taken to minimize the risk of compromise to the E9-1-1 network.

3.1 Authentication

Authentication is the process of verifying the claimed identity of a session requester. Mutual authentication is important to ensure that both the originator of the session and the recipient of the request are both satisfied with the credential information being provided. Authentication mechanisms are needed in the i2 solution to ensure that only trusted entities with existing relationships will be provided access to E9-1-1 data and services.

Authentication in the i2 solution is provided by using certificates. A certificate is a data object that includes the server's identity and its public key. The certificate is signed by computing its hash value and encrypting it using a certificate authority's private key. A certificate authority is a trusted third party that issues digital certificates. The certificate authority guarantees that the holder of the digital certificate is who they claim to be. NENA shall create (or contract for) a Valid Emergency Services Authority (VESA) to operate as a certificate authority, and to be the root of all certificates issued to entities participating in an i2 call.

It is recommended that elements involved in the i2 solution deploy strong authentication (RSA-1024 or better, as documented in RFC2313[14]) using X.509 certificates and Certificate Revocations Lists as profiled in RFC 3280[15] and best current practice.

3.2 Message Integrity

Message integrity mechanisms provide protection against unauthorized message modifications. One of the ways this is accomplished is by using one-way hash functions. Hashing is the transformation of a string of characters into a usually shorter, fixed-length value that represents the original string. If the original message is tampered with, the message hash will not match the original message. This helps to detect that the message was tampered with.

It is recommended that elements involved in the i2 solution deploy message integrity using Secure Hashing Algorithm-1 (SHA-1), as defined in RFC3174 or better.

3.3 Message Encryption

Message encryption is a process of disguising a message in such a way as to hide its substance. The need for encryption of messages is a function of the level of confidence in the network being used to implement the i2 solution interfaces. If the network being used to implement an i2 solution interface is vulnerable, then encryption techniques should be implemented to protect the messages.

If encryption is needed, Advanced Encryption Standard (AES), FIPS PUB 197[16] or better will be used as the means to encrypt the messages.

3.4 Network Element Security

An important aspect of maintaining security in a network is ensuring that the network elements that constitute the network are secure. This includes physical security of the equipment and ensuring that data contained in the network elements are accessed by only those personnel that have a need to access the data.

It is recommended that network elements involved in the i2 solution employ authorization and privacy mechanisms to protect E9-1-1 data.

The network elements should support the ability to authenticate users, control user access privileges, initiate audit trails, report security alarms, recover from intrusions, and monitor data and system integrity.

3.5 Network Layer Security

If the i2 solution interfaces are implemented on a network that is not private, secure and managed, tunneling is an alternative that could be used to implement the interfaces. One acceptable mechanism is to use IPSEC tunnels with strong authorization, integrity protection and privacy, at least equivalent or stronger than RSA-1024/SHA-1/AES joining network elements which are secured, and managed such that there is no reasonable possibility that anyone not specifically authorized to see E9-1-1 data (and specifically location data) has access to any system within the networks defined by such tunnels. Note that this usually implies that the tunnels are established between the actual network elements running the protocols, rather than the local area network on which such elements reside.

If tunneling is used to implement the i2 solution interfaces, it is recommended that IPSEC, RFC2401[17], be used with strong authentication using RSA-1024 or stronger, integrity protection using SHA-1 or better and ensuring privacy using AES or better.

3.6 Application Layer Security

The applications themselves can be secured using, for example, Transport Layer Security (TLS), RFC2246, with strong authorization, integrity protection and privacy, at least equivalent or stronger than RSA-1024/SHA-1/AES (RFC-3268 "*Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*" Chown) long as the systems the protocols are running on are reasonably protected against unauthorized persons being able to modify the applications.

It is recommended that TLS be used to secure Vx interfaces (i.e., V2, V3, V4, and V7).

3.7 Location Data Security

The existing Emergency Services Network provides a relatively high degree of security for correctness of information, integrity, and authorization of access, authenticity/secrecy, and accuracy

of information. The intent of the NENA i2 solution is to provide functional equivalency to the existing network services in an IP-based environment, and this includes ensuring that the location information is valid and secure.

Voice over IP presents new challenges and security issues as it breaks the bond between access and service provider characteristic of legacy networks and at this time lacks the legislative and regulatory requirements that apply to more conventional telephony services. These security threats present themselves in a number of forms and have varying degrees of severity should they be exploited to their full potential. This section attempts to outline the key security concerns related to location data, and where in the i2 solution these concerns are best addressed. This section does not in itself provide solutions to these concerns.

Current networks use location information to route calls to the local PSAP, and to provide a location to which emergency responders may be dispatched. Three important characteristics of existing networks contribute to the security of these functions:

1. The source of the location is attributable to a specific trusted source. Location is provided by the access/voice service provider.
2. The location information is applicable to a specific point in time. The location information is either used to directly route the call (as may be the case for wireless), or indirectly via the calling number/ANI (as for wireline). It is always retrieved at the time of call receipt.
3. The location information can be identified as belonging to a specific end-point. This may be a direct association as is the case with wireline, or it may be an indirect association, as is the case with ESRKs in wireless. The location information is known to apply specifically to the calling device; another device's location cannot be misrepresented as the calling device's location.

In order to provide service equivalence therefore, the location information obtained and used in the delivery of VoIP emergency calls must satisfy these three requirements.

The i2 solution proposes a Location Information Server (LIS) be the source for distributing location information within an access network. Furthermore the validity, integrity and authenticity of this information are directly attributed to the LIS operator. The i2 solution therefore should provide:

1. A mechanism to ensure that location data has been provided by a LIS with a known responsible operator and that it has not been changed by any other party since that LIS provided the data.
2. A mechanism to ensure that a location object (PIDF-LO document) cannot be applied to more than one calling device.
3. A mechanism to ensure that the location information is still true and applicable to the calling device at the time it is provided to the emergency network.

The majority of security concerns for the i2 solution are therefore focused on ensuring that location information is accurate, valid, authentic and associated with a specific call instance. While secrecy and privacy of location information may be of some importance, these are deemed secondary to

routing and PSAP requirements. Sections defining the individual i2 element interfaces will provide requirements addressing specific security aspects of each interface.

Location determination is out of scope for NENA, but we can offer guidance on what should be considered when designing mechanisms to report location:

1. The location object should be digitally signed
2. The certificate for the signer (LIS operator) should be rooted in VESA. For this purpose, VPC and ERDB operators should issue certs to LIS operators.
3. The signature should include a timestamp
4. Where possible, the Location Object should be refreshed periodically, with the signature (and thus the timestamp) being refreshed as a consequence.
5. Antispoofing mechanisms should be applied to the Location Reporting method.

4 Functional Requirements

This section provides high-level functional requirements for the new elements in the i2 solution architecture that are described briefly in Section 2.3. For elements defined in other standards (e.g., Call Server, Routing Proxy, Redirect Server), this document identifies only incremental functional requirements to support the i2 solution.

4.1 VSP Call Server/Proxy

This element is owned by the VSP and is always present, and always in the signaling path of a call. If the signaling protocol is SIP, this element is a proxy server as defined in RFC3261. The VSP Call Server receives a call from one of its subscribers on the V1 interface and must recognize that it is an emergency call. Procedures for this vary depending on protocol and end device capability. For SIP based systems, VSPs must be capable of recognizing an emergency call (e.g., based on the tel uri with digits 9-1-1 as well as recognizing the sip:sos@<localdomain>).

Upon determining that a call is an emergency call, the VSP must determine the location of the caller. Location Information may accompany the call (in SIP, this would be in the form of a PIDF-LO body on the INVITE message), may be requested of the endpoint, or the VSP may have a LIS which has the location of the caller.

The VSP Call Server may be implemented in one of several ways:

1. It may operate or contract with a VPC
2. It may operate or contract with a Routing Proxy
3. It may operate or contract with a Redirect Server

In case 1, the VSP Call Server maintains a V2 interface. It queries the VPC for ESRN/ESQK by sending information on the V2 interface. The VSP Call Server maintains a routing table which maps

an ESRN to the URI of the appropriate ESGW. It uses this table to obtain the URI, and forwards the call on the V4 interface, with the ESRN and ESQK, to the ESGW. At end of the call, the call server is responsible for sending a call termination message to the VPC which includes the identity of the ESGW that was used for the call.

In case 2, the VSP Call Server unconditionally forwards all emergency calls, to the Routing Proxy on the V6 interface. The Routing Proxy would be expected to interact with the VPC to obtain call routing information and to forward the call to the correct ESGW.

In case 3, the VSP Call Server unconditionally forwards all emergency calls, to the Redirect Server on the V5 interface. It should expect to receive the call back from the Redirect Server with ESRN and ESQK. The VSP Call Server would maintain a routing table which maps an ESRN to the URI of the appropriate ESGW. It would use this table to obtain the URI, and forward the call on the V4 interface, with the ESRN and ESQK, to the ESGW. . The Call Server notifies the redirect server when the call has terminated and this indication contains the identity of the ESGW.

In cases of failure, the Call Server shall be capable of providing contingency routing based on the last routing option that it receives

For Call Servers using SIP, the Record Route header should be specified to keep the server in the signaling path of the call.

The Call Server shall keep call event records for trouble shooting purposes.

It is recommended that the Call Server shall save, for trouble shooting purposes, the following information associated with a call –

- ESQK
- Identity of VPC used
- Date time stamp of VPC response
- Disposition of call (e.g., ESRN or LRO used)
- Call history

4.2 Routing Proxy Server

This element is optionally present in the call path. If the signaling protocol is SIP, this element is a proxy server as defined in RFC3261. When deployed, the Routing Proxy receives emergency calls (only) forwarded from the VSP Call Server on the V6. It maintains a V2 interface. It queries the VPC for ESRN/ESQK by sending information on the V2 interface. The Routing Proxy would maintain a routing table which maps an ESRN to the URI of the appropriate ESGW. It would use this table to obtain the URI, and forward the call on the V4 interface, with the ESRN and ESQK, to the ESGW.

For Routing Proxies using SIP, the Record Route header should be specified to keep the proxy in the signaling path of the call.

In cases of failure the routing proxy shall be capable of providing contingency routing based on the last routing option that it receives

For routing proxies using SIP, the Record Route header should be specified to keep the routing proxy in the signaling path of the call.

Routing proxy shall keep call event records for trouble shooting purposes.

It is recommended that the routing proxy shall save, for trouble shooting purposes, the following information associated with a call –

- ESQK
- Identity of VPC used
- Date time stamp of VPC response
- Disposition of call (e.g., ESRN or LRO used)
- Call History

4.3 Redirect Server

This element is optionally present. If the signaling protocol is SIP, this element is a proxy server as defined in RFC3261. When deployed, the Redirect Server receives emergency calls (only) forwarded from the VSP Call Server on the V5 interface. It maintains a V2 interface. It queries the VPC for ESRN/ESQK by sending information, including location, on the V2 interface. It then unconditionally forwards the SIP 300 Message on the V5 interface, with ESRN and ESQK back to the VSP Call Server. The VSP Call Server would then route the call, based on the ESRN, to the correct ESGW.

The Redirect Server shall support a mechanism to allow it to receive a call termination notification.

The Redirect Server shall support the capability to indicate to the VPC that a call has terminated.

4.4 ESGW

The ESGW takes VoIP delivered calls and converts them to Time Division Multiplexing (TDM) signaling for delivery into the E9-1-1 Selective Routing Network.

The ESGW implements the V4 interface. It accepts a call with an ESRN and ESQK and uses the ESRN to select an output trunk group to the E9-1-1 network. The ESGW maintains a mapping table between the ESRN and the appropriate output trunk group. It is expected that the ESGW will implement dedicated 9-1-1 trunks to the SR.

These trunk groups or routes use traditional telephony signaling schemes to deliver the emergency call over dedicated voice channels between the gateway and the E9-1-1 network. These trunks originate at the ESGW and terminate at the selective router, as designed to meet the needs and constraints of the particular Enhanced 9-1-1 network for the caller's location. It is assumed dedicated E9-1-1 trunks to the SR are used.

In general, the trunking protocol, and the trunk design will be determined based on the capabilities (and requirements) of the destination E9-1-1 network.

Likely candidates for these circuits are:

1) SS7 signaling where the IAM has the called number of 911, and the Charge and/or Calling Party Number the 10 digit ESQK used to represent the call key.

2) Traditional CAMA signaling (called number = 911 or 11 + ANI of the form I [single info digit] + a 7 ESQK value, both digit streams contained between the Kp and St pulses). Note that since the ESGW will be receiving a 10-digit ESQK value, this assumes that the ESGW will convert the received 10-digit ESQK value to a 7-digit ESQK value.

These may not be used to originating traffic back into the ESGW, but once the call is established, provide for two way voice communication.

In general, the 9-1-1 service provider will have technical standards, or accessibility letters that define the allowable signaling schemes allowable to be used within their network. In many cases, the ESGW operator may also need to negotiate with the individual Public Safety Operators within a given geographic area before these circuits can be ordered to, or through the SR Operator.

Sizing of trunk groups between ESGWs and SRs is a subject for a future study. This is a complicated issue because unlike wireline call delivery where an end office serves a fixed population, the population served by a VSP is expected to be variable. Further complicating this issue is the fact that a VSP is probably connected to multiple ESGWs and ESGWs are expected to be connected to multiple VSPs. This many-to-many relationship makes determination of VoIP 9-1-1 traffic loads at ESGWs an issue that needs further study.

4.5 ERDB

This section provides the high-level functional requirements for the ERDB.

The ERDB has two main functions:

- the ERDB is responsible for storing boundary definitions for each ESZ in its service area, along with associated routing information
- the ERDB is responsible for delivery of routing information to the VPC.

4.5.1 Receiving and Storing Routing Information

The ERDB shall support storage of the boundary definitions for ESZs and the mapping of civic address or geo-spatial coordinate location information to a particular ESZ.
The ERDB shall be able to identify the ESZ associated with any given civic address in its serving area, where the civic address can be uniquely mapped to an MSAG-valid address.
The ERDB shall be able to identify the ESZ associated with any given pair of coordinates that are within its serving area.
The ERDB also stores attributes for each ESZ. For each ESZ, the ERDB shall be able to store the following information needed for routing:

- an ESRN associated with the primary SR that serves the ESZ in the i2 solution
- the *routing ESN* within that primary SR that is associated with the ESZ.

Some PSAPs use *administrative ESNs*, different from the routing ESN associated with the ESZ. This administrative ESN is also used in the ALI DB to identify a particular set of Police, Fire, and

Medical English Language Translations. The ERDB shall also be able to store an administrative ESN for an ESZ, if applicable.
CRNs are 10-digit 24x7 PSAP numbers that are used for routing emergency calls under network failure conditions. A CRN must be associated with each SR/ESN combination. Therefore, if the ESRNs are assigned one per SR/ESN pair, the CRN will also be associated with the ESRN. If the ESRNs are assigned to an SR and more than one ESN, the CRN will need to be associated with the ESRN and the specific ESN.
ESRNs shall be defined as 10 digits in length, in order to assure compatibility of translations required within the ESGW.
ESNs shall be defined as at least 5 digits in length (including leading zeros), in order to assure compatibility with MSAG values.
The ERDB shall be able to associate a CRN with either one of

- a given ESRN
- a given ESRN/ESN pair.

The ERDB may also associate additional data with an ESZ that can assist in tracking and troubleshooting problems. This might include for example,

- a unique identifier for the SR serving that ESZ in the i2 solution.

4.5.1.1 Data Management

The ERDB shall support a database structure that will allow for additional attributes to be easily associated with an ESZ.

The ERDB database management shall allow for multiple agents to simultaneously perform database maintenance (data object creation, update, deletion) on the routing data.

The database structure shall be capable of supporting real-time queries.

4.5.1.2 Authentication and Authorization

The ERDB shall be able to authenticate the sources from which it receives source data for inclusion in the ERDB. Based on the credentials of the source, the ERDB shall control the source's access to view, enter, and modify information in the ERDB.

4.5.1.3 Data Integrity

The ERDB database management shall enforce consistency of routing information whether a given location is defined as a civic address or as geo-spatial coordinate information.

The ERDB shall provide for automatic as well as manually initiated audits of the integrity and consistency of the routing data.

4.5.2 Processing Routing Queries

The ERDB shall be able to receive either or both civic and geo location information in a routing query.

Whenever the ERDB receives a routing query containing valid location information from an authorized VPC, the ERDB shall attempt to map the location information to the applicable ESZ and its associated routing information.

If both civic location and geo location information are included in a routing query, the ERDB shall be configurable to support using either element or both, in a specified search order, in the attempt to determine the routing information

4.5.2.1 Authentication and Authorization of Routing Queries

The ERDB shall support the capability to authenticate the entities from which it is allowed to receive routing queries.

Based on the credentials of the entity from which a routing query is received the ERDB shall support the capability to control the access of the entity to routing information in the ERDB.

4.5.2.2 Civic Location Information (Street Address) Received in Routing Query

The ERDB shall be able to receive the components of a civic address that are defined for the Presence Information Data Format – Location Object (PIDF-LO) defined in the PIDF-LO draft of the IETF Geopriv WG. These include the following components that may be used in determining routing information:

- State/Province
- County Name
- Civic (MSAG) Community Name
- Postal Community Name
- Postal Code
- Prefix Directional
- Street Name
- Street Suffix
- Post Directional
- House Number
- House Number Suffix (if applicable)

The ERDB shall be able to recognize an alphanumeric County Name. In the USA, the ERDB shall also be able to recognize a numeric Federal Information Processing Standard[5] (FIPS) County ID in the County Name. In the USA, the ERDB shall support the capability to convert a County Name to a Federal Information Processing Standard[6] (FIPS) County ID value for the county, if County ID is used within the ERDB for determining routing in a given area.

[5] Federal Information Processing Standard (FIPS), PUB 6-4.
[6] Federal Information Processing Standard (FIPS), PUB 6-4.

The ERDB shall be able to recognize either Postal Addresses or MSAG Addresses, as defined in Section 4.7, received in the civic address information. If a valid address (i.e., one that can be uniquely mapped to an MSAG-valid address) is received, then the ERDB shall be able to use it to determine routing information and to identify MSAG-valid formats.
If the civic location information contains a valid address within the ERDB's serving area, the ERDB shall use this information to determine the ESRN, the routing ESN, and the CRN associated with the identified ESZ. If there is a separate administrative ESN associated with the ESZ, the ERDB shall also be able to determine the administrative ESN.

In addition, for postal civic addresses, the ERDB shall be able to transform a valid postal civic address to the MSAG-valid format for that address.

4.5.2.3 Geo Location Information Received in Routing Query

If the routing query contains geo location information (latitude and longitude), that identifies a location within the serving area of the ERDB, the ERDB shall be able to determine the ESRN, the routing ESN, and the CRN associated with the identified ESZ in response to the routing query. If there is a separate administrative ESN associated with the ESZ, the ERDB shall also be able to determine the administrative ESN.

The geo location information is expected to be in the form of decimal degrees, using WGS84 coordinate system.

4.5.2.4 Responding to Routing Queries

If the ERDB is able to successfully use the received location information to determine the routing information, the ERDB shall follow the requirements in Section 5.10 to send a response to the VPC, including the following routing information:

- ESRN
- [routing] ESN
- CRN, if available
- Administrative ESN, if applicable.
- An indication of whether civic or geo location information was used to determine routing (if both civic and geo location information were received).

If civic location information was received in the routing query, the ERDB shall also include the transformed address information in its response to the VPC. The MSAG-valid address includes the following data elements, as applicable:

- State/Province
- Civic (MSAG) Community Name
- Prefix Directional (if applicable)
- Street Name
- Street Suffix (if applicable)

- Post Directional (if applicable)
- House Number
- House Number Suffix (if applicable)

4.5.2.5 Steering of Routing Queries

If the ERDB receives a routing query from a VPC, and the received location information is not within the ERDB's serving coverage area, the ERDB may support one of the following:

— The ERDB may steer the routing query to the appropriate ERDB and then pass the received response from that remote ERDB toward the requesting VPC.

— The ERDB may indicate that the address is not found, following the requirements in Section 2.10 and Section 5.10, and may include a URI for an appropriate alternate ERDB in its response.

4.5.2.6 Error Handling

If the ERDB receives civic or geo location information that identifies a location within its serving area for which it cannot determine the routing information, the ERDB shall return a response to the VPC indicating that routing information is not available, also including the reason for the failure.

If the ERDB receives civic or geo location information that identifies a location which is not within its serving area and it cannot determine the ERDB to which the civic or geo location information should be steered, the ERDB shall return an error response to the VPC indicating that routing information is not available and indicating the reason for failure.

If the ERDB receives an error message in response to a routing query steered to another remote ERDB, the ERDB shall pass the received error response received from the remote ERDB to the VPC, including the reason for failure

4.5.2.7 Performance

The ERDB shall be able to respond to a routing query containing a valid, known civic location within 200 ms.

The ERDB shall be able to respond to a routing query containing a geo location with a pair of coordinates that are within the boundaries of its serving area. If the coordinates lie within the serving area of the ERDB, the ERDB shall be able to respond to the routing query within 200 ms.

4.5.3 Reliability and Availability

The ERDB shall be available to support routing queries with a reliability of 99.999%.

4.6 VPC

This section provides the high-level functional requirements for the VPC. The main functions of the VPC are to:

- support the routing of emergency calls originated by VoIP customers to the appropriate PSAP by providing critical routing information to the Call Server/Proxy
- deliver caller location information in response to queries from ALI databases.

4.6.1 Support for Emergency Call Routing

There are a number of capabilities required of the VPC to support its role in providing routing information to the Call Server/Proxy to support the routing of VoIP emergency calls. The VPC must be able to process routing requests from a Call Server/Proxy, and if necessary, interact with an LIS to obtain the caller's location information. The VPC must use the location information, obtained from the routing request or from the LIS, to generate a routing query to an ERDB to obtain routing information associated with the caller's location information. The VPC must then use this information to generate a response to the Call Server/Proxy's routing request. In addition, the VPC will have to support contingency/default routing under certain failure scenarios. The following subsections describe the functionality required of the VPC to support each of these aspects of VoIP emergency call routing.

4.6.1.1 Processing of Routing Requests from the Call Server/Proxy

The VPC shall be capable of receiving and processing a routing request from a Call Server/Proxy, over a V2 interface that contains the following information:

- Identification of the entity that is requesting emergency call routing, including a 24x7 number/address that can be used to reach that entity and the NENA ID associated with that entity
- An identifier that can be used to uniquely identify the call/transaction at the Call Server/Proxy
- An E.164 callback number that can be used by the PSAP to reach the call originator, if available
- A Location Information Element (LIE) containing either a PIDF-LO or a location key to support interactions with an LIS to obtain the PIDF-LO.
- An identifier for the caller's Voice Service Provider, if available

In addition, the VPC shall be capable of processing the following optional information in a routing request from a Call Server/Proxy:

- A Date Time Stamp indicating the time the message was sent
- An identifier for the destination VPC
- An identifier inserted by the originating network that may be used by an LIS to validate that the received Location Key belongs to the originating network.

The VPC shall support the capability to authenticate the entities from which it is allowed to receive routing requests.

Based on the credentials of the entity from which a routing request is received, the VPC shall support the capability to control the access of the entity to routing information accessible by the VPC.

4.6.1.2 Generation of Queries to LIS to Obtain Location Information

If the VPC does not receive a PIDF-LO in the LIE of the routing request from the Call Server/Proxy, the VPC may query an LIS for caller location information, based on agreements between the VPC provider, the LIS provider, and the VSP. If the VPC determines that a query should be launched, it shall use the contents of the Location Key in the LIE to determine the LIS that should be queried for the caller's location. Once it has determined which LIS to query, the VPC shall generate a query message that contains the following information:

- The identifier of the VPC
- The LIE containing Location Key information
- A Message ID that uniquely identifies the message, to support the correlation of the query and the response message by the VPC.

In addition, the VPC may include the following information in the query it sends to the LIS requesting caller location information:

- An identifier that can be used by the LIS to determine whether the Location Key belongs to the VEP that originated the request. This information shall be included if received by the VPC in the routing request from the Call Server/Proxy.
- A Date Time Stamp indicating the UTC date and time the message was sent.

The VPC shall be capable of receiving and processing a response message from the LIS that contains the following information:

- The identifier of the responding LIS
- The LIE containing the location key information, and if the request for location information is successful, caller location information
- An indication of whether or not caller location information was successfully determined, and the nature of the location information being returned (i.e., civic, geodetic, both)
- A Message ID that uniquely identifies the message to support correlation of the response with the query message.

In addition, the VPC shall be capable of processing the following optional information, if received in the response from the LIS:

- The Position Source, indicating the type of positioning used to determine the location (e.g., network cell sector, handset GPS).
- A Date Time Stamp indicating the UTC date and time that the message was sent.

4.6.1.3 Generation of Routing Queries to the ERDB

Once the VPC receives an LIE containing caller location information, the VPC shall query an ERDB to obtain routing data for the call. The VPC shall identify the appropriate ERDB to which to direct

the routing query by accessing discovery data that identifies the URL of the ERDB(s) that serves the emergency caller's location. If the VPC has received caller location information consisting of a PIDF document that contains more than one tuple, where each tuple contains a status element with a geopriv location element, the VPC shall select the first tuple (i.e., the tuple containing the highest priority location) as the basis for ERDB discovery. The VPC shall select the first piece of information in the first tuple as the basis for discovering the ERDB. (See Section 2.10 for further detailed description of the ERDB discovery mechanism.)

Having identified the ERDB to which to direct the routing query, the VPC shall formulate a query that contains the following information:

- A Message ID that will identify the message and allow for correlation of the query and the response
- The identifier of the node requesting the routing information (e.g., the VPC)
- A civic location, a geo location,, or both a civic location and a geo location

Note that the VPC shall use the first location-info element information to populate the routing query. If the location information contains a geo location, and the coordinate system associated with that geo location is something other than WGS84, the VPC shall convert the geo location to WGS84 prior to sending it to the ERDB in the routing query.

In addition to the information identified above, the VPC may also include the following information in the routing query to the ERDB:

- A Date Time Stamp indicating the UTC date and time that the message was sent
- Identification of the ERDB from which routing information is being requested.

4.6.1.4 Processing of Routing Responses from the ERDB

The VPC shall be capable of processing a routing response from the ERDB that contain the following information:

- A Message ID that allows for correlation of the query and the response
- The identity of the node directly responding to routing query sent by the VPC
- The ESRN associated with the caller's location
- The routing ESN associated with the caller's location
- The administrative ESN associated with the caller's location (if present in the routing data at the ERDB)
- The CRN that identifies the 24x7 E.164 number of the alternate PSAP to which emergency calls should be routed under various abnormal conditions, if present in the routing data at the ERDB. (See Section 2.8 for further discussion of contingency/default routing procedures.)
- An indication of whether the ERDB was successful in providing routing information, and the basis on which the routing information was determined (i.e., a civic location or a geo location)

- The MSAG-valid format of the civic address provided by the VPC in the routing query
- A VPC Identifier that identifies the VPC that initiated the query
- A Date Time Stamp that indicates the UTC date and time that the message was sent
- An identification of the ERDB that was the original source of the routing information (which may or may not be the same as the ERDB that is directly connected to the querying VPC)
- An identification of an alternate ERDB that might have the routing information requested by the VPC, if the directly connected ERDB does not have it.

Upon receiving the response message from the ERDB, the VPC shall use the ESRN/ESN contained in the response message to identify the appropriate pool of ESQKs for the call. From this pool of ESQKs, the VPC shall select an available ESQK value to associate with the call. The VPC shall also set a guard timer once the ESQK has been associated with the call. The specific value of the guard timer is to be determined. The VPC shall maintain an association between the ESQK and the other call-related information (e.g., callback number, location, Provider information) until it either receives an indication from the Call Server/Proxy that the call has terminated or the guard timer expires (whichever occurs first), at which point the ESQK value will be released.

The VPC shall hold one ESQK value within each pool in reserve to be used when there are no other ESQK values within the pool available for association with an emergency call request. The VPC shall associate this reserved (i.e., default) value with all new emergency call requests that require an ESQK from a particular pool until such time as another ESQK value within that pool becomes available.

4.6.1.5 Generation of Responses to Routing Requests from a Call Server/Proxy

Once the VPC has received the routing data from the ERDB, and determined the ESQK value for the call, it shall prepare a response to the routing request it received from the Call Server/Proxy. Under normal conditions, this response message shall contain the following information:

- The identifier of the responding VPC
- An identifier that uniquely identifies the call at the Call Server/Proxy
- The ESRN received in the ERDB response
- The ESQK allocated by the VPC to the call
- The CRN received in the ERDB response to be populated in the LRO parameter
- An indication of whether or not the VPC was successful in providing the requested routing information, and the basis for determining the routing information (i.e., routing information based on civic or geodetic information, obtained from the routing request or via a query to the LIS.

In addition, the VPC may also include the following optional information in the routing response to the Call Server/Proxy:

- A Date Time Stamp indicating the UTC date and time that the message was sent.
- The identifier of the entity that requested emergency call routing.

4.6.1.6 Release of ESQKs

To minimize the risk of running out of ESQKs, the i2 Solution calls for a disconnect indication to be sent to the VPC when a call is released, to enable the VPC to release ESQKs that are no longer in use. This is accomplished by having the Call Server/Proxy send a call termination message to the VPC at the conclusion of an emergency call. The VPC shall be capable of receiving a call termination message that contains the following information:

- Identification of the routing node directly adjacent to the VPC
- An identifier that uniquely identifies the call at the Call Server.
- The ESQK that was allocated by the VPC for the emergency call (i.e., the ESQK value that can now be returned to the ESQK pool at the VPC).
- The identifier of the ESGW that was used to direct the call to the Selective Router, if available.

In addition, the VPC shall be capable of receiving and processing the following information, if provided in the call termination message from the Call Server/Proxy:

- A Date Time Stamp indicating the UTC date and time the message was sent.
- The identifier of the VPC.

Upon receiving a call termination message, the VPC shall return the ESQK value identified in the message to the pool of available ESQKs, and shall respond by sending a call termination acknowledgment message that contains the identifier of the VPC and an identifier that uniquely identifies the call at the routing element that sent the termination message. The VPC may also include a Date Time Stamp in the acknowledgement message, indicating the UTC date and time the message was sent.

4.6.1.7 Support for Contingency/Default Routing

There are a number of errors or abnormal conditions (e.g., failures) that may occur in the process of routing emergency calls originated by VoIP users to the appropriate Selective Router in the Emergency Service Provider's network. This section describes abnormal conditions that might be detected by the VPC, and describes the actions that should be taken by the VPC under these conditions.

One type of error that may be detected at the VPC involves problems with the structure or content of the routing request sent to the VPC by the Call Server/Proxy, or queries from the VPC to the ERDB or LIS. These error scenarios include the following:

- The VPC receives a badly structured routing request from the Call Server/Proxy (i.e., the request message cannot be parsed or is malformed).

- The routing request from the Call Server/Proxy contains neither a Location Key nor a PIDF-LO.
- The VPC receives a PIDF-LO in the routing request from the Call Server/Proxy, but it cannot determine, based on the received location, which ERDB to query for the routing data.
- The VPC receives a PIDF-LO in the routing request from the Call Server/Proxy, but when it uses it to query the ERDB for routing data, it receives either an error response or no response from the ERDB.
- The VPC receives a Location Key in the routing request from the Call Server/ Proxy, but it cannot determine where to send the location query (i.e., it cannot determine the appropriate LIS).
- The VPC receives a Location Key in the routing request from the Call Server/ Proxy, and is unable to successfully retrieve a PIDF-LO from the LIS (i.e., it receives an error response or no response from the LIS).

In all of these scenarios, the VPC is unable to successfully obtain routing data from the ERDB and provide it in a response to the Call Server/Proxy.

If the VPC is unable to successfully obtain routing data from the ERDB and provide it in a response to the Call Server/Proxy, the VPC shall send a response message to the Call Server/ Proxy that indicates the nature of the error that occurred. The message may also include a default routing number (i.e., a 24x7 number associated with a call center), as determined based on prior agreements between the VPC provider, the VoIP Service Provider, and the call center to which calls are to be default-routed. (The default routing number will be populated in the Last Routing Option parameter of the response message.)

Another type of abnormal condition that might be encountered at the VPC is related to a lack of resources at the VPC. As described previously, one of the roles of the VPC is assigning an ESQK to an emergency call from the appropriate ESQK pool that is associated with the ESRN/ESN information received from the ERDB. It is possible, in certain situations, for the VPC to successfully receive routing data from the ERDB, but have no ESQKs available from the applicable pool (other than a default ESQK) to associate with the specific call instance. The ESQK exhaust could be caused by an unusually large number of calls being originated from a particular geographic area, or due to some error in the allocation of the ESQK pool or in the de-allocation process. If the VPC successfully receives routing data from the ERDB, but does not have an ESQK available from the pool associated with the ESRN/ESN provided in the ERDB response, the VPC shall return a routing response message to the Call Server/ Proxy that contains the reserved (i.e., default) ESQK value for the pool, along with the ESRN and CRN provided in the response from the ERDB. (The CRN will be populated in the Last Routing Option parameter of the response message.)

A potential error scenario that could be encountered at the VPC related to the release of ESQKs is the receipt of a call termination message containing an ESQK value that is not in use. If such an error occurs, it is desirable that the VPC log the error and make a maintenance count.

4.6.2 Delivery of Location Information

As described above, the VPC will play an important role in delivering call and location-related information for VoIP emergency calls to the ALI database for subsequent delivery to the PSAP to which the emergency call was routed. This will require the VPC to be capable of processing location information requests from an authenticated, authorized ALI database, and providing the call and location-related information associated with an identified call instance in response.

The VPC shall store call and location-related information about an emergency call at least until this information is delivered to the ALI database. In particular, the VPC shall store the location information provided to the ERDB in a routing query

For purposes of tracking and troubleshooting, it is desirable that the VPC retain archival storage for call and location-related data after an emergency call is released, for a configurable period of time, to be negotiated with the PSAPs served by the VPC. The VPC should retain, for example, a record of the Callback information, the allocated ESQK and the date/time it was allocated (to support searching for information related to a particular call instance), location information used for determining routing, VSP identification and ESGW identification information, the routing information received from the ERDB and used for routing the call and identification of the ERDB that provided the routing information.

To assist PSAPs in troubleshooting, the VPC shall support a user interface that will allow an authorized agent of the VPC operator to search for and view call and location-related data for any call instance associated with a given ESQK in a given time interval.

4.6.2.1 Processing Location Queries

The VPC may receive location queries from one or more ALI databases. The VPC must be able to identify and authenticate the entities from which it receives these queries to ensure that information is only provided to those entities that are entitled to receive it. Therefore, when the VPC receives a properly constructed Emergency Services Positioning Request (ESPOSREQ) message (as described in Section 5.8) from an ALI DB, the VPC shall first determine whether the requesting entity is authorized to access emergency call and location-related data. If the requesting entity is authorized, the VPC shall use the ESQK contained in the Emergency Services Routing Key parameter of the ESPOSREQ message to identify the call instance, and to look up the associated call and location-related information stored at the VPC.

4.6.2.2 Generating Responses to Location Queries

4.6.2.2.1 Successful Responses

If the VPC can successfully obtain the call and location-related data associated with the call instance identified by the ESQK in the ESPOSREQ message, the VPC shall construct an Emergency Services Positioning Request Response (esposreq) message and send it to the ALI database identified by the ESMEIdentification parameter in the received ESPOSREQ message. The esposreq message shall contain the following key pieces of information:

- The ESMEIdentification coded with the identification of the ALI Database that initiated the query.

- A PositionResult.
- One or both of:
  - Position information consisting of latitude and longitude as WSG84 information, and altitude in meters, if available. If present, a Position Source will also be provided to identify the method used to determine the location information.
  - A Location Description (consisting of detailed street address information), if the location information associated with the call instance is populated with a civic location.
- A Callback Number, if available in the information associated with the call instance.
- An Emergency Services Routing Key, populated with the ESQK received in the ESPOSREQ.
- An ESQK Date and Time Stamp.
- A CompanyID, if the data associated with the call instance includes the NENA ID for the VSP. If the NENA ID for the VSP is not available then the NENA ID of the entity at the other end of the V2 is provided.

See Section 5.8 for further details related to the coding of the esposreq message.

The VPC shall use the civic location information received in the response from the ERDB to populate the civic location information in this response message.

4.6.2.2.2 Error Responses

The VPC may be unable to provide location information in response to a request from the ALI database due to the following conditions:

- The VPC experiences a system failure resulting in the inability to look up the information
- The requesting entity is not authorized to access location data for emergency calls
- Unexpected data is received in the location request
- The ESQK identified in the request does not have any stored data associated with it.

If one of the above conditions occurs, the VPC shall report the error condition to the requesting ALI database by returning an Emergency Positioning Request Return Error message with the appropriate Error Code value. See Section 5.8 for further details related to the coding of this message.

If the VPC is receives a badly constructed query from an authenticated entity, the VPC shall report the problem by returning an Emergency Positioning Response Reject message containing the appropriate Problem Code. See Section 5.8 for further details related to the coding of this message.

4.6.3 Performance

The VPC shall take no more than 200ms to respond to routing requests from Call Servers/Proxies.

The target performance for responding to a location query from an ALI Database is 50ms.

4.6.4 Reliability and Availability

The VPC application shall be highly reliable and available. It is an objective that the VPC be available to a querying element (e.g., Call Server/Proxy, ALI Database) at a service availability level of 99.999%.

4.7 Validation Data Base (VDB)

This section provides the high-level functional requirements for the VDB. The main functions of the VDB are to:

- Store MSAG validation (MSAG valid civic addresses) for a given area – it is expected that there will be multiple VDBs supported by the various (entities) and each contains a mechanism to validate data to conform to the MSAG for the given jurisdiction.
- Perform MSAG Validation of a Civic Address request

The legally designated 9-1-1 authority for the jurisdiction may provide this service, or it may be delegated to an authorized entity.

4.7.1 Storage of MSAG Validation

The VDB shall support civic address information as defined by local MSAG(s) for a given region.

All modifications requests to data stored on the VDB shall be logged.

4.7.1.1 Data Management

The VDB database management shall allow for multiple agents to simultaneously perform database maintenance (data object creation, update, deletion).

The VDB shall support uploads of MSAG data from authorized sources.

The database structure shall be capable of supporting 24x7 real-time queries keyed to various elements of a civic address.

4.7.1.2 Data Management Authentication and Authorization

The VDB shall be able to authenticate the entities from which it receives source data for inclusion in the VDB.
Based on the credentials of the entity, the VDB shall control the entity's access to view, enter, and modify information in the VDB.

4.7.1.3 Data Integrity

The VDB database management shall enforce consistency of civic address information to MSAG format. (NOTE: This is even more critical since a postal address will be presented and it should be known at this time if the address can be formatted into a MSAG address since the ERDB will need to do this conversion when the call arrives at the VPC.).

The VDB shall maintain an audit trail of changes in the database

4.7.2 Perform Validation

The validation interface is described in Section 5.9.

The VDB shall be able to process and respond to VDB validation request messages.

The request shall use a standard message format that can be sent to any VDB (e.g. an XML message with the same elements) for any jurisdiction/region.

The elements/fields of the message shall align with NENA 02-010 data requirements, i.e. use already supported attribute names, when applicable.

Error responses shall be provided when validation fails.

Error response may contain suggestions for alternative address. The request could contain either postal or jurisdictional addresses but the response will return a postal address and may return a jurisdictional address.

Error responses shall provide information that enables a requestor to determine the type of error that occurred. When a VDB determines an address to be invalid, the VDB may return a URL that could be used to identify a resource that could provide additional helps and features in determining a valid location.

It is desirable that the VDB geo-code the validated address and return it in the response. The data needed to perform the geocoding should be approved by a public safety authority.

The VDB must be able to accept postal addresses and be able to return jurisdictionally accurate address information (including the correct community name and county for the 9-1-1 jurisdiction). The VDB must be able to accept a civic address (including the correct community name for the 9-1-1 jurisdiction) and be able to validate it. The VDB may also include postal address information (postal community and postal code) in the response. The VDB may support the option to include geo location information (latitude and longitude WGS84 coordinates) in the response to the location validation query.

The VDB shall provide a web services interface for civic address validation.

The VDB shall validate civic addresses submitted in the validateaddressRequest message against both the MSAG and, optionally, the country-specific Postal Service dataset.[7] If an address resolves

[7] All translations and searches done by the VDB to determine if an address is MSAG-valid must also be done by the ERDB when a call is being routed. This means that all data managed by the VDB

to one and only one MSAG entry, the address is considered to be valid. If the address resolves to zero MSAG entries or more than one MSAG entry, the address is considered to be invalid.

The VDB shall maintain translations from Postal Community Name to MSAG Community Name and vice-versa.

The VDB may maintain translations from Postal County Name to MSAG County ID.

The VDB shall maintain translations from the country-specific Postal Service abbreviations to MSAG abbreviations and vice-versa. MSAG abbreviations may differ among communities and counties.

The VDB shall ignore variations in upper and lower case to perform address searches (i.e. perform case-insensitive searches).

The VDB shall strip punctuation and translate non-standard abbreviations into standard country-specific Postal Service abbreviations before performing any database search (see Appendix B – Rules for Address Abbreviation).

The VDB may use a database or service based on postal service data to determine whether an address is a valid postal address. The postal service search may provide other helpful information to assist in the MSAG address validation (such as County Name).

The VDB may accept and parse into the appropriate fields malformed data such as HouseNum and StreetName entered into the same field or directionals embedded in the StreetName field before validating the submitted Address. The response will be a well-formed address (or addresses).

The VDB shall always returns pre/post directional and suffixes in the appropriate fields in the validateResponse message.

The VDB shall implement the V7 interface documented in Section 5.9.

If a submitted address cannot be automatically validated by the VDB, the VDB operator shall research these addresses and either create or update the appropriate Postal to MSAG translations. The VDB operator shall provide an email address (e.g., discrepancy@domain.com) that the LIS operator could use to send the unvalidated address to the VDB provider for further research. If the address still cannot be validated, the VDB shall return a more detailed explanation of why the address is invalid. Note: Resolution of discrepancies may require coordination with the appropriate ERDB providers and or MSAG Operators.

4.7.2.1 Authentication and Authorization of Validation Queries

The VDB may authenticate the entities from which it is allowed to receive validation queries.

must also reside in the ERDB and that any translations or data conversions done by the VDB must also be done by the ERDB.

Based on the credentials of the entity from which a query is received the VDB may restrict the ability of the entity to some validation queries e.g., it may be able to validate locations in some regions but not others.

4.7.2.2 Performance

The VDB shall be able to respond to a civic validation request within 500 ms.

The VDB shall be able to respond to at least 20000 validation requests per 1 hour.

4.7.3 Reliability and Availability

The VDB shall be available to support validation requests with an availability of 99.9%.

4.8 Location Information Server (LIS)

The LIS sits within or at the edge of the access network and invokes applicable positioning technologies enabling consistent and reliable location information to be attributable to an answerable source. It may support a simple request/response message that allows the VPC to obtain the location of a client without the client user identity being required. It may allow clients to request their location directly. The LIS must support at least one of the functions but it is recommended that the LIS support both functions. The LIS supports a location information credentialing system that provides assurances of the applicability, currency, and identity of the source of the location information. Precisely where a LIS resides in the network, how it determines location and the type of location (geo or civic) that it returns will be dependent on a number of factors, among these are:

- The nature of the connection used by the client. That is, whether it is a residential broadband connection, an enterprise IP switch connected client, a wireless client connecting via a campus wireless LAN, a client connecting to a wide area broadband wireless connection, etc.
- Legacy circumstances. That is, the extent to which the clients, access devices, and switches have native support for location delivery versus the need to overlay a solution for location determination on existing infrastructure.
- The type of location information and accuracy required for a given target environment. For example, are static civic addresses with sufficient geodetic accuracy for routing sufficient or is a more accurate geodetic location required in the absence of a civic address?

4.8.1 Detailed LIS Requirements

The LIS is a critical component in the support of emergency services for VoIP. The location of the caller is critical both in terms of routing the call to the correct emergency call centre and in terms of emergency service dispatch to the emergency. In providing location, however, there are a number of important attributes that should be associated with both the location information and the manner in which it is provided. These are summarized in the following list:

1. Where the client must be aware of the LIS, the LIS shall support consistent mechanisms by which it can be "discovered" by client devices in the access network in order that location information and location keys can be obtained.

2. When providing a client key or signed location, the LIS shall support an expiry mechanism by which it will delete its record of a client device within an agreed period of time unless it is renewed by the client[8].
3. The LIS shall support a mechanism by which location can be provided to a requesting client device in the served access using a standardized and open protocol such that all clients can assume a consistent mechanism
4. Location shall be coded in a standardized fashion such that systems and devices which utilize delivered location will be able to do so in a consistent fashion.
5. The location information shall be able to be provided with associated "credentials" to ensure the applicability of the location to the device.
    a. The credentials should reliably identify the source of the location (i.e. the LIS operational identity)
    b. The credentials should identify a unique client ID that the location is associated with.
    c. The credentials should identify a specific time after which the location should no longer be considered valid.
6. The LIS shall support a mechanism whereby a client provided location can be augmented with location credentials by the LIS if that client provided location can be determined by the LIS to be representative of the client's actual location (e.g. a more accurate client provided GPS fix may be provided with credentials if the LIS can confirm the location falls within known boundaries of the client's actual location)
7. The LIS shall support the delivery of a "Location Key" at the request of the client device, which can be used by the client or other network elements to query that client's location information directly from the LIS.
    a. The location key shall uniquely identify the LIS such that it can be queried over the IP network.
    b. The location key shall include a unique client ID which is associated with the client device which requests the key.
    c. The client ID and its uniqueness shall be meaningful only in the scope of the individual LIS
    d. The client ID will not be associable with the identity of the user of the device nor shall it indicate the physical identity of the device (e.g. it cannot be the MAC address).
8. The LIS shall support a standardized and open communications protocol to support the query of location information using a location key such that querying network elements can assume a consistent mechanism for doing so.
9. The LIS shall support encrypted communications between itself and the client device such that exchanges of location information and location keys remain private.
10. The LIS shall enforce authentication on querying network entities such that they must have permission to query the location of a device using a location key (e.g. the querying entity can present emergency service credentials).

[8] There is currently limited Standards support for signing location but it is expected that more support will available by the time the i2 solution is deployed.

11. The LIS shall support encrypted communications between itself and querying network elements such that exchanges of location information on client IDs remains concealed.
12. The LIS shall support a mechanism for validation of civic location information, refer to Section 5.9.
13. The LIS shall be able to support periodic revalidation of civic location information.

4.8.2 LIS Query Protocol and Location Information Format

In order for nomadic devices to be able to obtain information reliably and transparently regardless of the IP access network that they "roam" into, it is necessary that there be a consistent means of discovering and communicating with the LIS functional entity within the access network. To support roaming across national network boundaries, it should be possible for a single VoIP client implementation to determine location information in the same way regardless of the access network. To facilitate this requirement, it is recommended that LIS interaction be based on a specification from a global standards body. Given its specificity to IP access networks, a protocol specification from the IETF is recommended as being most appropriate.

The necessary functions for the LIS protocol to support are as follows:

- A discovery mechanism must be provided. This may be an explicit indication of the serving LIS entity identity provided, for example, by DHCP or DNS. Optionally, a broadcast and response message that allows a client device to find a LIS in the access network may be supported.

A direct query to the LIS to provide location is recommended.

4.9 ALI Database

This section provides functional requirements on the ALI DB that shall be implemented in support of the i2 solution.

The ALI database shall be configured with the following information associated with the ESQK:

- The associated VPC (including identifier/address and contact information)
- A new default VoIP Class of Service, designated as “V”
- A default Administrative ESN to be used to identify the appropriate English Language Translations for the emergency responders in the serving area identified by the ESQK.

The ALI database provider must support a V-E2 interface to the VPC and be able to use it to request and receive location information for VoIP emergency calls. The V-E2 interface is described in Section 5.8. The ALI database shall interpret the uses of data elements on the V-E2 interface as described in Section 5.8.

These procedures may differ from the processes that would be used to receive data from a wireless carrier’s Mobile Positioning Center (MPC).

The ALI DB shall include a NENA identifier for the VPC as the secondary Company (Data Provider) ID sent to the PSAP in the response to its ALI query, if this information is supported on the ALI to PSAP interface.

The ALI DB shall be capable of receiving both civic location and geo location over the V-E2 interface. The ALI DB shall deliver either civic or geo or both depending on the ALI-to-PSAP interface supported.

5 Detailed Interface Specifications

This section provides an overview of interfaces defined in this standard. This section is intended to give the reader a better understanding of what role each of the interfaces provides and also to provide the detailed specifications for the identified interfaces. Wherever possible, this document refers to existing standards defined elsewhere.

Each interface addresses a security mechanism to be used as part of the message exchange. If the interface is implemented over a public network, the security mechanisms described in Section 3, such as exchange of certificates and securing lower layers of the protocol must be implemented. If the interface is implemented over a private but shared network, the security mechanisms described in Section 3 should be implemented. If the network that joins the network elements is private, secured, and managed such that there is no reasonable possibility that anyone not specifically authorized to see E9-1-1 data (and specifically location data) has access to any systems on that network, it will not be required to deploy additional security measures described in Section 3.

The XML schema associated with the interfaces defined in this section can be found at the following location -

http://www.nena.org/xml_schemas/nena.htm

5.1 V0 – LIS to VoIP Endpoint

The V0 interface is the name given to the interface by which an end-device is informed or may request its location by an entity in the access network. At the time of writing several works are in progress for providing location to end-points using layer 2 mechanisms. These include, but are not limited to:

1. DHCP Geodetic information using RFC-3825[6]
2. DHCP Civic information using draft-ietf-geopriv-dhcp-civil-05[7].
3. LLDP-MED - TR41.4-05-02-014-L to be published as ANSI/TIA-1057

The client-device will need to make some request to the network to obtain location information and format the information into a PIDF-LO.

There are proposals to address Layer 3/Layer 7 mechanisms for direct delivery of location formatted as PIDF-LO to the VoIP end point. A strong motivation for considering Layer 3/Layer 7 mechanisms is to meet the need of a significant portion of access service providers that are not able to use the Layer 2 mechanisms described above.

The detailed specification of this interface is out of scope for the i2 solution.

5.2 V1 – VoIP endpoint to Call Server

The V1 interface represents the link between the client-device and a call server. It is over this link the user establishes a call, and conveys location information. Location conveyance in call establishment is being developed in the wider VoIP community. At present the most advanced work is in the IETF and deals with location conveyance over SIP, draft-ietf-sipping-location-

requirements-02[12]. It is a recommendation of the i2 architecture that the V1 interface be capable of transporting either location or location key information regardless of the protocol being used to support the voice service. If the end point and the VSP are unable to provide a location or a location key, calls might not get routed to the appropriate PSAP. In the case of call servers closely associated with the access network, the call server may be able to obtain this information directly from the LIS. The i2 architecture does not identify an interface for this nor any recommendations for how it may be done.

This interface is out of scope for the i2 solution.

5.3 V2 – Call Server/Routing Proxy/Redirect Server to VPC

Since the VPC is considered to be part of the emergency service network, the V2 interface is specified in this document.

This section describes the VoIP E9-1-1 i2 migration standard for the V2 interface between the VoIP Call-Server/Proxy and the VPC as shown in Figure 2-1. This interface provides a means for the Call-Server to request emergency services routing information from the VPC, and to inform the VPC, at call termination, when a routing/query key is no longer required. The interface consists of four messages and these are introduced in subsequent paragraphs. The V2 interface is XML-based.
The V2 interface is likely to need to operate in a variety of network environments, some trusted, and some not. It for this reason that the HTTPS protocol using webservices has been selected as the transport mechanism for the V2 interface, as this provides strong security mechanisms and readily able to traverse enterprise and commercial firewalls when correctly configure.

5.3.1 Message Definitions

There are two sets of Request/Response messages (for a total of 4 messages). The first message set requests and receives routing instructions. The second message set indicates that an emergency call has concluded. The remainder of Section 5.3.1 details the 4 messages that make up communication across the V2 interface.

5.3.1.1 Emergency Services Routing Request (ESRRequest)

The ESRRequest message is sent from the query node (Call-Server/Routing Proxy/Redirect Proxy) to the VPC to request a routing and query key pair. The valid parameters for the ESRRequest message are included in the following table.

Table 5-1 - ESRRequest Parameters

Parameter	Condition	Description
source	Mandatory	The identifier of the node requesting routing information directly from the VPC.
vsp	Conditional	The identifier of the caller's voice service provider

call-id*	Mandatory	Any identifier that can be used to uniquely identify the call at the requesting node
datetimestamp	Optional	Date Time Stamp indicating UTC date and time that the message was sent
callback*	Conditional	E.164 number that can be dialed by a PSAP operator to reach the call originator
lie	Mandatory	The Location Information Element.
call-origin	Optional	An ID inserted by the originating network that allows LIS to validate if the call is originating network.
vpc	Optional	The identifier of the destination VPC.

* In some cases the <*callback*> number will uniquely identify the call at the Call-Server. In such a case, the <*call-id*> parameter will contain the value of the <*callback*> number parameter. There is no formal requirement that this be the case however, and only the value contained in the <callback> parameter shall be used to deliver the callback number over the V-E2 interface.

The <*source*> element identifies the node directly requesting emergency call routing from the VPC over the V2 interface. It includes the source node (hostname), a NENA administered identifier (nena-id) a 24x7 contact number (contact), and an optional uri (cert-uri) provide a link to the provider's VESA issued certificate. The <*source*> must be a trusted entity of the VPC.
source format:

```
<source>
        <organization-name>James's cool VSP</organization-name>
        <hostname>cs34.example.com</hostname>
        <nena-id>nena1</nena-id>
        <contact>tel:+398348975439823</contact>
        <cert-uri>https://cs34.example.com/certificate.crt</cert-uri>
</source>
```

The <organization-name> is a free form text field into which the node owner may place their company name or other label. This field is optional.
The <hostname> identifies the fully qualified domain name of the directly requesting node. This field is optional
The <nena-id> is the NENA administered company identifier (NENA Company ID) of the node requesting routing information over the V2 interface. This field is mandatory
The <contact> is a telephone number by which the directly requesting node operator can be reached 24 hours a day, 7 days a week. This field is mandatory.

The <cert-uri> provides a means of directly obtaining the VESA issued certificate for the requesting node. This field is optional

The <*vsp*> *element* identifies the Voice Service Provider for the call. This element is used to identify the original voice service provider, in cases where the original VSP is not the same entity as the one requesting routing information over the V2 interface. In cases where the voice service provider and the entity requesting routing information are not the same, the source element is used to identify the entity requesting routing information over the V2 interface and the vsp element is used to identify the voice service provider.

```
<vsp>
        <organization-name>Martin's super VSP</organization-name>
        <hostname>cs34.example.com</hostname>
        <nena-id>nena1</nena-id>
        <contact>tel:+398348975439823</contact>
        <cert-uri>https://cs34.example.com/certificate.crt</cert-uri>
</vsp>
```

At least the <hostname> and/or the <nena-id> MUST be provided. The <organization-name>, <contact> and <cert-uri> fields are optional.

The <*call-id*> element is an identifier that can be used to uniquely identifier the call at the Call-Server.
<call-id>767673678674835784587</call-id>

The <*callback*> number is a tel-uri of the format “tel: +1-212-691-8215”. This identifies the E.164 number that can be dialed to reach the caller. This is the number that will be included in the callback number field in the ESPOSREQ response message to the ALI.

The <*lie*> is the Location Information Element. This element contains location information that is used to determine the routing and query keys to be used for the call. This parameter is MANDATORY, and if not provided, the VPC MUST providing default routing or an error to the requesting node. If the <*lie*> is present in the ESRRequest, then it may contain a LocationKey, a PIDF-LO (geodetic and or Civic), or both. The exact mechanism used to determine the routing and query keys is dependent on the contents of the <*lie*>.

```
<lie>
        <location-key> 3c01abe092@lis.example.com </location-key>
        <presence xmlns="urn:ietf:params:xml:ns:pidf"
                xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
                xmlns:gml="urn:opengis:specification:gml:schema-xsd:feature:v3.0"
                entity="3c01abe092@lis.example.com">
                <tuple id="sg89ab">
                        <status>
                                <gp:geopriv>
```

```
                    <gp:location-info>
                <gml:position>
                    <gml:Point gml:id="point1" srsName="epsg:4326">
                        <gml:pos>37.775 -122.422</gml:pos>
                    </gml:Point>
                </gml:position>
                <cl:civilAddress>
                    <cl:country>US</cl:country>
                    <cl:FLR>2</cl:FLR>
                </cl:civilAddress>
              </gp:location-info>
              <gp:usage-rules>
              </gp:usage-rules>
            </gp:geopriv>
          </status>
         <timestamp>2003-06-22T20:57:29Z</timestamp>
        </tuple>
      </presence>
</lie>
```

The LIE example above shows both Geo Location and Civic address information, which is acceptable, but in most cases it is expected that either Geo Location or Civic Location would be sent in the LIE.

The <*call-origin*> parameter is used by the VPC when it sends a LocationKey to the LIS over the V3 interface. The LIS is able to use this parameter to determine if the LocationKey received belongs to the originating network. Use of this parameter is LIS implementation specific and is subject to local access network policy.

The <*datetimestamp*> is the date time stamp in UTC time indicating the time that the message was sent from the requesting node. This field is optional, but if not included, then the VPC must maintain an accurate date and time stamp in any call event records so that an audit trail is readily accessible.
<datetimestamp>**2004-12-12T21:28:43+10:00**<datetimestamp>

The <*vpc*> *element* identifies the VPC from which routing information is being requested.

```
<vpc>
        <organization-name>Martin's super VPC</organization-name>
        <hostname>cs34.example.com</hostname>
        <nena-id>nena1</nena-id>
        <contact>tel:+398348975439823</contact>
        <cert-uri>https://cs34.example.com/certificate.crt</cert-uri>
</vpc>
```

The coding of the VPC is element is the same as the coding for the source element.

5.3.1.1.1 LIE PIDF-LO Routing

When the LIE contains a PIDF Location Object (PIDF-LO), the VPC will perform a lookup in the ERDB, to obtain the routing key (ESRN), an ESN, and a contingency routing number (CRN) for the PSAP. Using the ESRN and ESN the VPC can identify and allocate an ESQK. The ESRN, ESQK, and CRN are subsequently returned to the Call-Server in an ESRResponse message, with the CRN being carried to the Call-Server as an LRO.

5.3.1.1.2 LIE LocationKey Routing

The LocationKey provides information to the VPC on where to get the location of the caller. The LocationKey may explicitly indicate a client-id and a LIS, say in the form or a URI, or it may be a different form of identifier, such as callback number, that the VPC can use internally to determine a LIS and subsequently request a location object. Having determined the LIS from the LocationKey, the VPC then passes the LIE to the LIS and receives a LIE back, this time containing the original LocationKey and a PIDF-LO. The VPC is then able to route based on the PIDF-LO as it did in the Section 5.3.1.1.1.

5.3.1.1.3 ESRRequest Message Format

The high-level message format for the ESRRequest message is shown below:

```
<esr-request xmlns="urn:nena:xml:ns:es:v2"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:nena:xml:ns:es:v2 v2.xsd">
      <vpc>
            <organization-name>Anand's VPC</organization-name>
            <hostname>vpc.example.com</hostname>
      </vpc>
      <source>
            <organization-name>Terry's re-direct proxy</organization-name>
            <hostname>rp34.example.com</hostname>
            <nena-id>nena1</nena-id>
            <contact>tel:+398348975439823</contact>
            <cert-uri>https://rp34.example.com/certificate.crt</cert-uri>
      </source>
      <vsp>
            <organization-name>Nadine's Call-Server</organization-name>
            <hostname>cs98.example.com</hostname>
            <nena-id>nena2</nena-id>
            <contact>tel:+15554476632</contact>
            <cert-uri>https://cs98.example.com/certificate.crt</cert-uri>
      </vsp>
      <call-id>610239946019573</call-id>
      <callback>610239946019573</callback>
      <lie>
            <location-key>3c01abe092@lis.example.com</location-key>
            <presence xmlns="urn:ietf:params:xml:ns:pidf"
                              xmlns:pidf="urn:ietf:params:xml:ns:pidf"
                              xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
                              xmlns:gml="http://opengis.net/gml"
entity="pres:user@example.com">
                  <tuple id="a6fea09">
```

```
                        <status>
                              <gp:geopriv>
                                    <gp:location-info>
                                          <gml:position>
                                                <gml:Point gml:id="point1"
srsName="epsg:4326">
                                                      <gml:pos>42.5463 -
73.2512</gml:pos>
                                                </gml:Point>
                                          </gml:position>
                                    </gp:location-info>
                              <gp:usage-rules />
                              </gp:geopriv>
                  </status>
                  <timestamp>2004-12-01T09:28:43+10:00</timestamp>
                  </tuple>
            </presence>
      </lie>
 <call-origin>Some arbitrary string in here</call-origin>
      <datetimestamp>2004-12-12T21:28:43+10:00</datetimestamp>
</esr-request>
```

5.3.1.2 Emergency Services Routing Response (ESRResponse)

The ESRResponse message is sent by the VPC to a routing entity (Call-Server/Routing Proxy/Redirect Server) in response to an ESRRequest message. Valid parameters for the ESRResponse message are contained in the following table.

Table 5-2 - ESRResponse Parameters

Parameter	Condition	Description
vpc	Mandatory	The identifier of the responding VPC
call-id	Mandatory	An identifier that uniquely identifies the call at the Call-Server
esrn	Conditional	The Routing Key determined by the VPC to

		allow routing of the call to the Selective Router servicing the local area in which the call was made.
esqk	Conditional	The Query Key allocated by the VPC to uniquely identify the call within ESZ
lro	Conditional	The last routing option. This routing option should only be used by the call-server or proxy as a last resort. The actually meaning of the LRO is different depending on what other information is returned in response to the query.
result	Mandatory	Code indicating the reason for success of failure to determine a n ESRN and ESQK. See the next table for mode details.
datetimestamp	Optional	Date Time Stamp indicating UTC date and time that the message was sent.
destination	Optional	The identifier of the routing node immediately adjacent to the VPC.

The <*vpc*> *element* identifies the VPC.

```
<vpc>
      <organization-name>National VPC Services</organization-name>
      <hostname>vpc34.example.com</hostname>
      <nena-id>nena1</nena-id>
      <contact>tel:+398348975439823</contact>
      <cert-uri>https://vpc34.example.com/certificate.crt</cert-uri>
</vpc>
```

The <nena-id> and <contact> fields are mandatory while the other fields of the <vpc> element are optional.

The <*destination*> element identifies the node that directly requested emergency call routing information from the VPC. It includes the source node (hostname), a NENA administered Company ID identifier (NENA Company ID) a 24x7 contact number (contact), and optional parameters for the organization's name and uri (cert-uri) for the operator's VESA issued certificate. The <*destination*> must be a trusted entity of the VPC.
Destination format:

```
<destination>
      <organization-name>Generic Redirect Proxys</organization-name>
      <hostname>rp34.example.com</hostname>
      <nena-id>nena1</nena-id>
      <contact>tel:+398348975439823</contact>
      <cert-uri>https://rp34.example.com/certificate.crt</cert-uri>
</destination>
```

The <organization-name> is a free form text field into which the node owner may place their company name or other label. This field is optional.
The <hostname> identifies the fully qualified domain name of the directly requesting node, either this, or the <nena-id> MUST be provided.
The <nena-id> is the NENA administered company identifier (NENA Company ID), either this, or the <hostname> MUST be provided.

The <*call-id*> is an identifier that uniquely identifies the call at the requesting node.

The <*esrn*> is the ESRN determined by the ERDB to correspond to the emergency service zone (ESZ) belonging to the PSAP. A valid value must be returned in this field for the call to be successfully routed. An <*esrn*> MUST only be provided if a corresponding <*esqk*> is provided. The format of the <esrn> is expected to be a 10-digt North American Numbering Plan Number.

The <*esqk*> is the ESQK allocated by the VPC. This key identifies an ESN for a specific PSAP, as well as the call instance at the VPC. A valid value must be returned in this field for the call to be successfully routed to correct PSAP, and for location information to be supplied from the VPC to the PSAP. A <*esqk*> MUST only be provided if a corresponding <*esrn*> is also provided. The <esqk> is expected to be a 10-digit North American Numbering Plan Number.

The <*lro*> last routing option provides the routing node with a "last chance" destination for the call. The LRO may be the Contingency Routing Number (CRN) which is a 24x7 PSAP emergency number, or it may be a national or default call centre, the service type will depend on the condition that resulted in the providing of the LRO. Ultimately the usage of LRO routing data for call delivery is down to decisions made internally to the routing node. There may be occasions when the VPC only returns an LRO, examples of this may be invalid or unavailable location information, VPC resource limitations, or the invoking of local PSAP routing policies. When primary routing options fail, and no LRO is provided the routing node is required to provide specific default handling, which may include dropping the call.
The <*result*> indicates to the routing node whether or not the VPC was able to provide routing information and the means by which the routing data was determined, alternatively if no routing

information could be provided the source of the problem. The <*result*> therefore provides a means by which the Voice Service Provider can monitor the quality of the routing information provided by a VPC operator. A complete list of valid <*result*> codes is detailed in Table 5-3 - Result Codes. Both the value and the name of the code are expected to be sent in the in this element (e.g., 200 SuccessGeodetic).

The <*datetimestamp*> is the date time stamp in UTC time indicating the time that the message was sent from the VPC. This field is optional, but if not included, then the routing node must maintain an accurate date and time stamp in any call event records so that an audit trail is readily accessible.

Table 5-3 - Result Codes

Value	Name	Description
200	SuccessGeodetic	VPC has successfully determined the routing information based on geodetic information contained in the initial ESRRequest
201	SuccessLISGeodetic	VPC has successfully determined the routing information based on geodetic information obtained from the LIS.
202	SuccessCivic	VPC has successfully determined the routing information based on civic information contained in the initial ESRRequest
203	SuccessLISCivic	VPC has successfully determined routing information based on civic information obtained from the LIS
400	LROBadLocation	No *ESRN* can be determined from the location provided in the LIE. This may be because the LIE is malformed, or because the location does not map to a provisioned PSAP boundary. LRO is provided, but this is really default routing.
401	LRONoLIS	The VPC is unable to determine the LIS from which to get the location. An LRO is returned.
402	LRONoLocation	The VPC was unable to get a location for the client from the LIS. An LRO is returned.
403	LROBadMessage	The ESRRequest received by the VPC could not be parsed or was malformed. An LRO is returned
404	LRONoAuthorization	The requesting node's ESRRequest message failed authorization at the VPC. An LRO is provided.

Value	Name	Description
405	ErrorBadLocation	VPC was unable to get routing information based on the sourced location. VPC is unable to provide an LRO for routing.
406	ErrorNoLIS	VPC was unable to determine the LIS based on a provided locationkey. VPC is unable to provide an LRO for routing.
407	ErrorNoLocation	The VPC is unable to get a location from the LIS for the locationkey provided. VPC is unable to provide an LRO for routing.
408	ErrorBadMessage	The ESRRequest received by the VPC could not be parsed or was malformed. VPC is unable to provide an LRO for routing.
409	ErrorAuthorization	The requesting node's ESRRequest message failed authorization at the VPC. VPC is unable to provide an LRO for routing.
500	LRONoResource	VPC was unable to allocate an ESQK and an LRO is provided to enable default routing
501	LROGeneralError	A general error is encountered and the VPC provides a LRO to enable default routing
502	ErrorNoResource	The VPC is unable to allocate an ESQK, and no CRN was provided from the ERDB. VPC is unable to provide an LRO for routing.
503	ErrorGeneral	Any error cause that is not listed above. VPC is unable to provide an LRO for routing.

5.3.1.2.1 ESRResponse Message Format

The following is an ESRResponse message showing a successful response (result = 200). The message contains valid <*ersn*>, <*esqk*> and <*lro*> values.

```
<esr-response xmlns="urn:nena:xml:ns:es:v2"
    xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
    xsi:schemaLocation="urn:nena:xml:ns:es:v2 v2.xsd">
    <result>200</result>
    <vpc>
        <organization-name>Right first time VPC</organization-name>
            <hostname>vpc.example.com</hostname>
            <nena-id>nena1</nena-id>
            <contact>tel:+398348975439823</contact>
            <cert-uri>https://vpc.example.com/certificate.crt</cert-uri>
    </vpc>
    <destination>
            <organization-name>James's Call-Server</organization-name>
```

```
            <hostname>cs34.example.com</hostname>
            <nena-id>nena1</nena-id>
            <contact>tel:+398348975439823</contact>
            <cert-uri>https://cs34.example.com/certificate.crt</cert-uri>
    </destination>
    <call-id>610239946019573</call-id>
    <esrn>b57fd957a059c5a027b5</esrn>
    <esqk>469327927621542</esqk>
    <lro>tel:+160910920672398</lro>
    <datetimestamp>2004-12-12T21:28:53+10:00</datetimestamp>
</esr-response>
```

5.3.1.3 Emergency Services Call Termination Message (ESCT)

The ESCT message is sent from the routing node to the VPC at the conclusion of the emergency call. The intent of this message is to return the <*esqk*> associated with the call back to the pool of available query keys for use by the VPC, and to inform the VPC as to which ESGW was used to direct the call to the Selective Router. The valid parameters for the ESCT message are included in the following table.

Table 5-4 - ESCT Parameters

Parameter	Condition	Description
source	Mandatory	The identifier of the routing node directly adjacent to the VPC
esqk	Conditional	The ESQK to return to the VPC pool
esgw	Conditional	The identifier of the ESGW used to direct the call to the selective router
datetimestamp	Optional	Date Time Stamp indicating UTC date and time that the message was sent
call-id	Mandatory	The identifier that uniquely identified the call at the Call-Server
vpc	Optional	The identifier of the VPC.

The <*source*> element identifies the node directly requesting emergency call routing from the VPC. It includes the source node (hostname), a NENA administered company identifier (nena-id) a 24x7 contact number (contact), and an optional uri (cert-uri) provide a link to the provider's VESA issued certificate. The <*source*> must be a trusted entity of the VPC.
Source format:

```
<source>
      <organization-name>CS-2K</organization-name>
      <hostname>cs34.example.com</hostname>
```

```
        <nena-id>nena1</nena-id>
        <contact>tel:+398348975439823</contact>
        <cert-uri>https://cs34.example.com/certificate.crt</cert-uri>
</source
```

The <organization-name> is a free form text field into which the node owner may place their company name or other label. This field is optional.
The <hostname> identifies the fully qualified domain name of the directly requesting node, this field is optional.
The <nena-id> is the NENA administered company identifier (NENA Company ID), this field is mandatory.
The <contact> is a telephone number by which the directly requesting node operator can be reached 24 hours a day, 7 days a week.
The <cert-uri> provides a means of directly obtaining the VESA issued certificate for the requesting node.

The <*vpc*> *element* identifies the VPC.

```
<vpc>
        <organization-name>South-West VPC</organization-name>
        <hostname>vpc34.example.com</hostname>
        <nena-id>nena1</nena-id>
        <contact>tel:+398348975439823</contact>
        <cert-uri>https://vpc34.example.com/certificate.crt</cert-uri>
</vpc>
```

At least the <hostname> and/or the <nena-id> MUST be provided. The <contact>, <organization-name> and <cert-uri> fields are optional.

The <*esqk*> is the ESQK that was allocated by the VPC for the call. This is the ESQK that can now be returned to the pool of ESQKs available for use by the VPC.

The <*esgw*> is the identifier for the ESGW that was used to direct to the call to the selective router. If LRO was used to route the call then element MUST not be present in the ESCT message. The <esgw> is expected to be in the form of an uri.

The <*call-id*> is the identifier that uniquely identifies the call at the querying node.
The <datetimestamp> is the date time stamp in UTC time indicating the time that the message was sent from the routing node. This field is optional, but if not included, then the VPC must maintain an accurate date and time stamp in any call event records so that an audit trail is readily accessible.

5.3.1.3.1 ESCT Message Format

The format for the ESCT message is defined below:

```
<esct xmlns="urn:nena:xml:ns:es:v2"
                xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
                xsi:schemaLocation="urn:nena:xml:ns:es:v2 v2.xsd">
```

```
<vpc>
        <organization-name>James's VPC</organization-name>
        <hostname>vpc.example.com</hostname>
</vpc>
<source>
        <organization-name>National Call-Servers</organization-name>
        <hostname>cs34.example.com</hostname>
        <nena-id>nena1</nena-id>
        <contact>tel:+398348975439823</contact>
        <cert-uri>https://cs34.example.com/certificate.crt</cert-uri>
</provider>
<esgw>
        <organization-name>Richardson Texas ESGW-1</organization-name>
        <hostname>esgw4.example.com</hostname>
        <nena-id>nena4</nena-id>
        <contact> tel:+927-555-5555</contact>
</esgw>
<esqk>123456789456123</esqk>
<call-id>sips:123456789456123@cs34.example.com</call-id>
<datetimestamp>2004-12-14T09:44:39+10:00</datetimestamp>
</esct>
```

ESCTAck message is sent from the VPC to the routing entity (call server/routing proxy/redirect proxy) in response to an ESCT message. The valid parameters for the ESCTAck message are contained in the following table.

Table 5-5 ESCTAck Message Parameters

Parameter	Condition	Description
call-id	Mandatory	Identifies the call at the routing element
vpc	Mandatory	The identifier of the VPC.
datetimestamp	Optional	Date Time Stamp indicating UTC date and time that the message was sent

The <*call-id*> is the identifier that uniquely identifies the call at the routing element.

The <*vpc*> *element* identifies the VPC.

```
<vpc>
        <organization-name>Monster VPC</organization-name>
        <hostname>vpc34.example.com</hostname>
        <nena-id>nena1</nena-id>
        <contact>tel:+398348975439823</contact>
        <cert-uri>https://vpc34.example.com/certificate.crt</cert-uri>
</vpc>
```

At least the <hostname> and/or the <nena-id> MUST be provided. The <contact>, <organization-name> and <cert-uri> fields are optional.

The <*datetimestamp*> is the date time stamp in UTC time indicating the time that the message was sent from the VPC. This field is optional, but if not included, then the routing node must maintain an accurate date and time stamp in any call event records so that an audit trail is readily accessible.

5.3.1.3.2 ESCTAck Message Format

```
<esct-ack xmlns="urn:nena:xml:ns:es:v2"
                        xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
                        xsi:schemaLocation="urn:nena:xml:ns:es:v2 v2.xsd">
                        <vpc>
                                <organization-name>Monst VPC</organization-name>
                                <hostname>vpc.example.com</hostname>
                                <nena-id>nena1</nena-id>
                                <contact>tel:+398348975439823</contact>
                                <cert-uri>https://vpc.example.com/certificate.crt</cert-uri>
                        </vpc>
                        <datetimestamp>2004-12-14T10:11:06+10:00</datetimestamp>
</esct-ack>
```

5.3.2 Call Flows, Key Scenarios and Semantics

Section 5.3.1 described in detail the 4 messages that make up communication across the V2 interface. This section will describe the key call scenarios and show the message flows between the various network elements.

5.3.2.1 ESRRequest contains valid Location

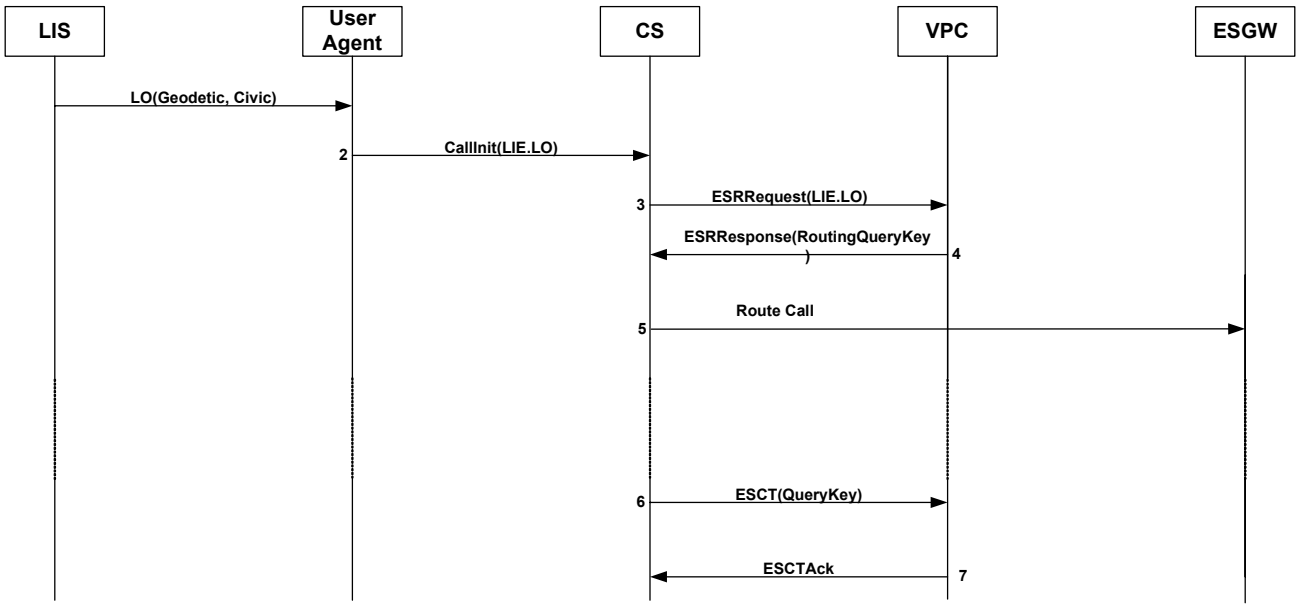


Figure 5-1 PIDF-LO Routing

1. The LIS provides PIDF-LO containing geodetic and or civic information to the User Agent.
2. The UA initiates an emergency call to the Call-Server and includes the PIDF-LO in the call initiation message.
3. The Call-Server allocates the UA a callback number, and constructs an ESRRequest message containing the Call-ID, callback number, and LIE containing the PIDF-LO. The Call-Server sends the ESRRequest message to the VPC.
4. The VPC receives the ESRRequest from the Call-Server and authenticates the Call-Server. The VPC uses the location contained in the PIDF-LO to determine an ESRN and LRO. The VPC allocates an ESQK. The VPC constructs an ESRResponse message containing the ESRN, ESQK, and LRO and returns this to the Call-Server.
5. The Call-Server uses the returned ESRN to determine the correct ESGW and subsequently routes the call.
6. The Call-Server detects that call has concluded, and that the ESQK is no longer required. The Call-Server sends an ESCT message containing the ESQK and ESGW identifier to the VPC.
7. The VPC accepts the ESCT message, authenticates the Call-Server, returns the ESQK to the pool of available keys, and notes the ESGW in its call event records. The VPC sends an ESCTAck message to the Call-Server

5.3.2.2 ESRRequest contains a LocationKey

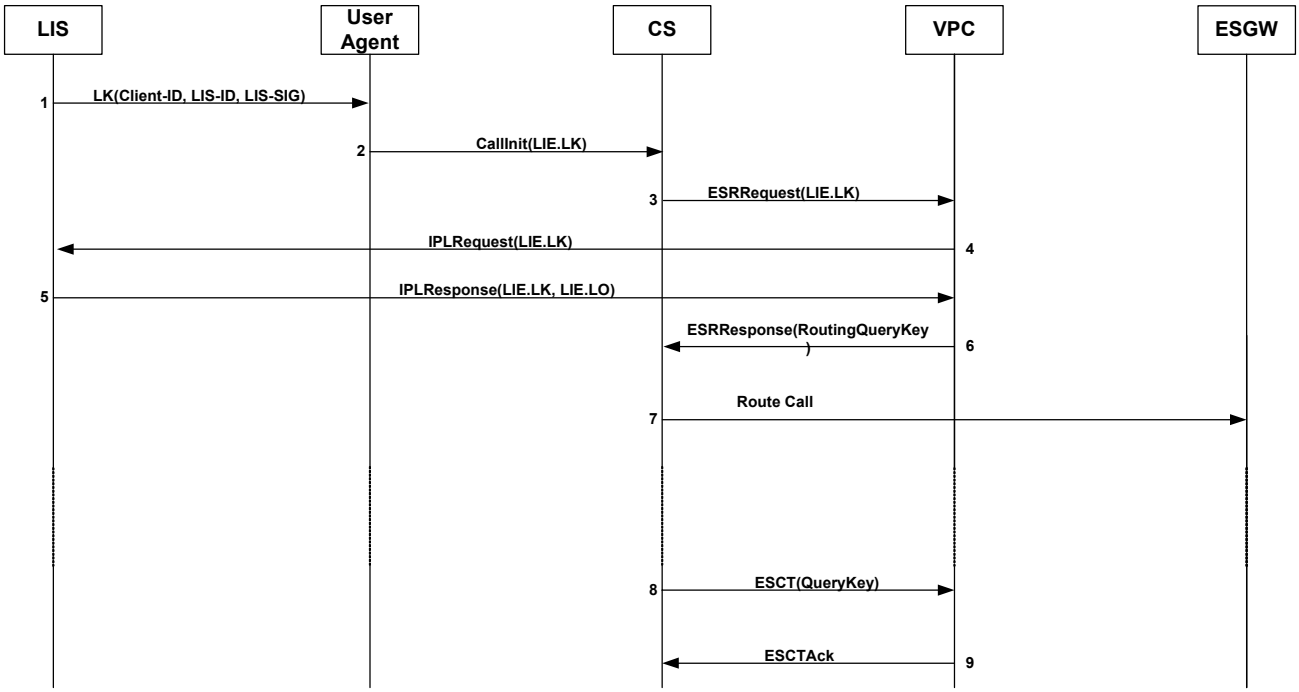


Figure 5-2 LocationKey Routing

1. The LIS provides a LocationKey containing a Client-ID, and LIS-ID to the User Agent. The locationkey may explicitly identifier a client and LIS, or it may contain a value that implies these identities to the VPC. Regardless of the actual implementation, the locationkey provides sufficient information to enable to the VPC to request the location of a UA.
2. The UA initiates an emergency call to the Call-Server and includes the LocationKey in a LIE which is sent with the call initiation message.
3. The Call-Server allocates the UA a callback number, and constructs an ESRRequest message containing the Call-ID, callback number, and LIE. The Call-Server sends the ESRRequest message to the VPC.
4. The VPC receives the ESRRequest from the Call-Server and authenticates the Call-Server. The VPC uses the LIS-ID to send the LIE to the LIS, and request a LocationObject.
5. The LIS authenticates and VPC and validates the LocationKey. The LIS returns a LIE to the VPC containing a valid PIDF-LO.
6. The VPC uses the location returned by the LIS to request an ESRN and LRO. The VPC allocates an ESQK. The VPC constructs an ESRResponse message containing the ESRN, ESQK, and LRO and returns this to the Call-Server.
7. The Call-Server uses the returned ESRN to determine the correct ESGW and subsequently routes the call.

8. The Call-Server detects that call has concluded, and that the ESQK is no longer required. The Call-Server sends an ESCT message containing the ESQK and ESGW identifier to the VPC.
9. The VPC accepts the ESCT message, authenticates the Call-Server, returns the ESQK to the pool of available keys, and notes the ESGW identifier in the call event records. The VPC sends an ESCTAck message to the Call-Server

5.3.2.3 VPC returns an Error

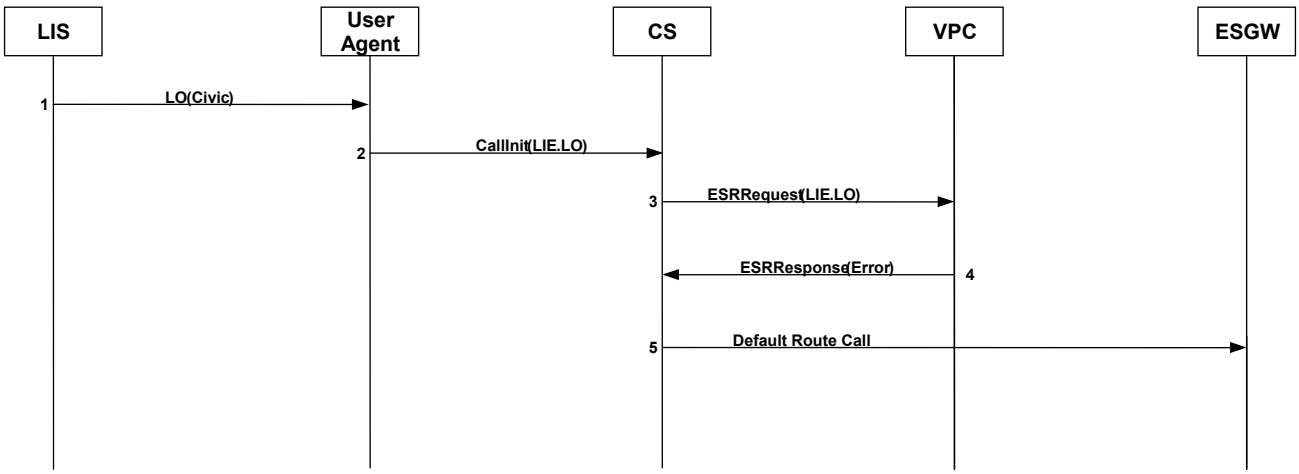


Figure 5-3 Routing Error

1. The LIS provides a PIDF-LO containing Civic address information to the User Agent.
2. The UA initiates an emergency call to the Call-Server and includes the PIDF-LO in the call initiation message.
3. The Call-Server allocates the UA a callback number, and constructs an ESRRequest message containing the Call-ID, callback number, and a LIE containing the PIDF-LO. The Call-Server sends the ESRRequest message to the VPC.
4. The VPC receives the ESRRequest from the Call-Server and authenticates the Call-Server. The VPC is unable to determine routing based on the location so returns an error in the ESRResponse to the Call-Server with no LRO.
5. The Call-Server detects the error and performs its default routing behavior in this situation, which may be to send the call to a default PSAP, or it may drop the call.

5.3.3 V2 Interface Security

The V2 interface will need to operate in a variety of network environments, some trusted, and some not as described in previously. V2 is a XML-based interface and should be used with a suitable security mechanism as defined in Section 3. When the connection between the routing entity and the VPC is not a trusted network, both the routing entity and VPC are expected to be protected with IPSEC or TLS, and thus require a certificates rooted in VESA. Even in a trusted network, TLS protection is advisable. The VPC is the server, and the routing entity is the client in this interface. Mutual authentication is required when cryptographic security is deployed.

5.4 V3 – VPC to LIS

This section describes the VoIP E911 i2 migration standard for the V3 interface between the VPC and LIS. This interface provides a means for the VPC to request VEP location information from the LIS for the purposes of determining call routing information, and location updates for mobile users. The interface consists of two messages and these are introduced in subsequent paragraphs. The V3 interface is XML-based.

5.4.1 Message Definitions

The V3 interface is made up of a query response message pair. The first message is sent from the VPC to the LIS requesting location information for a specific client. The second message is sent from the LIS to the VPC in response to this request. The remainder of section 5.4.1.1 details the 2 messages that make up communication across the V3 interface.

5.4.1.1 IP Provide Location Request (IPLRequest)

The IPLRequest message is sent from the VPC to the LIS to request the location of a UA. The valid parameters for the IPLRequest message are shown in Table 5-6.

Table 5-6 IPLRequest message parameters

Parameter	Condition	Description
vpc	Mandatory	The identifier of the VPC
lie	Mandatory	The Location Information Element containing the LocationKey.
CallOrigin	Optional	ID of the call originator
datetimestamp	Optional	Date Time Stamp indicating UTC date and time that the message was sent
message-id	Mandatory	Used to uniquely identify a message

The <*vpc*> *element* identifies the VPC.

```
<vpc>
      <organization-name>National VPC Services</organization-name>
      <hostname>vpc34.example.com</hostname>
      <nena-id>nena1</nena-id>
      <contact>tel:+398348975439823</contact>
      <cert-uri>https://vpc34.example.com/certificate.crt</cert-uri>
</vpc>
```

All fields in the <*vpc*> element are expected to be populated with the exception of <organization-name> which is optional.

The *lie* contains the LocationKey. The LocationKey identifies the VEP allowing the LIS to lookup the location of the VEP.

```
<lie>
      <location-key> 3c01abe092@lis.example.com </location-key>
<lie>
```

The *CallOrigin* parameter may be used the LIS to determine if the LocationKey belongs to the UA that originated the request. Usage of this field is implementation dependent, if the field is included in the V2 request then it should be populated to the V3 request also.

The *datetimestamp* is the date time stamp in UTC time indicating the time that the message was sent from the VPC. This field is optional, but if not included, then the LIS must maintain an accurate date and time stamp in any location event records so that an audit trail is readily accessible.

The *message-id* field is used to correlate the query with the response. The IPLResponse message will include a Message-ID element with the same integer value as it received. This element is useful when a persistent connection is supported by the VPC to keep track of outstanding responses. The field is defined to be an integer that supports up to 6 digits, value 0-999999.

5.4.1.1.1 IPLRequest Message Format

The high-level message format for the IPLRequest message is shown below:

```
<?xml version="1.0" ?>
<ipl-request xmlns="urn:nena:xml:ns:es:v3"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:nena:xml:ns:es:v3 v3.xsd">
      <message-id>209344</message-id>
      <vpc>
            <hostname>vpc.example.com</hostname>
            <nena-id>nena1</nena-id>
            <contact>tel:+398348975439823</contact>
            <cert-uri>https://vpc.example.com/certificate.crt</cert-uri>
      </vpc>
      <lie>
            <location-key>pres:3c01abe092@lis.example.com</location-key>
      </lie>
      <call-origin>SIP/2.0/UDP
      cs34.example.com;branch=z9hG4bK776asdhds</call-origin>
      <datetimestamp>2004-12-12T21:28:43+10:00</datetimestamp>
```

```
</ipl-request>
```

5.4.1.2 IP Provide Location Response (IPLResponse)

The IPLResponse message is sent by the LIS to theVPC in response to an IPLRequest message. Valid parameters for the IPLResponse message are contained in the following table.

Table 5-7 IPLResponse message parameters

Parameter	Condition	Description
lis	Mandatory	The identifier of the responding LIS
lie	Mandatory	Location Information element containing a LocationKey and if successful a PIDF-LO.
result	Mandatory	Indicates the result of the location request. See Table 5-8 for more details.
datetimestamp	Optional	Date Time Stamp indicating UTC date and time that the message was sent.
message-id	Mandatory	Used to uniquely identify a message

Table 5-8 IPLResponse ResultCodes

Value	Name	Description
200	SuccessLISLocation	LIS returns a Civic address, Geodetic location or both
400	ErrorLISNoLoc	The LIS is unable to determine a location for the client. In this case the LIS should return a generic location that can be used to provide default routing.
401	ErrorLISUnkownClient	The LIS does not recognize the provided Client-ID. In this case the LIS should return a generic location that can be used to provide default routing.

402	ErrorLISStaleClient	The LocationKey provided to the LIS is old. In this case the LIS should return the last known location
403	ErrorLISFraud	The LocationKey provided to the LIS did not originate from the UA to whom the key was assigned. . No location is provided
404	ErrorLISGeneral	Any error cause that is not listed above and the LIS can provides a generic location that can be used to provide default routing.
500	ErrorLISInternal	Any error cause that is not listed above and the LIS does not provide location.

The <*lis* element identifies the LIS.

```
<lis>
      <organization-name>Local access networks </organization-name>
      <hostname>lis34.example.com</hostname>
      <nena-id>nena1</nena-id>
      <contact>tel:+398348975439823</contact>
      <cert-uri>https://lis34.example.com/certificate.crt</cert-uri>
</lis>
```

All fields in the <*lis*> element are expected to be populated with the exception of <organization-name> and which is optional.

The LIS will determine the location of the user that corresponds to the Client-ID contained in the LocationKey parameter of the inbound <*lie*>. The determined location may be a geodetic location, of a civic address, or both may be returned. A geodetic location should always be provided for fallback route selection. The PIDF-LO is included along with the originating LocationKey and packaged in a responding <*lie*>. The <*lie*> and *ResultCode* are then returned to the VPC.

In the event that the LIS is unable to provide Client location information an error *result* is returned. The <*lie*> returned in this case will consist only of the original LocationKey. Valid *result* codes are listed in Table 5-8.

The <*datetimestamp*> is the date time stamp in UTC time indicating the time that the message was sent from the LIS. This field is optional, but if not included, then the VPC must maintain an accurate date and time stamp in any call event records so that an audit trail is readily accessible.

The <*message-id*> field is used to correlate the query with the response. If the element is included in the IPLRequest message, the IPLResponse message will include a <*message-id*> element with the same integer value as it received. This element is useful when a persistent connection is supported by the VPC to keep track of outstanding responses. The field is defined to be an integer that supports up to 6 digits, value 0-999999.

5.4.1.2.1 IPLResponse Message Format

There are two forms of the IPLResponse message, the successful case, where the returned LIE contains a LocationObject, and the error situation, where the LIE only contains the initial LocationKey. These two forms are illustrated below, with the success case being illustrated first.

```
<ipl-response xmlns="urn:nena:xml:ns:es:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:nena:xml:ns:es:v3 v3.xsd">

      <message-id>209344</message-id>

      <result>201</result>

      <lis>

            <hostname>lis.example.com</hostname>

            <nena-id>nena1</nena-id>

            <contact>tel:+398348975439823</contact>

            <cert-uri>https://lis.example.com/certificate.crt</cert-uri>

      </lis>

      <lie>

            <location-key>pres:3c01abe092@lis.example.com</location-key>

            <presence xmlns="urn:ietf:params:xml:ns:pidf"
      xmlns:pidf="urn:ietf:params:xml:ns:pidf"
      xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
      xmlns:gml="http://opengis.net/gml" entity="pres:user@example.com">

                  <tuple id="a6fea09">

                        <status>

                              <gp:geopriv>

                                    <gp:location-info>

                                          <gml:position>

                                                <gml:Point>

                                                      <gml:pos
                                    srsName="urn:EPSG:geographicCRS:4326">42.5463
-73.2512</gml:pos>

                                                </gml:Point>

                                          </gml:position>

                                    </gp:location-info>

                                    <gp:usage-rules />

                              </gp:geopriv>
```

```
                        </status>
                        <timestamp>2004-12-01T09:28:43+10:00</timestamp>
                    </tuple>
                </presence>
            </lie>
            <pos-source>RadioNetworkAccessPoint</pos-source>
            <datetimestamp>2004-12-12T21:28:43+10:00</datetimestamp>
</ipl-response>
```

```
<ipl-response xmlns="urn:nena:xml:ns:es:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:nena:xml:ns:es:v3 v3.xsd">
      <message-id>209344</message-id>
      <result>500</result>
      <lis>
            <hostname>lis.example.com</hostname>
            <nena-id>nena1</nena-id>
            <contact>tel:+398348975439823</contact>
            <cert-uri>https://lis.example.com/certificate.crt</cert-uri>
      </lis>
      <lie>
            <location-key>pres:3c01abe092@lis.example.com</location-key>
      </lie>
      <datetimestamp>2004-12-12T21:28:43+10:00</datetimestamp>
</ipl-response>
```

5.4.2 V3 Interface Security

The V3 interface will need to operate in a variety of network environments, some trusted, and some not as described in previously. V3 is a webservices interface and should be used with a suitable security mechanism as defined in section 3. When the connection between the LIS and the VPC is not a trusted network, both the LIS and VPC are expected to be protected with IPSEC or TLS, and thus require a certificates rooted in VESA. Even in a trusted network, TLS protection is advisable. The LIS is the server, and the VPC is the client in this interface. Mutual authentication is required when cryptographic security is deployed.

5.4.3 Call Flows, Key Scenarios and Semantics

Section 5.4.3 described in detail the 2 messages that make up communication across the V3 interface. This section will describe the key call scenarios and show the message flows between the various network elements.

5.4.3.1 LIS returns location in response to IPLRequest

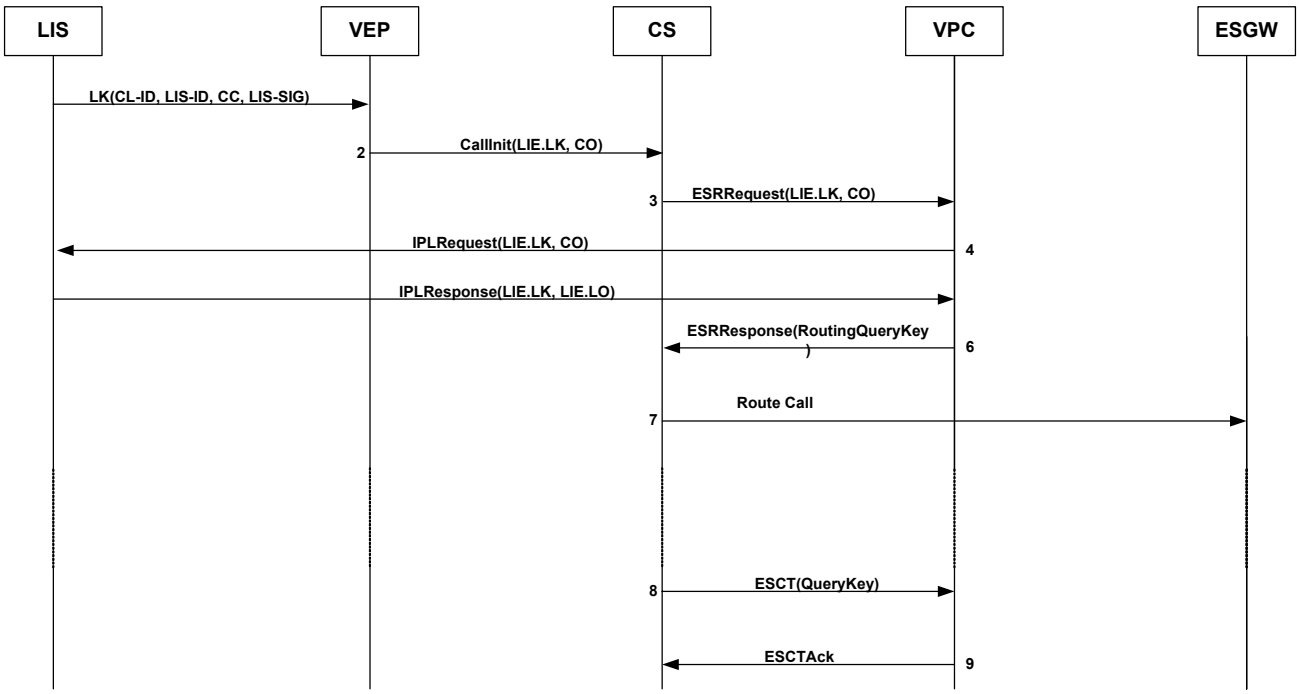


Figure 5-4 LIS returns location

1) The LIS server provides a LocationKey to the VEP.
2) The UA initiates an emergency call to the Call-Server and includes the LocationKey in a <*lie*> which is sent with the call initiation message.
3) The Call-Server optionally allocates the UA a callback number, and constructs an ESRRequest message containing the <*call-id*>, <*callback*> and <*lie*>. The Call-Server sends the ESRRequest message to the VPC.
4) The VPC receives the ESRRequest from the Call-Server and authenticates the Call-Server. The VPC uses the <*location-key*> contained in the <*lie*> to send the <*lie*> to the LIS requesting a location.
5) The LIS authenticates the VPC and validates the <*location-key*>. The LIS returns a <*lie*> to the VPC containing a valid location.
6) The VPC uses the location contained to request an ESRN, ESN, and CRN from the ERDB. The VPC uses the ESRN and ESN to allocate an ESQK. The VPC constructs an ESRResponse message and returns this to the Call-Server.
7) The Call-Server uses the returned information to subsequently route the call.
8) The Call-Server detects that call has concluded, and that the ESQK is no longer required. The Call-Server sends an ESCT message containing the ESQK to the VPC.
9) The VPC accepts the ESCT message, authenticates the Call-Server, and returns the ESQK to the pool of available ESQK. The VPC sends an ESCTAck message to the Call-Server

5.4.3.2 LIS returns location error

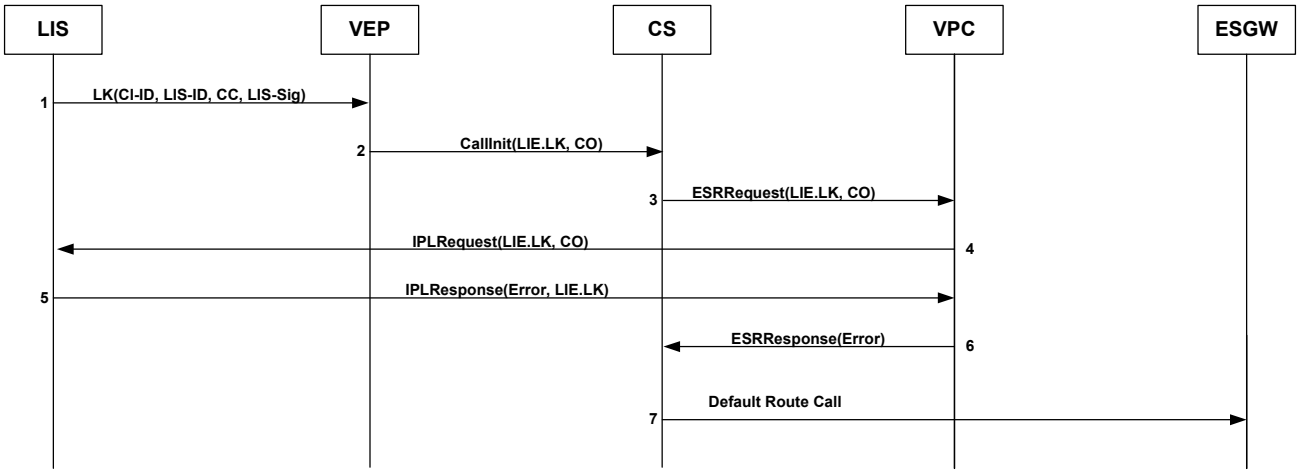


Figure 5-5 LIS returns location

1. The LIS server provides a LocationKey to the VEP.
2. The UA initiates an emergency call to the Call-Server and includes the <*location-key*> in a <*lie*> which is sent with the call initiation message.
3. The Call-Server optionally allocates the UA a callback number, and constructs an ESRRequest message containing the <*call-ied*>, <*callback*> and <*lie*>. The Call-Server sends the ESRRequest message to the VPC.
4. The VPC receives the ESRRequest from the Call-Server and authenticates the Call-Server. The VPC uses the <*location-key*> to send the <*lie*> to the LIS requesting a location.
5. The LIS authenticates and VPC and validates the <*location-key*>. The LIS is unable to determine the location of the client and returns an error to the VPC.
6. The VPC detects the error and in turn returns an error to the Call-Server.
7. The Call-Server detects the error and performs its default routing behavior in this situation, which may be to send the call to a default PSAP, or it may drop the call.

5.5 V4 Interface

This interface is expected to make use of SIP (as described in IETF RFC 3261) but other protocols can be used provided they meet the requirements included in this document. The V4 interface, outlined within the current NENA's i2 architecture, defines the communication protocol and messaging between a Proxy Server and an IP/TDM Gateway into the existing Emergency Services network. The gateway into the emergency services network is referred to as an ESGW. This interface specification is intended to outline the required data fields, with formats and examples, by which a SIP Proxy Server can properly assemble and send data – and also so that the Emergency Services Gateway knows what data format to expect, in order to further set-up and facilitate the completion of an emergency voice call to the appropriate E9-1-1 network element.

The V4 interface, defined to exist within the NENA i2 architecture, provides the final leg of IP messaging into the existing TDM-based Emergency Services Network. In the network implementation examples shown within this document, the V4 interface is always implemented between a SIP Proxy Server and an ESGW.

5.5.1 V4 Interface Architecture

Due to the flexibility of SIP, a variety of signaling paths leading up to the V4 interface may exist, including proxy configurations which terminate the V4 interface. Because of this network variability, the V4 interface may terminate to a 9-1-1 Call Server/Proxy, or any other (SIP) 9-1-1 Call Proxy. Despite other variations which may exist in practice, the following scenario depicts a simple i2 implementation and call flow. The 9-1-1 Call Server receives route information, (provided by the VPC), which then it uses to complete the call to the ESGW. The 9-1-1 Call Server formats a SIP INVITE message and sends it over the V4 interface to the ESGW. This model is depicted in Figure 4-1.

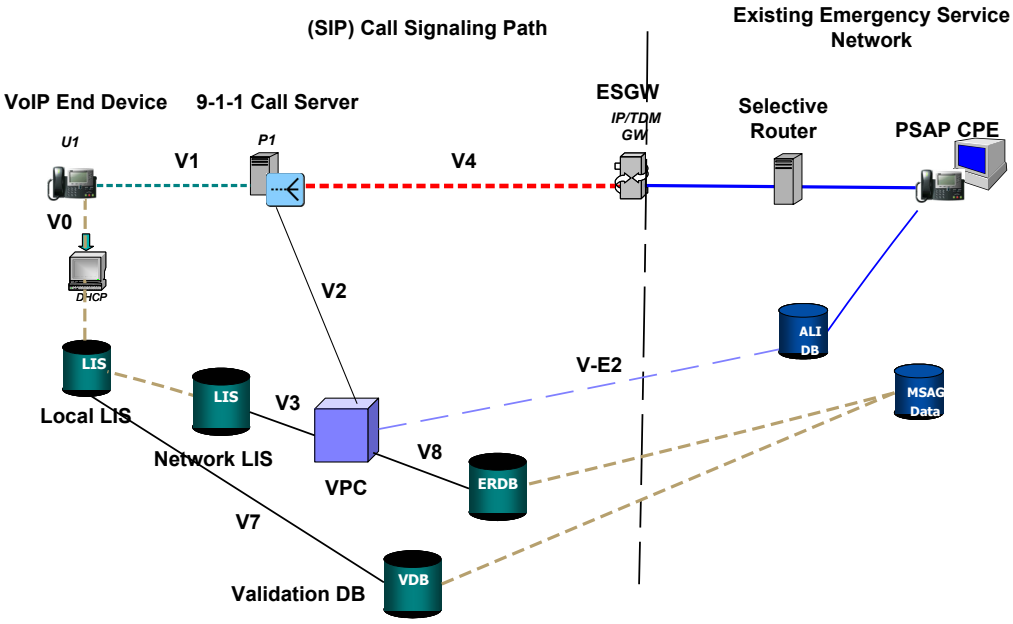


Figure 5-6 V4 Interface

5.5.2 V4 Security

The V4 interface will need to operate in a variety of network environments, some trusted, and some not as described in previously. V4 is a SIP interface and should be used with a suitable security mechanism as defined in Section 3. When the connection between the Call Server and the ESGW is not a trusted network, both the Call Server and ESGW are expected to be protected with IPSEC or TLS, and thus require certificates rooted in VESA. Even in a trusted network, TLS protection is advisable. Mutual authentication is required when cryptographic security is deployed.

5.5.3 V4 Interface Call Flow

The following call flow represented by a ladder diagram shows an emergency 9-1-1 call where the call server queries the VPC to obtain necessary 9-1-1 call routing information and then uses the received routing information to route the call to the ESGW. This messaging scenario is graphically depicted in figure 5-1. Messages which pertain to the V4 interface shown in red. Also included is a detailed call flow process description.

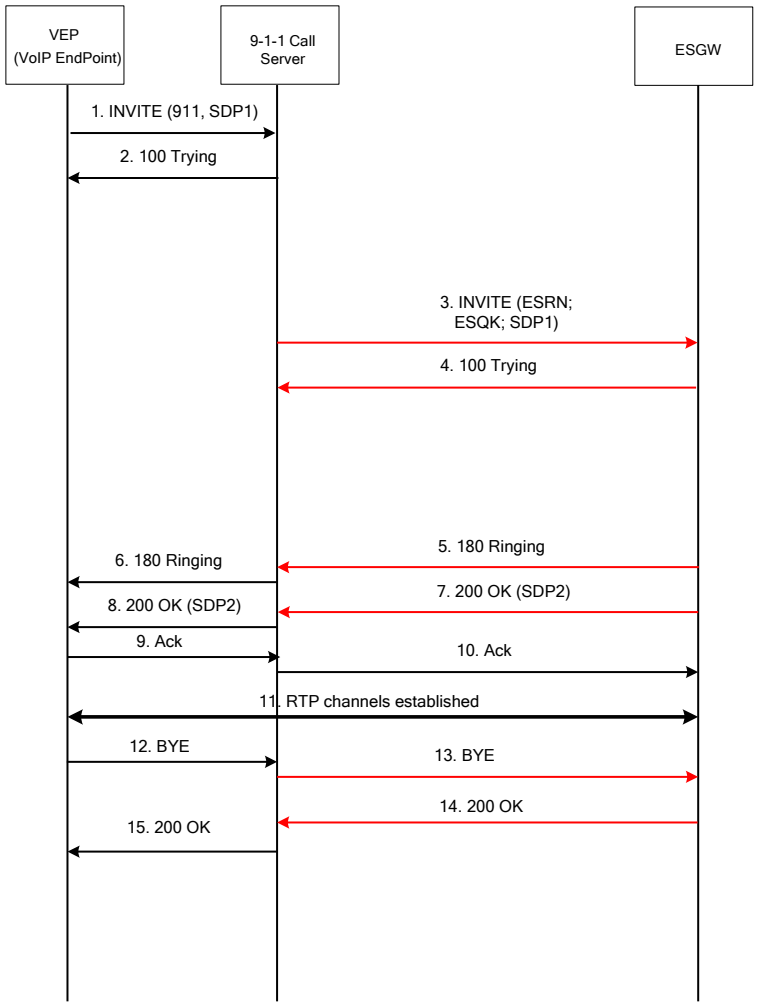


Figure 5-7 V4 interface – Call Flow

Detailed description of the procedure:

1. A VoIP Endpoint (VEP), which has registered with the VoIP Service Provider and has a known and validated location, initiates a 9-1-1 emergency call by sending a SIP INVITE message with 911 as dialed number and its media capabilities encapsulated in a SDP payload (denoted as SDP1), to the 9-1-1 Call Server.

2. The 9-1-1 Call Server responds back to the VEP with a SIP 100 Trying message.

3. The 9-1-1 Call Server requests routing information from the VPC. Using the information provided by the VPC, the 9-1-1 Call Server sends an INVITE to the ESGW in order for the ESGW to set up the call to the Selective Router using the ESRN to determine the appropriate trunk group. The ESQK is sent as the caller's identity.
4. The ESGW responds back to the 9-1-1 Call Server with a SIP 100 Trying message.
5. A SIP 180 Ringing message is returned from the ESGW to the 9-1-1 Call Server to indicate that the call has been delivered to the Selective Router.
6. A SIP 180 Ringing message is returned from the 9-1-1 Call Server to the VEP.
7. A SIP 200 OK message from the ESGW to the 9-1-1 Call Server to indicate that the call has been answered.
8. A SIP 200 OK message from the 9-1-1 Call Server to the VEP.
9 A SIP Ack is returned from the VEP to the 9-1-1 Call Server to acknowledge receipt of the 200 OK message.
10. A SIP Ack is returned from the 9-1-1 Call Server to the ESGW.
11. RTP channels are established end-to-end between the VEP and the ESGW.
12. After some time, the emergency caller releases the call and the VEP initiates a SIP BYE message to the 9-1-1 Call Server.
13. The 9-1-1 Call Server sends a SIP BYE message to the ESGW. (Note: Each call could be terminated from either end, though VEP call termination shown here.)
14. The ESGW sends a SIP 200 OK message to the 9-1-1 Call Server.
15. The 9-1-1 Call Server sends a SIP 200 OK to the VEP.

5.5.4 V4 Message Parameters

5.5.4.1 Sending of SIP INVITE message

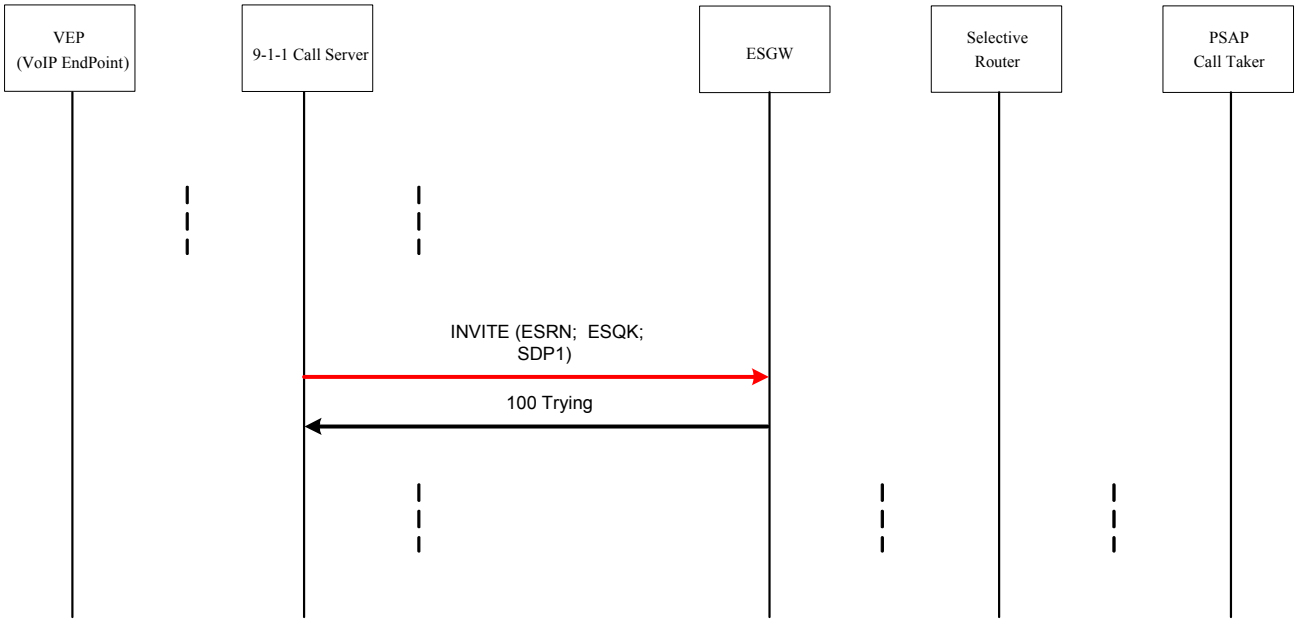


Figure 5-8 SIP INVITE

The message originates as a SIP INVITE from the 9-1-1 Call Server to the ESGW. Valid parameters for this message are included in the following table.

I2 Data Element	Condition	SIP Header found in	Description
Provider-ID	Mandatory	Via	The identifier of the Call Service provider (VSP).
ESQK (Emergency Service Query Key)	Conditional*	P-Asserted-Identity	Key allocated for the call for ALI query.
ESRN (Emergency Service Routing Number)	Conditional*	Request-URI	Number used to direct the call to the Emergency Service Gateway and SR trunk

Table 5-9 SIP INVITE - Standard Message Elements

* Both ESRN and ESQK are requested. Mandatory when available.

5.5.4.2 SIP 200 OK (SDP2) message

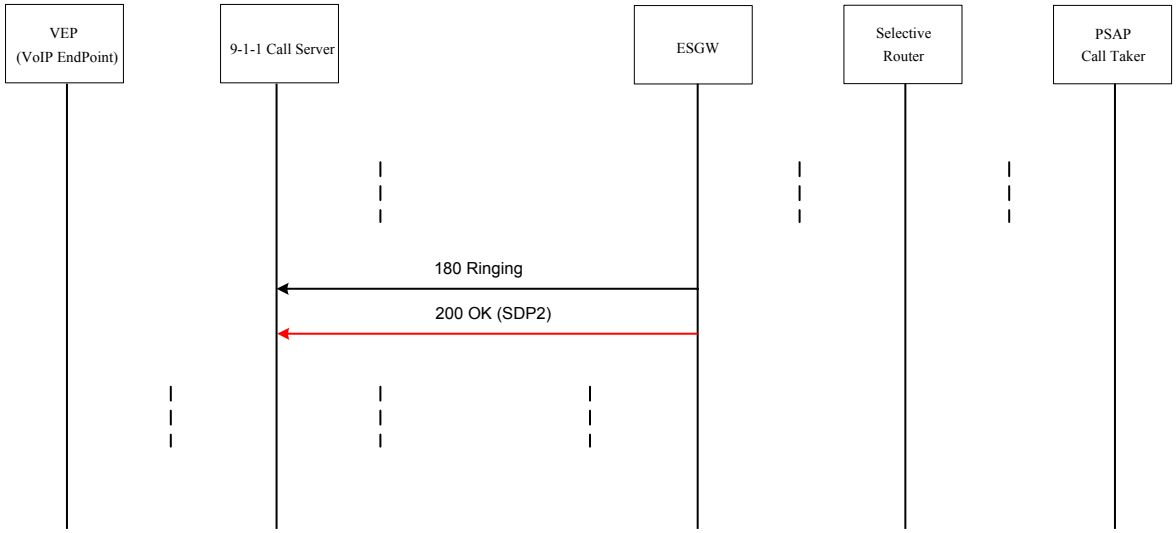


Figure 5-9 SIP 200 OK

The message originates as a SIP 200 OK from the ESGW. Valid parameters are included in the following table.

Parameter	Condition	SIP Header	Description
ESGW-ID	Mandatory	Via	The identifier (IP Address or FQDN) of the ESGW Service provider.

Table 5-10 SIP 200 OK

5.5.4.3 SIP BYE message (Termination from the VEP shown only)

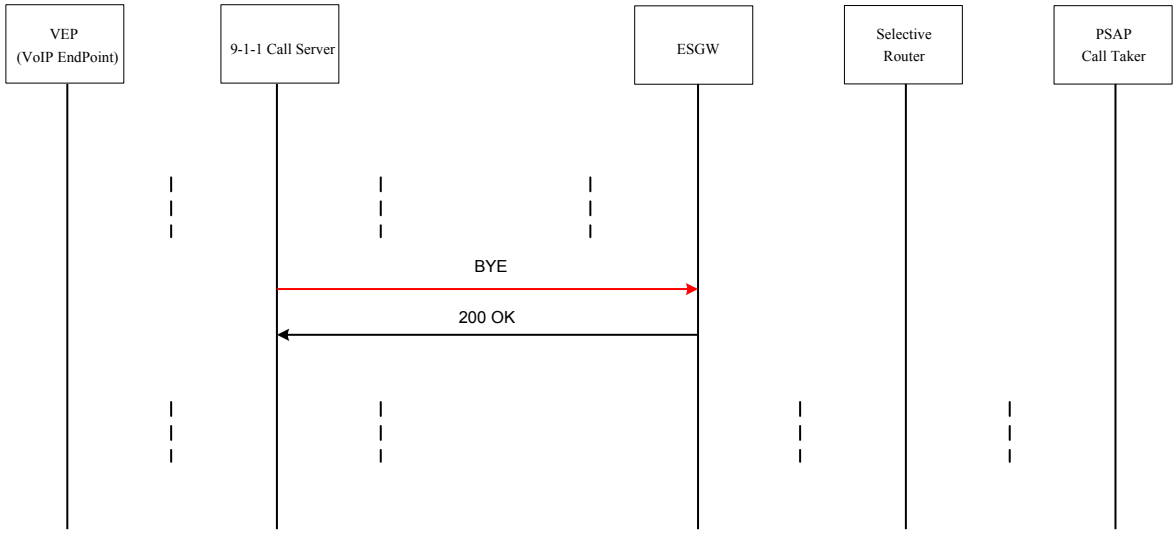


Figure 5-10 SIP BYE

The message originates as a SIP BYE from the VEP (in the case where the emergency caller releases the call). Valid parameters for this message are included in the following table.

Parameter	Condition	SIP Header	Description
CallBacknumber	Mandatory	From	Subscriber's originating TN

Table 5-11 SIP BYE

5.5.5 Specification of the V4 interface

5.5.5.1 Transport of SIP based V4 interface

UDP will be the default transport mechanism of V4 SIP interface with port 5060.
TCP will be used as alternative transport of V4 SIP interface, with port 5060.

5.5.5.2 SIP Methods, Messages and Information Elements

The implementation of V4 interface shall support the SIP methods and responses documented within this document, and as defined in RFC2543 and RFC3261.
The following table contains data labels for E9-1-1 call routing:

Data Element:	Example of:	Description:
ESQK	4445114444	Emergency Services Query Key
ESRN	1111111111	Emergency Services Routing

		Number
CallBacknumber	3333333333	Subscriber TN

Table 5-12 SIP Example Parameter Data

5.5.5.3 SIP INVITE message to ESGW:

When a Proxy Server/Call Server implementation is deployed connecting the V4 interface on one end and the ESGW on the other end, it is assumed that the Proxy Server will be interconnected to the VPC via the V5 or V2 interface. In either case, the Request URI (SIP INVITE) and P-Asserted-Identity header information should be constructed as follows:

```
INVITE sip:+1-ESRN@vsp.com;user=phone SIP/2.0
Via: SIP/2.0/UDP
callserver@vsp.com;branch=z9hG4bK4b43c2ff8.1
Max-Forwards: 68
To: <sip:911@vsp.com>
From: <sip:+1-Callbacknumber@vsp.com;user=phone>
P-Asserted-Identity: <sip:+1-ESQK@vsp.com>
```

5.5.5.3.1 ESGW SIP message handling:

When receiving a SIP INVITE with P-Asserted-Identity header, ESGW shall extract the number in the URI of P-Asserted-Identity over to the Calling Party Number parameter on the trunk interface to Selective Router.

5.5.5.3.2 SIP URI format

In all supported SIP messages for the V4 interface, the URI included in: From, Via, and Contact headers shall have one of the following formats:

number@domainname:port,
number@ipaddress:port, or
ipaddress:port

Where:

- number is a number string that contains up to 15 digits, e.g. 1234567890@10.1.1.22
- URI in the From field shall be identical to the URI in the LIS
- Definitions are based on RFC1034
- Port number may be absent if default port is used

5.5.5.4 Identifying a call instance

The following rules apply to the 9-1-1 Call Server, 9-1-1 Proxy Server, and ESGW.
For a call instance, the SIP BYE and CANCEL shall have the following information elements, which are required to be the same as the first SIP INVITE from the VoIP initiation endpoint for that call instance.

- Request-URI***;***
- To ***tag;***
- From ***tag;***
- Call-ID***;***
- CSeq ***(including method);***
- Via ***(Top) header***

For a call instance, the SIP ACK shall have the following information elements, consistent with the initial SIP INVITE received to the 9-1-1 Call Server for that call instance.

- Request-URI;
- From ***tag;***
- Call-ID
- CSeq ***(not including method);***
- Via ***(Top) header***

Any retransmitted SIP INVITE shall be identical to the first SIP INVITE.

Please refer to IETF RFC 3261 for more details on SIP message codings.

5.5.6 SIP Messages Examples

This section identifies what information is included in the headers exchanged in the SIP INVITE, 200 OK, and the SIP BYE messages over the V4 interface.
Note: Location information (PIDF-LO) and credential information within the SIP messaging, as part of a multipart Mime SIP message is retained. This means that parts can be used to authenticate, inform, and direct, but these parts are not to be removed during the transference of SIP messaging. The end result is that the V4 must support the inclusion of a PIDF-LO and associated credential information within the subsequent SIP INVITE messages.

SIP INVITE EXAMPLE - Represents V4 SIP INVITE (direction is 9-1-1 Call Server -> ESGW)

```
INVITE sip:+ ESRN@esgwprovider.com;user=phone SIP/2.0
Via: SIP/2.0/UDP callserver@vsp.com;branch=z9hG4bK4b43c2ff8.1
```

```
Max-Forwards: 68
To: <sip:911@vsp.com>
From: <sip:+1-Callbacknumber@vsp.com;user=phone>
P-Asserted-Identity: <sip:+ ESQK@vsp.com>
Call-ID: 123456789@vsp.com
CSeq: 1 INVITE
Content-Type: multipart/mixed; boundary="simple boundary"

--simple boundary
Content-type: application/cpim-pidf+xml; charset=us-ascii

(LO not shown)


--simple boundary
Content-type: application/pkcs-mime

(encrypted LO + From:URI message digest not shown)

--simple boundary
Content-Type: application/sdp

(SDP not shown)

--simple boundary
```

SIP 200 OK Example -- Represents V4 SIP 200 OK, (direction is ESGW -> 9-1-1 Call Server)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP gateway@esgw.com;branch=z9hG4bK4b43c2ff8.1
To: <sip:911@vsp.com>
From: <sip:+1-Callbacknumber@vsp.com;user=phone>
Call-ID: 123456789@vsp.com
CSeq: 1 INVITE
Contact: <sip:911@esgw.com>
Content-Type: application/sdp
Content-Length: 148

(SDP not shown)
```

SIP BYE Example - Represents V4 SIP BYE, (direction is 9-1-1 Call Server -> ESGW)

```
BYE sip:+ESRN@esgwprovider.com;user=phone SIP/2.0
Via: SIP/2.0/UDP callserver@vsp.com;branch=z9hG4bK4b43c2ff8.1
```

```
From: <sip:+1-Callbacknumber@vsp.com;user=phone>
To: <sip:911@vsp.com>
Call-ID: 123456789@vsp.com
CSeq: 1 BYE
Content-Length: 0
Max-Forwards: 69
```

SIP BYE Example - Represents V4 SIP BYE, (direction is ESGW -> 9-1-1 Proxy Server)

```
BYE sip: +1-Callbacknumber@vsp.com SIP/2.0
Via: SIP/2.0/UDP gateway@esgw.com;branch=z9hG4bK4b43c2ff8.1
Call-ID: 123456789@vsp.com
From: <sip:ESQK@vsp.com>
To: <sip: +1-Callbacknumber@vsp.com;user=phone>
CSeq: 1 BYE
Content-Length: 0
Max-Forwards: 69
```

5.5.7 Assumptions

1. The sip:uri user=token parameter has a token value equal to 'phone' to ensure existing gateway support (the use of an alternative token value would likely require software changes in various SIP based equipment.
2. The P-Asserted-Identity SIP header is used to specify the ESQK value, since the impact on subsequent ESGW processing will be minimized.
3. Either ordering or qvalues (ref. RFC3261) will be used to distinguish execution priority of multiple Contact headers.
4. ESRN number length will be specified as 10 digit numbers.
5. The logging of the specific ESGW used for the call will be done within the VPC and conveyed to the VPC using the 200 OK, then NOTIFY SIP messages.
6. The SIP 200 OK message from the ESGW will contain a Contact header, listing the IP address of the ESGW utilized.

5.6 V5 Interface

The V5 E9-1-1 VoIP interface defines the communication protocol and behaviors between the VoIP Call-Server (CS) and a SIP UA that performs Redirect Server (RS) functionality using Session Initiation Protocol (SIP), per RFC 3261, in response to an INVITE for the purpose of routing. In addition, the RS-UA will Subscribe to the CS to be Notified upon call termination. This document defines a V2 interface between the RS and Location Server (VPC) that would be the method to interface to the VPC is not an internal application on the RS.

5.6.1 Technical Description

The V5 interface is between the Call Server/Routing Proxy and a Redirect Server. It provides a means for the Call Server/Routing Proxy to request emergency service routing information. The protocol used is SIP. The Redirect Server receives an INVITE method and interfaces to the VPC,

either internally or via the V2 interface, to provide the emergency call parameters. The Redirect Server then formats a 3XX response with the emergency call parameters.

5.6.2 Transport of SIP based V5 interface

UDP will be the default transport mechanism for the V5 interface. TCP is an alternative transport. TCP/TLS (sips) should be used for interfaces where public access is required.

5.6.2.1 Emergency Service Routing Request (ESRRequest)

The message originates as a SIP INVITE from the Call-Server/Routing Proxy. Valid parameters for the INVITE ESRRequest are included in Table 5-13. The table below shows a subset of the parameters is SIP message that are significant with respect to the V5 interface.

Parameter	Condition	SIP Header	Description
Provider-ID	Mandatory	Via	Call Server entity requesting routing instructions.
URI-ID	Mandatory	From	Contains either a E.164 callback number (normal case) or identifier used to obtain the caller's information from a LIS.
PIDF-LO	Conditional- Note1	MIME body	Source of location information.

Table 5-13 SIP ESRRequest

NOTE 1. Sent if present

5.6.2.2 Emergency Services Routing Response (ESRReponse)

The SIP 300 message response is sent from the Redirect Server to the Call-Server/Routing Proxy in response to an INVITE (ESRRequest). Valid parameters for the SIP 300 (ESRResponse) response are contained in the table below.

Parameter	Condition	SIP Header	Description
Provider-ID	Mandatory	Via	Redirect Server responding to INVITE.
RoutingQueryKey (ESQK)	Conditional	PAI	Key allocated for the call.
RoutingNumber (ESRN)	Conditional	Contact	Number used to direct the call to the ESGW.
LRO	Conditional	Contact	Contingency Routing Number to be used for fallback or returned for error conditions (with no ESRN/ESQK)

Table 5-14 SIP ESRResponse

5.6.2.3 Emergency Services Call Termination (ESCT)

To enable call termination reporting using existing SIP methods, emergency calls must include subscription as part of the exchange with the Redirect Server. A **SUBSCRIBE** method is sent from the Redirect Server to the Call Server following the ESRRequest. This is to make the Call Server aware that notification should be sent upon termination of the call. When the Call Server detects the call has completed, a **NOTIFY** method is sent to the redirect server. The redirect server informs the VPC, either internally or by sending an ESCT message over the V2 interface (refer to Section 5.3), to enable the ESQK allocated for the call to be released and to inform the VPC of the ESGW that was used.

5.6.2.3.1 Initiate Subscription to Call

Following the 300 response from the RS, a SUBSRIBE is sent from the RS to the Call Server to convey that the RS desires to receive messages pertaining to this particular dialog (the emergency caller). The Call Server responds with a NOTIFY to acknowledge receipt of the SUBSCRIBE. The tables below reflect this initial exchange:

Parameter	Condition	SIP Header	Description
Provider-ID	Mandatory	Via	The identifier of the Redirect server.
FROM	Mandatory	From	RS URI and tag associated with the subscription
Package	Mandatory	Event	Identify type of event being subscribed to

Parameter	Condition	SIP Header	Description
			and the call-id value associated with this subscription
Timer	Manadatory	Expires	On initial subscription this value is set to the ESQK timeout value.

Table 5-15 SUBSCRIBE (Initial subscription)

Parameter	Condition	SIP Header	Description
Provider-ID	Mandatory	Via	Contains Call Server URI
URI-ID	Mandatory	From	URI of the caller sent in the From header.
State	Mandatory	Subscription-State	Status of the call - active
Dialog-content		Content-Type: dialog-info	Dialog package – refer to call flow examples. Provides the entity (caller URI-ID), state=current value, call-Id of this particular leg of the call, and tag.

Table 5-16 NOTIFY (Ack from CS)

5.6.2.3.2 Call Terminates

When the call ends, either caller or Emergency service end, the RS gets notified that the call has completed. Below shows the parameters in the NOTIFY when the call completes.

Parameter	Condition	SIP Header	Description
Provider-ID	Mandatory	Via	Contains Call Server URI
URI-ID	Mandatory	From	URI of the caller sent in the From header. URI associated with ESQK for the call.
State	Mandatory	Subscription-State	Status of the call is active
Dialog-content		Content-Type: dialog-info	Dialog package – refer to call flow examples. Provides the entity

Parameter	Condition	SIP Header	Description
			(caller URI-ID), call-Id of this particular leg of the call, state=**terminated**, and tag.

Table 5-17 NOTIFY (CS to RS on Termination)

5.6.2.3.3 Final Exchange to Confirm

This exchange is necessary to notify the CS that the subscription is over. The CS could indicate the call is over without the need of this final exchange if the CS supports setting the Subscription-state value to terminated, and then that closes the subscription, making it unnecessary for the RS to send this exchange as defined below:

Parameter	Condition	SIP Header	Description
Provider-ID	Mandatory	Via	The identifier of the Redirect server.
FROM	Mandatory	From	RS URI and tag associated with the subscription
Package	Mandatory	Event	Identify type of event being subscribed to and the call-id value associated with this subscription
Timer	Manadatory	Expires	0 – indicates the subscription is over

Table 5-18 SUBSCRIBE (Final Confirmation)

Parameter	Condition	SIP Header	Description
Provider-ID	Mandatory	Via	Contains Call Server URI
URI-ID	Mandatory	From	URI of the caller sent in the From header. URI associated with ESQK for the call.
State	Mandatory	Subscription-State	Status of the call is active
Dialog-content	Mandatory	Content-Type: dialog-info	No content

Parameter	Condition	SIP Header	Description
Length	Mandatory	Content-Length	0 – means no content

Table 5-19 NOTIFY (Ack from CS for final Confirm)

5.6.3 SIP Exchange Example

This section identifies what information is included in the headers exchanged between the Call Server Entity requesting emergency call routing instructions and RS (refer to ESRRequest/ESRResponse and ESCT sections earlier for parameter definitions):

The following would be representative of the SIP INVITE (ESSRequest).

Message 1: Call Server to Redirect Server over V5 Interface

INVITE sips:911@RS-UA Provider-ID SIP/2.0
Via: SIP/2.0 /TCP CS-Provider-ID;branch=z9hG4bKrandomstuff1
To: 911 <sips:911@RS-UA-Provider-ID.com>
From: CPN <sip: URI-ID@myvsp.com>;tag=value
Call-ID: Call-Idvalue-**1**
CSeq: 1 INVITE
`Content-Type: multipart/mixed; boundary="simple boundary"`
`Content-Length: XXXX`

Refer to draft-ietf-sipping-location-requirements-02[12] for additional information.

The following would be representative of the 300 Response (ESRResponse):
Message 2: RS to CS over the V5 Interface

SIP/2.0 300 Multiple Choices
Via: SIP/2.0 /TCP CS-Provider-ID;branch=z9hG4bKrandomstuff1
To: 911 <sips:911@RS-UA-Provider-ID.com>
From: URI-ID <sip: URI-ID@myvsp.com>;tag=**A-value**
Call-ID: Call-Idvalue-**1**
CSeq: theCSeqvalue1 INVITE
Contact: <sips:+1-ESRN@CS-Provider-ID?P-asserted-identity:=<sips:+1-ESQK@ CS-Provider-ID >>
Contact: <sips:+1-LRO@ CS-Provider-ID >

Call is sent to the ESGW by CS:

Message 3: CS to ESGW over V4 Interface

INVITE sips:+1-ESRN@ESGW Provider-ID SIP/2.0
Via: SIP/2.0 /TCP CS-Provider-ID;branch=z9hG4bKrandomstuff1

To: 911 <sip:911@CS-Provider-ID>
From: URI-ID <sip:URI-ID@myvsp.com>;tag= **A-value**
P-asserted-identity:<sip:+1-ESQK@CS-Provider-ID>
Call-ID: Call-Idvalue-**1**
CSeq: theCSeqvalue1 INVITE
Etc.

The following would be representative of the SUBSCRIBER/NOTIFY exchange:

Message 4: RS to CS over V5 Interface

SUBSCRIBE CS-Provider-ID SIP/2.0
Via: SIP/2.0 /TCP RS-UA-Provider-ID;branchz9hG4bKrandomstuff3
Call-ID: Call-Idvalue**2**
To: <sip:URI-ID@myvsp.com>
From: RS-UA-Provider-ID ;tag=RS-1234
Cseq: 12121 SUBSCRIBE
Event: dialog; call-id="Call-Idvalue**1**";from-tag= **A-value** (INVITE, from)
Expires: (VPC ESQK expiration timer value)

…..
200 OK SUBSCRIBE in reply

Message 5: CS to RS over V5 – immediate Notify confirming the subscription and containing current state

NOTIFY sips: RS-UA-Provider-ID SIP/2.0
Via: SIP/2.0/TCP CS-Provider-ID;branchz9hG4bKrandomstuff4
To: CS- Provider-ID;branch=z9hG4bKrandomstuff4
Call-ID: Call-Idvalue**2**
From: <sip:URI-ID@myvsp.com>;from-tag3
Cseq: 1 NOTIFY
Event: dialog
Subscription-State: active;expires=timeleft
Content-Type: dialog-info
Content-Length: <body-length>

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info"
version="0"
state="full"
entity=":URI-ID@myvsp.com> <dialog id="as7d900as8" call-id="Call-Idvalue**1**"
local-tag="RS1234(from SUBSCRIBE)" direction="initiator">
<state>whatever it is right now</state>

```
  </dialog>
</dialog-info>
```

200 OK NOTIFY in reply
200 OK INVITE in reply from ESGW
CS sends NOTIFY on Answer to RS and gets 200 OK NOTIFY in reply

Message 7: CS to RS over V5 after CS receives BYE from ESGW
(NOTE: Can come from VEP as well, same result)

NOTIFY sips: RS-UA-Provider-ID SIP/2.0
Via: SIP/2.0/TCP CS-Provider-ID;branch=z9hG4bKrandomstuff4
Call-ID: Call-IDValue**2**
To: cs3.myvsp.com
From: <sip:URI-ID@myvsp.com>;from-tag3
Cseq: 1 NOTIFY
Event: dialog
Subscription-State: active;expires=timeleft
Content-Type: dialog-info
Content-Length: <body-length>

```
<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info"
          version="2"
          state="full"
          entity=":URI-ID@myvsp.com>  <dialog id="as7d900as8" call-id=" Call-IDValue1"
        local-tag=" RS-1234(from SUBSCRIBE)" direction="initiator">
   <state>terminated</state>
  </dialog>
</dialog-info>
```

Message 8: RS to CS over V5 Interface to Confirm termination of the Subscription

SUBSCRIBE CS-Provider-ID SIP/2.0
Via: SIP/2.0 /TCP RS-UA-Provider-ID;branchz9hG4bKrandomstuff3
Call-ID: Call-Idvalue**2**
To: <sip:URI-ID@myvsp.com>
From: RS-UA-Provider-ID ;tag=RS-1234
Cseq: 12121 SUBSCRIBE
Event: dialog; call-id=" theCall-Idvalue**1**";from-tag= **A-value** (INIVITE, from)
Expires: **0**

…..

200 OK SUBSCRIBE in reply

Message 9: CS to RS over V5 –Notify confirming completion of the subscription

NOTIFY sips: RS-UA-Provider-ID SIP/2.0
Via: SIP/2.0/TCP CS-Provider-ID;branchz9hG4bKrandomstuff4
To: CS- Provider-ID;branch=z9hG4bKrandomstuff4
Call-ID: Call-Idvalue**2**
From: <sip:URI-ID@myvsp.com>;from-tag3
Cseq: 1 NOTIFY
Event: dialog
Subscription-State: terminated;expires=0
Content-Type: dialog-info
Content-Length: 0

NOTE: If the CS sends a NOTIFY that indicates that the call is over, the CS can set the Subscription-state value to terminated, and that closes the subscription, making it unnecessary for the RS to send another SUBSCRIBE with expires=0.

200 OK NOTIFY in reply

5.6.3.1 ESSRequest Details - SIP INVITE Request

Provider-ID – The identity of the VoIP Service Provider (Call Server). This is included in the **Via** header as part of the URI in the form of an IP address.
URI-ID – An identifier that pertains to the emergency caller for the call in progress at the Call-Server. For i2 this is expected to be call back number, but can be a standard SIP URI that enables retrieval of the caller's information, e.g. from a LIS. This parameter is included in the **From** header as part of the URI. If it is a Callback number then the format is expected to be a PSTN dialable (E.164) and routable number.
PIDF- LO – If the LO is included, it contains information on the caller's location. The format of the PIDF-LO is defined by the V1 interface and is included as a PIDF-LO body within the SIP INVITE.

When an INVITE is received, a request is sent to the VPC via V2 or internally for routing instructions.

5.6.3.2 ESSResponse Details - SIP 3XX Response

Once the Redirect Server has received the ESQK, ESRN, and LRO from the VPC, it formats and sends a **300 Multiple Choices** response. Most of the headers received in the INVITE are echoed back and two **Contact** headers are added. The Contact headers are ordered such that the first header contains ESRN/ESQK information and the second one contains the LRO for fallback. A qvalue parameter can be optionally added to each line to explicitly provide ordering.
Contact header (first line)– this header is added to the 300 response. It contains the ESRN and a Pre-asserted Identity, PAI, containing the ESQK, e.g., **Contact: <ESRN>?PAI:<ESQK>:qvalue=#**

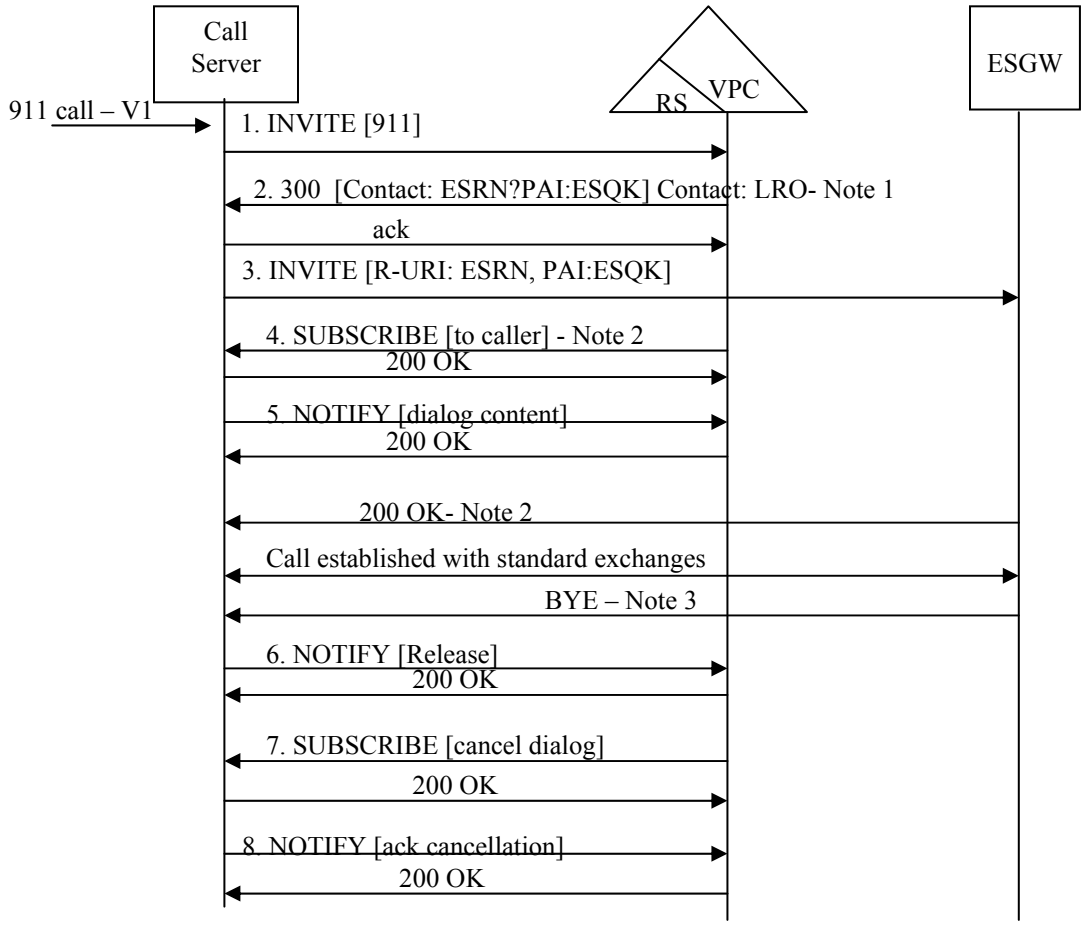
Contact header (second line) - it contains the LRO, e.g., **Contact: <LRO>:qvalue=#**. The LRO is used by the Call Server/Routing Proxy for contingency routing.

NOTE: The 300 response may just contain one **Contact** header with only the LRO. This is a valid return and indicates that the VPC was unable to provide the ESRN/ESQK. The Call Server/Routing Proxy would then use the LRO to route the call.

5.6.4 V5 Security Requirements

The V5 interface will need to operate in a variety of network environments, some trusted, and some not as described in previously. V5 is a SIP interface and should be used with a suitable security mechanism as defined in Section 3. When the connection between the Call Server and the Redirect Server is not a trusted network, both the Call Server and Redirect Server are expected to be protected with IPSEC or TLS, and thus require a certificates rooted in VESA. Even in a trusted network, TLS protection is advisable. Mutual authentication is required when cryptographic security is deployed.

5.6.5 Query/Response Flows



NOTES:
1. ESQK is placed in a P-Asserted Identity. Second Contact header contains LRO
2. 200 OK from the INVITE to ESGW can come before the SUBSCRIBE
3. BYE can come from either direction

1. A caller invoked an emergency call that is received at the Call Server. The Call Server sends an INVITE to the Redirect Server (RS).
2. The Redirect Server requests the VPC to determine the routing key based on information contained in the INVITE. The VPC allocates an ESQK and determines the routing number, ESRN for the call and provides this information to the Redirect Server. The Redirect Server formats a 300 response containing the routing information back to the Call Server. A standard SIP ACK is returned to the RS to acknowledge receipt of the 300 response.
3. The Call Server sends an INVITE to the ESGW to set up the call to the Selective Router using the ESRN to determine the appropriate ESGW. The ESQK is sent as the caller's identity.
4. The RS also sends a SUBSCRIBE method to the Call Server so that it is kept in the loop when the call disconnects. A 200 is returned to acknowledge receipt.

5. The Call Server returns a NOTIFY to acknowledge receipt of the SUBSCRIBE and the RS responds with a 200 acknowledgement.

The call has been established and the caller and PSAP can now communicate. The message exchange to establish the call is standard SIP signaling is not shown.

6. Some time later, the call is released. (The call may be terminated from either direction.) The Call Server sends a NOTIFY with the URI-ID of the caller to the RS. The RS receives the information and forwards it on to the VPC to enable the VPC to release the ESQK.
7. The RS sends another SUBSCRIBE to cancel the subscription to the dialog and receives a 200 ack from the CS.
8. The CS sends a NOTIFY to confirm the cancellation and the RS responds with a 200 ack.

5.7 V6 Interface

The V6 interface is defined as a SIP interface from a Call Server to a 9-1-1 Routing Proxy. This interface is used where the Call Server desires to unconditionally route all emergency calls to an entity that will both determine the route and forward the call to the correct ESGW. The Call Server does not need to remain in the call setup path.

5.7.1 Architecture

This SIP-based implementation of a VoIP emergency call network incorporates a 9-1-1 Routing Proxy to which all emergency calls are forwarded. The V6 interface is the SIP messaging between the Call Server and the Routing Proxy. The Routing Proxy then contacts the VPC (possibly using the V2 interface) to obtain ESRN and ESQK and forwards the call to the correct ESGW. This network model is depicted in Figure 5-11.

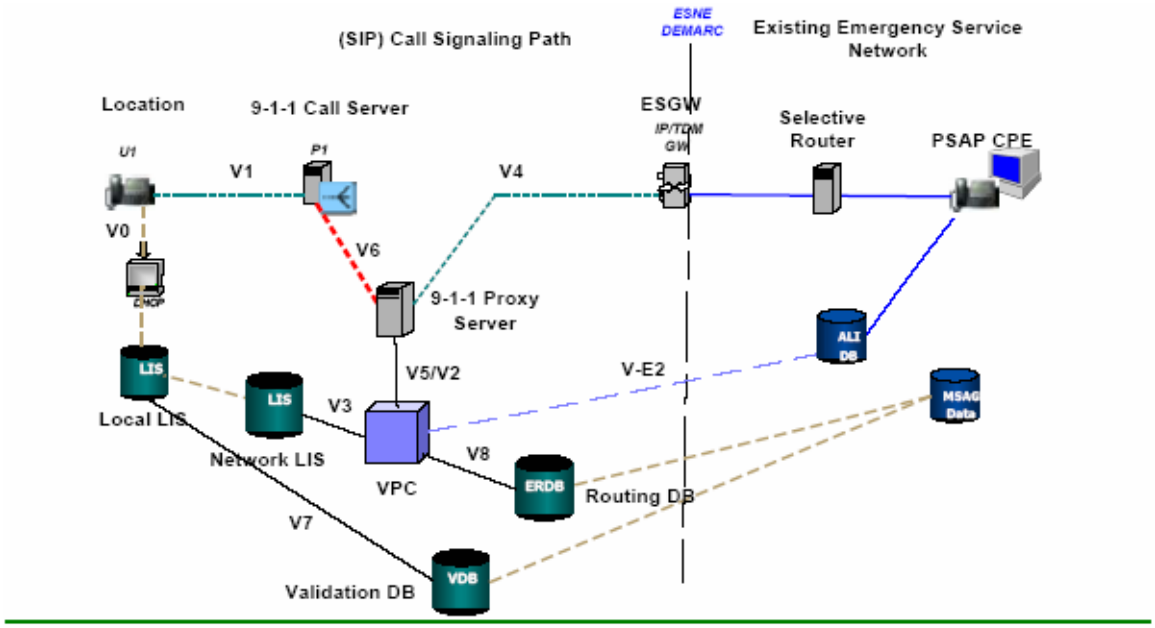


Figure 5-11 9-1-1 Proxy Server Control Model

5.7.2 Functional Call Flow

The following call flow represents a typical 9-1-1 call where the Call Server utilizes a 9-1-1 Proxy Server which has a connection to a VPC. All necessary call information is passed to the 9-1-1 Proxy Server using a SIP INVITE. After the proper route is determined by the VPC using the V2 or V5 interface, the 9-1-1 Proxy Server routes the call to the appropriate ESGW via the V4 interface.

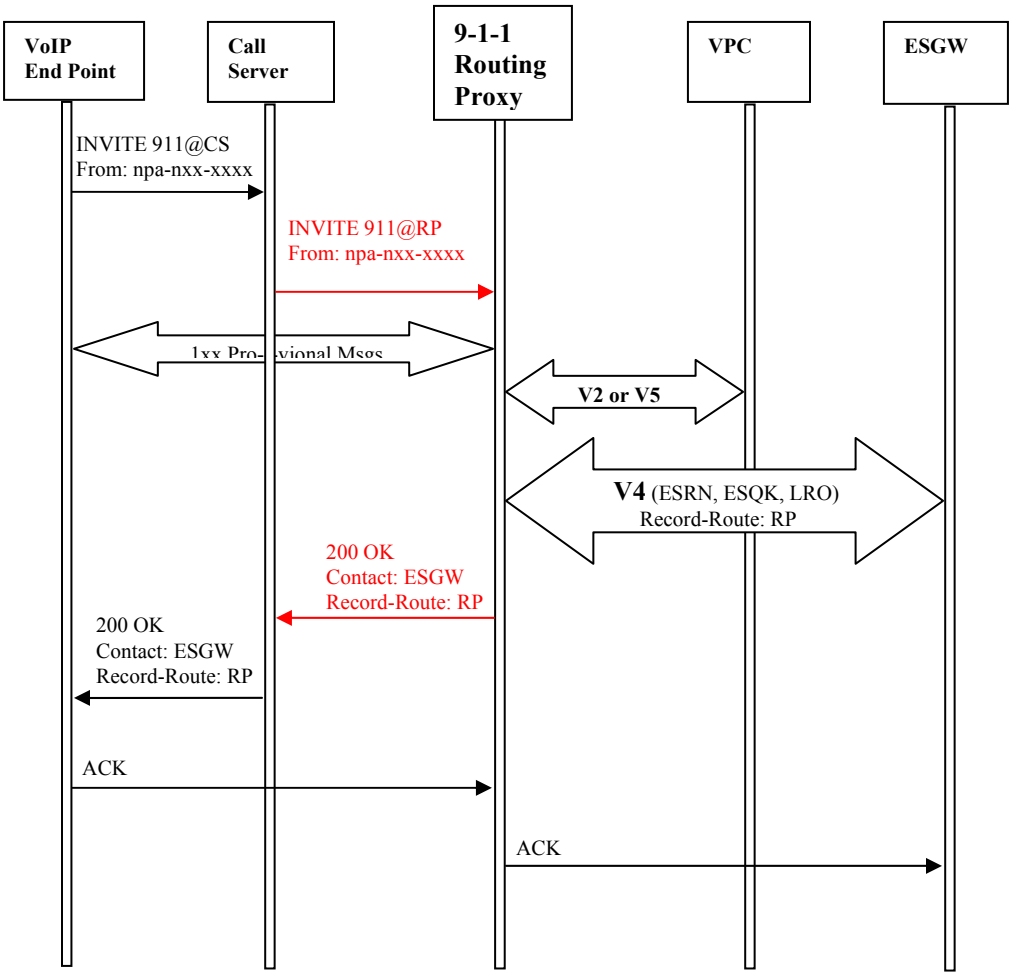


Figure 5-12 V6 interface Call Flow

5.7.3 Specification of the V6 interface

5.7.3.1 Transport of SIP based V6 interface

UDP will be the default transport mechanism for the V6 interface.
TCP will be used as an alternative transport for the V6 interface.

5.7.3.2 SIP Methods, Messages and Information Elements

The implementation of V6 interface shall support the SIP methods and responses documented in RFC2543 and RFC3261.

5.7.3.3 Security

The V6 interface will need to operate in a variety of network environments, some trusted, and some not as described in previously. V6 is a SIP interface and should be used with a suitable security mechanism as defined in Section 3. When the connection between the Call Server and the Routing Proxy Server is not a trusted network, both the Call Server and Routing Proxy Server are expected to be protected with IPSEC or TLS, and thus require a certificates rooted in VESA. Even in a trusted network, TLS protection is advisable. Mutual authentication is required when cryptographic security is deployed.

5.7.4 Assumptions

When a 9-1-1 Proxy Server control model implementation is used, the 9-1-1 Proxy Server will be interconnected to the VPC via the V2 or V5 interface or the equivalent messaging set.

5.8 V-E2 Interface

The V-E2 interface, in the context of the i2 Solution Migration architecture, defines the communication protocol and messaging between a VPC and an ALI DB. This interface specification outlines the required data fields, with formats and examples, by which a VPC shall properly assemble and send emergency call-related data in response to a query from an ALI DB, in order to facilitate the delivery of emergency call-related data to a conventional i2 Solution PSAP.

5.8.1 Technical Description

The V-E2 interface is between a VPC and the ALI DB. This interface is based on the E2 interface between a wireless Mobile Positioning Center (MPC) and an Emergency Services Message Entity (ESME) described in NENA-05-001[9], which is in turn based on TIA J-STD-036-B. This document provides incremental requirements, describing the differences from NENA 05-001.

The technical description and the network architecture described in Sections 3 and 4 of NENA 05-001 shall apply with the following clarifications for the i2 Solution. In the i2 Solution architecture, the VPC takes the place of the MPC in the architecture and the ESME is referred to as an ALI, as illustrated in Figure 5-13.

[9] NENA-05-001, *NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2 Interface*, December 2003.

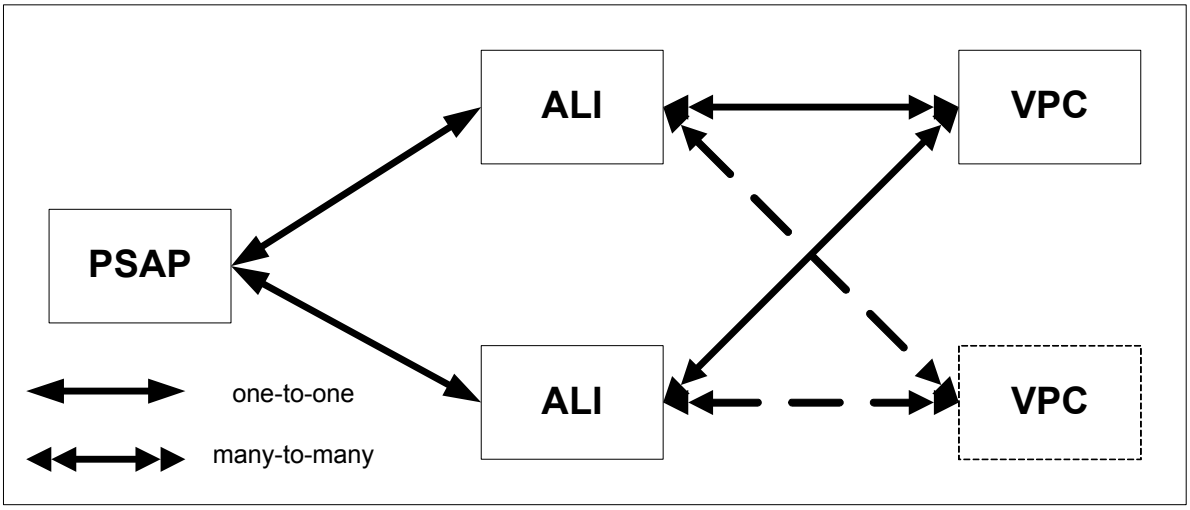


Figure 5-13. V-E2 Interface Architecture

It is not recommended that an E2 interface as described in TIA J-STD-036A (rather than NENA 05-001) be used as the basis for the VPC to ALI interface. However, if this is the case, the ALI will not be able to receive civic location information. It may receive some information, e.g., Call Back Number or geo location if it is available. Please refer to Appendix A.

If a PAM interface is used for communications between the VPC and the ALI, this is not specified as part of the i2 Solution.

VPC operators may determine to reuse existing physical interfaces to establish V-E2 logical connection along side existing E2+ logical connections based on business agreements.

5.8.2 Messages

There are four Request/Response messages defined in NENA 05-001 that are defined here for use in requesting and responding to requests for emergency call information from the VPC. The remainder of this section details the four messages that make up communication across the V-E2 interface.

The VPC and the ALI DB shall be able to support the messages and parameters defined in NENA 05-001, as modified in this document for use across the V-E2 interface.

5.8.2.1 Emergency Services Position Request (ESPOSREQ)

The ESPOSREQ message is sent from the ALI DB to the VPC to request call and location related information from the VPC for an emergency call, identified by a query key, the Emergency Services Query Key (ESQK). The valid parameters for the ESPOSREQ message are included in the following table. The ALI DB shall use the Position Request parameter to make the initial request for location information as well as to request updates of location.

Table 5-20. ESPOSREQ Parameters

Parameter	§ Ref. in NENA 05-001	Condition	Description/Value
Package Type=Query with Permission	9.1.1	M	Query with Permission
Transaction ID	9.1.2	M	
Component Sequence	9.2.1	M	
Component Type	9.2.2	M	Invoke (Last)
Component ID	9.2.3	M	
Operation Code	9.2.4	M	Private TCAP
Parameter Set	9.2.7	M	
ESMEIdentification	9.3.1	M	
Position Request Type	9.3.2	M	
Emergency Services Routing Key (esprKey)	9.3.3	M[10]	Emergency Services Query Key (ESQK)
Callback Number	9.3.4	NA[11]	Not Used in this version of the i2 Solution. The current version of the i2 Solution uses the Wireline Compatibility Mode which includes delivery of only the ESQK to the PSAP. Therefore, this parameter is not populated.

[10] This parameter is Optional in NENA 05-001 for wireless call information provided to the ESME from the MPC. However, when the E2 interface is used to support VoIP call information from a VPC to an ESME, this parameter must be populated with the Emergency Services Query Key.

[11] This parameter is Optional in NENA 05-001 for wireless call information provided to the ESME from the MPC. However, when the E2 interface is used to support VoIP call information from a VPC to an ESME, this parameter must not be populated..

5.8.2.2 Emergency Services Position Request Response (esposreq)

This message is sent from VPC to the ALI to inform the ALI of the position of the VoIP Endpoint.

Table 5-21. Emergency Services Position Request Response (esposreq) Parameters

Parameter	§ Reference in NENA 05-001	§ Ref. in this doc.	Inclusion Condition	Description/Value
Package Type	9.1.1	-	M	Response
Transaction ID	9.1.2	-	M	
Component Sequence	9.2.1	-	M	
Component Type	9.2.2	-	M	Return Result (Last)
Component ID	9.2.3	-	M	
Parameter Set	9.2.7	-	M	
Position Result	9.3.8	-	M	
PositionInformation	9.3.9			
Geographic Position	9.3.9.2	1.1.3.3	O	Geo Location
Position Source	9.3.9.3	5.8.3.3	O	Method of location determination
CallbackNumber	9.3.5	5.8.3.4	O[12]	Caller's E.164 number
Emergency Services Routing Digits	9.3.7	5.8.3.4	NA	Not used. (In the future this parameter might be populated with ESQK)
GeneralizedTime	9.3.11 (and 9.3.9.1?)	5.8.3.6	O	Timestamp for assignment of ESQK
MobileIdentificationNumber	9.3.12	5.8.3.7	NA	Not used
InternationalMobileSubscriber Identity (IMSI)	9.3.13	-	NA	Not used
MobileCallStatus	9.3.14	-	NA	Not used
CompanyID	9.3.15	5.8.3.8	M[13]	Name of the VSP (up to 15 characters)

[12] This parameter is Optional in NENA 05-001 for wireless call information provided to the ESME from the MPC. However, when the E2 interface is used to support VoIP call information from a VPC to an ESME, this parameter must be populated with an E.164 number identifying the Callback Number of the emergency caller, if it is available to the VPC.

[13] This parameter is Optional in NENA 05-001 for wireless call information provided to the ESME from the MPC. However, when the E2 interface is used to support VoIP call information from a VPC to an ESME, this parameter must be populated with identification for the VoIP Service Provider, if it is available to the VPC. If one is not available, the VPC must substitute its own name.

LocationDescription	9.3.16	5.8.3.9	O	Tagged elements

The VPC shall use the civic location information if received in the response from the ERDB to populate the civic location information in this response message.

5.8.2.3 Emergency Services Position Request Response Return Error

This message is sent from the VPC to the ALI to inform the ALI that the requested action was not performed. The Error Code contains the reason for the failure.

Table 5-22. Emergency Services Position Request Response Return Error Parameters

Parameter	§ Reference in NENA 05-001	§ Reference in this document	Condition	Description/Value
Package Type	9.1.1	-	M	Response
Transaction ID	9.1.2	-	M	
Component Sequence	9.2.1	-	M	
Component Type	9.2.2	-	M	Return Result (Last)
Component ID	9.2.3	-	M	
Error Code	9.2.5			
Parameter Set	9.2.7	-	M	

No new error codes have been identified for this application.

5.8.2.4 Emergency Services Position Request Response Reject

This message is sent from the VPC to the ALI to inform the ALI that the invoke message contains a Transaction or Component Level protocol error. The problem code describes the nature of the protocol error.

Table 5-23. Emergency Services Position Request Response Reject Parameters

Parameter	§ Reference in NENA 05-001	§ Reference in this document	Condition	Description/Value
Package Type	9.1.1	-	M	Response

Parameter	§ Reference in NENA 05-001	§ Reference in this document	Condition	Description/Value
Transaction ID	9.1.2	-	M	
Component Sequence	9.2.1	-	M	
Component Type	9.2.2	-	M	Return Result (Last)
Component ID	9.2.3	-	M	
Problem Code	9.2.6			
Parameter Set	9.2.7	-	M	

No new problem codes have been identified for this application.

5.8.3 Emergency Services Protocol (ESP) Parameters

This section identifies the use and also differences from NENA 05-001 that shall be supported when the V-E2 interface is implemented between a VPC and the ALI.

5.8.3.1 ESMEIdentification

The ESMEIdentification parameter shall be populated with the identification of the ALI requesting the location information.

5.8.3.2 Position Information – Geographic Position Parameter

If coordinate-based location information is provided to the VPC for the emergency call, this information shall be used to populate the Position Information – Geographic Position Parameter. Specifically, the VPC shall obtain the geo-location parameters from the PIDF-LO contained in the Location Information Element parameter of the Emergency Services Routing Request received by the VPC over the V2 interface as described in Section 5.3. (If the VPC receives the Location Information Element directly from an LIS, the following requirements apply if a geo-location object is included.) The contents of these geo-location parameters shall be mapped to the V-E2 interface Geographic Position parameter described in Section 9.3.19.2 of NENA 05-001, with one exception, noted below.

- If the received geo-location object information does not include altitude or uncertainty parameters, the VPC shall use the Type of Shape and Shape description corresponding to "Ellipsoid Point"
- (FUTURE, for further study) If the received geo-location object information includes uncertainty and confidence but not altitude parameters, the VPC shall use the Type of Shape and Shape description corresponding to "Ellipsoid Point with Uncertainty."

- If the received geo-location object information includes altitude, with or without uncertainty parameters, and the altitude type is specified as "meters," the VPC shall use the Type of Shape and Shape description corresponding to "Point with altitude and uncertainty."
- The degrees of latitude shall be used to populate the Degrees of Latitude in the Type of Shape and Shape description parameter. If degrees of latitude are provided in a format different from the one supported on the V-E2 interface, or if the degrees of latitude are provided in a coordinate system different from the one supported on the V-E2 interface (i.e., WGS84), the VPC shall convert the latitude information to a format suitable for coding of degrees of latitude on the V-E2 interface.
- The degrees of longitude shall be used to populate the Degrees of Longitude in the Type of Shape and Shape description parameter. If degrees of longitude are provided in a format different from the one supported on the V-E2 interface, or if the degrees of longitude are provided in a coordinate system different from the one supported on the V-E2 interface (i.e., WGS84[14]), the VPC shall convert the longitude information to a format suitable for coding of degrees of longitude on the V-E2 interface.
- (Future) If an Uncertainty parameter value is included and available to the VPC, the VPC may use this information to populate the Uncertainty code and Confidence parameters of the Type of Shape and Shape description parameter.
- If an Altitude parameter is included, and the Altitude type is specified as "meters," the VPC shall use its contents to populate the Altitude in the Type of Shape and Shape description used for Point with Altitude and Uncertainty. If uncertainty/confidence values are not available to the VPC, when an Altitude parameter is included, the value of K for the uncertainty code and confidence shall be populated with 0 to indicate "no information." If Altitude Uncertainty/Confidence are included, the VPC shall use this information to populate the Altitude Uncertainty code and Confidence parameters in the Type of Shape and Shape description parameter. If Altitude uncertainty/confidence values are not available to the VPC, when an Altitude parameter is included, the value of K for the uncertainty code and confidence shall be populated with 0 to indicate "no information."
- If an Altitude parameter is included, and the Altitude type is specified as "floor," the VPC shall use the use its contents to populate the Location parameter contained in the Location Description parameter described in NENA 05-001, Section 9.3.16, subject to the additional requirements described in Section 5.8.3.9.

[14] Military Standard WGS84 , METRIC MIL-STD-2401, Military Standard – Department of Defense World Geodetic System, 11 January 1994.

5.8.3.3 Position Information - Position Source Parameter

The VPC shall use the "Method" parameter included in the PIDF-LO to populate the Position Source parameter. The V-E2 interface shall support the new codings of the Position Source referred in the shown in Table 5-24. Values of this parameter can be used by the ESME to identify this call as a VoIP call.
If the "Method" parameter is not included in the PIDF-LO, the VPC shall populate the Position Source parameter with the value corresponding to "IP-Unknown."

Table 5-24. Mappings of "Method token" values of the PIDF-LO to codings of the Position Source Parameter in the esposreq Response Message

Location Object parameter (PIDF-LO: "Method token" Value)	Position Source parameter value (decimal)**	Position Source parameter value meaning
<Not provided in PIDF-LO>	128	IP – Unknown
Manual: entered manually by an operator or user, e.g., based on subscriber billing or service location information	129	IP – Manual entry
DHCP: provided by DHCP (used for wireline access networks, see 802.11 below)	130	IP - Network Assisted – (e.g., via DHCP)
Triangulation: triangulated from time-of-arrival, signal strength or similar measurements	131	IP – Network Assisted – RF Derived (e.g., ToA, Triangulation)
Cell: location of the cellular radio antenna	132	IP – Radio Network Access Point (e.g., lat/lon of cellualar tower or of 802.11 transceiver)
802.11: 802.11 access point (used for DHCP-based provisioning over wireless access networks)	132	IP – Radio Network Access Point (e.g., lat/lon of cellualar tower or of 802.11 transceiver)
	133	IP - Radio Network Sector (e.g. lat/lon of centroid of cellular sector coverage area, or centroid of 802.11 coverage area with directional antennas)
GPS: Global Positioning System	134	IP – GPS (e.g., GPS in the handset)*
A-GPS: GPS with assistance	135	IP – A-GPS (e.g., network-assisted GPS)*
	136	Derived, via Transformation (e.g. either Geo-Coding or Reverse-Geo-Coding)

* Note: The values for GPS and A-GPS are provided here separately in order for contextual distinction that implemented systems may rely on (i.e. GPS fix for a *VoIP* emergency call).

** These values have been proposed and liaisons have been initiated to reserve these values for assignment by NENA in the i2 Solution.

5.8.3.4 Callback Number

The Callback Number parameter shall be populated with an E.164 number that represents the emergency caller in the i2 Solution. This Callback Number shall be derived by the VPC from the Callback parameter of the Emergency Services Routing Request described for the V2 interface in Section 5.3.

5.8.3.5 Emergency Services Routing Key

The VPC shall populate the Emergency Services Routing Key parameter with the Emergency Services Query Key received in the ESPOSREQ message and used by the VPC as a key to obtaining the emergency call related information used in this response.

5.8.3.6 Generalized Time

The VPC shall populate the Generalized Time parameter with the time that the ESQK was allocated to the current emergency call (with which it is associated and for which location information is being provided).

5.8.3.7 Mobile Identification Number (use for: Main Telephone Number)

The VPC may populate the Mobile Identification Number with the Main Telephone Number (applicable in Muli-Line Telephone Systems) if one is provided for the emergency call. Otherwise, this optional parameter can be omitted.

5.8.3.8 Company ID

The VPC shall populate this parameter with the name of the VoIP Service Provider, if available.

5.8.3.9 LocationDescription

The VPC shall populate the Location Description parameter with the appropriate data fields tagged using the NENA version 4 XML tags as defined in the NENA 02-010, *Standards for Recommended Formats & Protocols For Data Exchange*, and as described in NENA 05-001, Section 9.3.16.
The VPC shall use the information obtained from the civic address location object to populate these fields, using the mapping described in Table 5-25.

Table 5-25. Mappings of Civic Address Data Elements and Other Data Elements to Tagged Fields in Location Description Parameter

Location Object parameter (PIDF-LO: Civic Address Type)	Populated by the VPC	NENA XML 4.0 tag in Location Description parameter
PIDF-LO: Civil: HNO		Location Description: <HNO>
PIDF-LO: Civil: HNS		Location Description: <HNS>
PIDF-LO: Civil: PRD		Location Description: <PRD>
PIDF-LO: Civil: STN		Location Description: <STN>

Location Object parameter (PIDF-LO: Civic Address Type)	Populated by the VPC	NENA XML 4.0 tag in Location Description parameter
PIDF-LO: Civil: STS		Location Description: <STS>
PIDF-LO: Civil: POD		Location Description: <POD>
PIDF-LO: Civil: A3		Location Description: <MCN>
PIDF-LO: Civil: A1		Location Description: <STA>
PIDF-LO: Civil: County Name[15]		Location Description: <COI>
PIDF-LO: Civil: LOC		Location Description: <LOC>*
PIDF-LO: Civil: FLR (CAtype27) – To be supported soon		Include "FL<content>" in LOC <content>*
PIDF-LO: Civil: LMK		Not supported.
	NENA ID of the VSP	Location Description: <CPF>
PIDF-LO: Civil: NAM		Location Description: <NAM>

*NOTE: This information shall be included in the contents of the <LOC> tagged field as follows:

- If included in the PIDF-LO, these fields shall be concatenated in the following order: Floor, Location (LOC).
- Each field shall be directly preceded by the indicated abbreviation (i.e., FL, LOC), and shall be separated from the next field by the character "~" (tilde).
- If the information for a given field cannot be included completely (i.e., without truncating it), then the last (truncated) field to be included shall also end with the character "~" (tilde) to indicate that it has been truncated.

The VPC operator and the E9-1-1 Service Provider/Database operator should determine if an administrative ESN value can be transmitted over the V-E2 interface without causing any detrimental affects to the 9-1-1 system.

If supported, the VPC shall use the administrative ESN received from the ERDB to populate the ESN tagged field in the Location Description parameter. If an administrative ESN is not available for the call, then the VPC may use the value of the Routing ESN to populate the ESN, or shall omit the ESN tagged value from the Location Description parameter.

5.9 V7 Interface

This section describes the V7 interface between the V7 Client (e.g., LIS) and the VDB. The V7 Client shall use this capability to verify that an address is VDB valid.

The most common initial use case is that a VOIP subscriber completes a web page requesting E911 service (the web site being provided by the VSP). The E911 web page will require the user to enter the postal address where Emergency Services should be directed. The web page will then submit the

[15] The VPC must convert the received County Name to a FIPS County Code.

postal address to the VDB as a web service call to validateAddress[16]. Another use case will be support of LIS requests for location validation for more than a single address as records are added, modified, or re-validated. In this case the LIS may also use this protocol to send web service calls to the appropriate VDB(s). Section 5.9.5 provides additional Use Cases and recommendations for client implementations of the V7 Interface.

5.9.1 V7 Interface Requirements

The validateAddress request shall require the following data elements to be supplied:

- StreetName
- MSAGCommunity *or* PostalCommunity *or* both
- StateProvince
- Country

The validateAddress may require the following data elements to be supplied:

- PrefixDirectional
- StreetSuffix
- PostDirectional
- CountyName
- CountyID
- PostalCode
- HouseNum
- HouseNumSuffix

The VDB shall return the Postal Address, MSAG Community Name, information as to whether the address is valid and, optionally, the geo-code of the address when the validation succeeds. The VDB may return MSAG County ID (if it is present in the MSAG).

The VDB shall return suggested alternate Postal Address(es) when the validation fails (if alternates exist).

It is recommended that V7 clients submit address using only country-specific postal service abbreviations; however V7 clients may submit addresses using any non postal service abbreviations.

The VDB shall return addresses using only country-specific postal service street suffix abbreviations and directional abbreviations in the appropriate fields.

When MSAGCommunity and PostalCommunity are both present in the request the VDB shall first use MSAGCommunity to search the VDB database. If a match is not found using MSAGCommunity it shall use PostalCommunity to search the VDB database.

When only one Community is present in the request the VDB shall use that information to search the VDB database.

If a single match for the submitted Address is found the web service shall return a “no error” condition and the data from the VDB database search. If no match is found and the VDB is

[16] Determination of which VDB to call is being specified in Section 2.10

searching the DB using PostalCommunity, the VDB shall lookup MSAGCommunity from the translation table. If a translation value is found the VDB shall search the database with the translated community name. If a single match is found the web service shall return a "no error" condition and the data from the VDB database search.

If the preceding searches have not found a match the VDB may use other search mechanisms to find likely matches for the address. Some alternate methods are:

- return where HouseNum = <input house num>, StreetName sounds (e.g. soundex algorithm) like <input street name>, State = <input state> and Zip = <input zip>
- search for alternate spellings for StreetName and Abbreviations in a translation table

In this case, if any matches are found the web service will return an "error—but alternatives found" code and return up to a specified number of matches[17]. If no matches are found the web service will return an "error—no matches found" code.

If the submitted address is for a geographical area that is not in the serving area of the VDB, the VDB may return a URI for another VDB that may serve that area. In the case of an error condition, the VDB may opt to include an AlternateURI field to identify an additional resource for additional helps and features to determine a valid civic location

5.9.2 Validated Address to PIDF-LO Mapping

This table shows how data elements returned by the V7 interface would be mapped to PIDF-LO for an emergency call. The Validated data tag names shown in the following table are from the validateAddressResponse returned by the V7 interface. The coordinates will be provided using WGS84 using EPSG 4326 format.

Validated Address Element	**PIDF-LO Element**
HouseNum	HNO
HouseNumSuffix	HNS
PrefixDirectional	PRD
StreetName	A6
PostDirectional	POD
MSAGCommunity	A3
PostalCommunity	PCN[18]
StateProvince	A1
CountyName	A2
PostalZipCode	PC
Country	Country
Latitude	gml:coordinates

[17] The maximum number of alternatives to be provided may be configurable by the VDB operator.
[18] PCN is documented in draft-ietf-geopriv-dhcp-civil-05 but does not appear to be included in draft-ietf-geopriv-pidf-lo-03. A request will be made to the IETF to include PCN in the pidf-lo.

Longitude	gml:coordinates

Table 5-26 Validated Data Tag Names

5.9.3 Security

This section describes the VoIP E911 i2 migration standard for the V7 interface between the VDB and LIS. The V7 interface is XML-based.

The V7 interface will need to operate in a variety of network environments, some trusted, and some not. It is for this reason that the V7 interface is a webservices interface and should be used with a suitable transport layer encryption protocol such as TLS. This provides strong security mechanisms and is readily able to traverse enterprise and commercial firewalls when correctly configured. The LIS is expected to be a VESA certified entity, and the configuration of the LIS should be such that it uses a server-side VESA certificate that is presented to the VDB on session establishment. This allows the VDB to validate the LIS credentials before agreeing to accept and provide location information. The VDB may use this information for billing or other purposes

5.9.4 WSDL Description

The WSDL used in this Web Service definition uses the data types and tag names defined in the NENA 4 Generation 1, Release 0 schemas. See http://www.nena.org/xml_schemas/Current%20Release/ALI%20Type%20Library/ALITypeLib.xsd and http://www.nena.org/xml_schemas/Current%20Release/XALI-SchemaFamily/Schema%20Maps.htm for documentation of the referenced data types. Elements from the ALI Type library use the alins name space in the snippets shown below. See http://www.nena.org/xml%5Fschemas/ for NENA defined XML schema. See Appendix B for the full WSDL definition.

To use Location Validation, the caller invokes the Web Service – encoding the address in the validateAddressRequest message shown below. The VDB shall validate the data received against the appropriate VDB database and return an indicator of the data's validity and one or more addresses that may be matches for the input address.

5.9.4.1 validateAddress

5.9.4.1.1 validateAddressRequest

The XML submitted to validateAddress is described as follows (the type definitions for the data elements are defined in the NENA ALI Type Library schema which is specified in the WSDL schema definitions):

```
<message name="validateAddressRequest">
  <part name="parameters" element="y:ValidateAddressIn"/>
</message>

  <xs:element name="ValidateAddressIn">
    <xs:complexType>
```

```
        <xs:annotation>
         <xs:documentation>Message ID is an optional field -- if sent in by the caller it will be
echoed back out in the response. Customer ID will be assigned by the VDB operator and will be
provided to the customer.
         </xs:documentation>
        </xs:annotation>
        <xs:sequence>
         <xs:element name="MessageID" type="xs:string" minOccurs="0" maxOccurs="1"/>
         <xs:element name="CustomerID" type="xs:string" minOccurs="0" maxOccurs="1"/>
         <xs:element name="StreetAddress" type="y:StreetAddressType" minOccurs="1"
maxOccurs="1"/>
        </xs:sequence>
       </xs:complexType>
     </xs:element>

<xs:complexType name="StreetAddressType">
   <xsd:annotation>

    <xsd:documentation>Civic Address in NENA format using NENA field definitions.

   </xsd:documentation>

  </xsd:annotation>
  <xs:all>
     <xs:element name="HouseNum" type="tns:HouseNumType" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="HouseNumSuffix" type="alins:HouseNumSuffixType" minOccurs="0"/>
     <xs:element name="PrefixDirectional" type="tns:PrefixDirectionalType" minOccurs="0"
maxOccurs="1"/>
     <xs:element name="StreetName" type="tns:StreetNameType" minOccurs="1"
maxOccurs="1"/>
     <xs:element name="StreetSuffix" type="tns:StreetSuffixType" minOccurs="0"
maxOccurs="1"/>
     <xs:element name="PostDirectional" type="tns:PostDirectionalType" minOccurs="0"
maxOccurs="1"/>
     <xs:element name="MSAGCommunity" type="tns:MSAGCommunityNameType"
minOccurs="0" maxOccurs="1"/>
     <xs:element name="PostalCommunity" type="tns:PostalCommunityNameType" minOccurs="0"
maxOccurs="1"/>
     <xs:element name="CountyName" type="xs:string" minOccurs="0" maxOccurs="1"/>
     <xs:element name="CountyID" type="tns:CountyIDType" minOccurs="0" maxOccurs="1"/>
     <xs:element name="StateProvince" type="tns:StateProvinceType" minOccurs="1"
maxOccurs="1"/>
     <xs:element name="PostalCode" type="tns:ZipType" minOccurs="0" maxOccurs="1"/>
```

```
    <xs:element name="Country" type="xs:string" minOccurs="1" maxOccurs="1"/>
  </xs:all>
</xs:complexType>
```

Required parameters are:

- StreetName
- MSAGCommunity or PostalCommunity (either or both may be submitted)
- StateProvince
- Country

5.9.4.1.1.1 Example Request:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <SOAP-ENV:Body>
                <m:validateAddress xmlns:m="http://www.nena9-1-1.org/schemas/2004/msag">
                        <MessageID>abcdef</MessageID>
                        <CustomerID>LISID</CustomerID>
                        <StreetAddress>
                          <HouseNum>700</HouseNum>
                          <StreetName>LAVACA</StreetName>
                          <StreetSuffix>ST</StreetSuffix>
                          <PostalCommunity>AUSTIN</PostalCommunity>
                          <StateProvince>TX</StateProvince>
                          <PostalCode>78701</PostalCode>
                          <Country>US</Country>
                        </StreetAddress>
                </m:validateAddress>
        </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

5.9.4.1.2 validateAddressResponse

The validateAddressResponse returns a ReturnCode showing Success or Error. It also returns a true/false field (Valid) that shows whether the submitted address is valid. It contains an array of Street Addresses that will contain a single address (for Success) or one to ‘n’ (n to be determined by the VDB operator) addresses (for Failures if any ‘n’possible matches were found).

When the Return Code 210 = Success (locaiton is MSAG Valid but address was modified), the VDB shall include the modified information in the validateAddressResponse message. For example, if submitted AV is changed to AVE in order to validation, or if John Carpenter Freeway is submitted and changed to Hwy 144, the modified value is used in the StreetAddress included in the AddressList in the validateAddressResponse.

If the submitted address is for a geographical area that is not served by the VDB the Response may contain URI for a VDB that does serve that area in the AlternateURI field. In the case of an error condition, the VDB may opt to include an AlternateURI field to identify an additional resource for additional helps and features to determine a valid civic location

```
<message name="validateAddressResponse">
  <part name="parameters" element="y:ValidateAddressOut"/>
</message>

    <xs:element name="ValidateAddressOut">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="MessageID" type="xs:string" minOccurs="0" maxOccurs="1"/>
          <xs:element name="ReturnCode" type="y:ReturnCodeType" minOccurs="1"
maxOccurs="1"/>
              <xs:element name="Valid" type="y:ValidType" minOccurs="1" maxOccurs="1"/>
          <xs:element name="AddressList" type="y:AddressGeoType" minOccurs="0"
maxOccurs="unbounded"/>
          <xs:element name="AlternateURI" type="xs:anyURI" minOccurs="0" maxOccurs="1"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>
```

The Address List contains zero or more elements of this type (ordered from best match to the worst match):

```
      <xs:complexType name="AddressGeoType">
            <xs:all>
                  <xs:element name="Civic" type="y:StreetAddressType"[19] minOccurs="1"
maxOccurs="1"/>
                  <xs:element name="GeoPosition" type="alins:GeoPositionType"
minOccurs="0" maxOccurs="1"/>
            </xs:all>
      </xs:complexType>
```

There will be no Addresses returned if the input address fails validation and no alternative addresses are found.

Return Code	Description
200	Success (location is MSAG Valid)

[19] See the StreetAddressType definition from validateAddressRequest.

210	Success (location is MSAG Valid but address was modified).
551	Street Name is required
552	Community is required
553	State/Province is required
555	Prefix Directional must contain only the characters N, S, E, W and must be from 1-3 in length. See ALI Type Library definition for tns:PrefixDirectionalType.
556	Post Directional must contain only the characters N, S, E, W and must be from 1-3 in length. See ALI Type Library definition for tns:PostDirectionalType.
558	State not found
559	Community not found
560	Street not found
561	House number is out of range
562	Not in Serving Area. If this error is returned the Response may or may not include value for the Alternate URI.
500	Internal Server Error (to indicate System Failure)

Table 5-27 Return Codes

5.9.5 V7 Client Considerations/Recommendations

The V7 standard addresses only the messaging between a V7 client (e.g. a LIS) and V7 server (e.g. a VDB). This document/section/appendix presents some suggestions/guidelines that are outside the scope of the V7 standard. Following these guidelines will help a VDB and V7 client developer ensure that their users can validate addresses quickly, and help ensure that the V7 client is well behaved with respect to a V7 server.

5.9.5.1 Overview

A typical V7 client will provide a GUI to a user to collect addresses for validation. The V7 client will use the data from the GUI to create and send V7 messages to the VDB (the V7 server). The V7 client will receive the V7 response message, parse the message, then use the parsed data to populate fields in the GUI presented to the User.

This appendix will present two types of V7 clients: a V7 client in a wiremap LIS implementation and a V7 client in a VSP's Subscriber self-provisioning "web portal." This document focuses on these two types from the much wider spectrum in order to keep the discussion more concrete.

5.9.5.2 Wiremap LIS

The user for this type of V7 client will be the "administrator" of the wiremap LIS installation. The administrator will need to validate addresses when the LIS is first installed. Whenever new physical

ports are wired, the administrator may need to validate addresses for those ports. Also addresses will need to be re-validated on a periodic basis.

This document assumes that the LIS solution presents web pages as the GUI to the LIS administrator.

Recommendation: The form presented to the LIS administrator should have distinct fields for each part of the address, and those fields should match the fields in the underlying V7 messages.

Recommendation: The form should use drop-downs for fields where the V7 interface suggests the clients limit the data they send to relatively few values.

> For example, if the V7 interface says that clients should limit the values submitted for directionals to one of [e.g., N, S, E, W, NE, NW, SE, SW] it's best to use a drop-down on the web page forms presented to the LIS administrator. Using drop-downs help minimizes the round-trip interactions required of the LIS administrator to validate an address.

Recommendation: For fields where the V7 interface suggests the clients limit the data they send to large but well known set of values, those fields should be validated prior to sending V7 messages.

> For example, if the V7 interface says that clients should limit the values for submitted street suffixes to those listed in country-specific Postal Standards, it would be impractical to try to populate a web form drop-down with so many values. So it would be better to allow the LIS administrator to enter suffixes free-form in a suffix field. Because the list is well known, the LIS should validate the street suffix prior to sending a V7 message.
>
> These validations could be client-side javascript, or validations running within the LIS webserver prior to sending the V7 message. The result of a validation should be a suggestion to change the suffix prior to submitting for full validation. The LIS administrator should always be able to proceed even if they don't accept this suggestion.
>
> It is best for the LIS V7 implementation to do these types of simple validations, because the VDB is not required to suggest alternatives. By doing these validations and making suggestions up front, the LIS can insure a better user experience for the LIS administrator.

Recommendation: When the V7 response contains address alternatives, the GUI should display the alternatives in the same order, indicating the first alternative is likely the best choice.

5.9.5.3 VSP Subscriber self-provisioning "web portal"

The user for this type of V7 client will be a VoIP Subscriber (the owner/user of the VoIP handset). This address validation interaction will occur when the Subscriber first signs up with the VSP, or when a subscriber changes their location (e.g. moves to a new address).

Recommendation: The Subscriber should use a GUI on a web page to submit their address.

To minimize data entry, the VSP GUI could pre-populate the form with the Subscriber's E-911 address. If the VSP does not have this information available they may pre-populate the form with the Subscriber's billing address. But the Subscriber must still go through some kind of GUI to confirm the address for purposes of emergency calls.

Recommendation: The form presented to the Subscriber should have distinct fields for each part of the address, and those fields should match the fields in the underlying V7 messages.

This is the same recommendation as for a LIS.

Some VSPs may choose to utilize more sophisticated software in their web portal that can parse a more free-form address. VSPs cannot rely on the VDB to perform these types of sophisticated parsings.

Recommendation: The form should use drop-downs for fields where the V7 interface suggests the clients limit the data they send to relatively few values.

This is the same recommendation as for a LIS

Recommendation: For fields where the V7 interface suggests the clients limit the data they send to large but well known set of values, those fields should be validated prior to sending V7 messages.

This is the same recommendation as for a LIS.

As with a LIS, failure in this validation should be a suggestion to change, but the Subscriber can proceed with validation without accepting this suggestion.

Recommendation: When the V7 response contains address alternatives, the GUI should display all of the alternatives.

If the Subscriber selects one of the alternatives, there is no need to submit the selected address for validation, because the VDB will only return addresses that are valid.

5.10 V8 Interface

The V8 interface, in the context of the i2 Solution Migration architecture, defines the communication protocol and messaging between a VPC and an ERDB, or between ERBBs.

5.10.1 Technical Description

The V8 interface is between a VPC and the ERDB or between ERDBs. The ERDB is the entity that stores the boundary information for emergency service zones. The ERDB should be able to accept

queries that contain geo-spatial or civic location information. When queried with location information, it returns the ESRN, routing ESN, MSAG formatted civic address (if queried with civic location information) and CRN, if available, which is used for contingency routing. In addition, the ERDB may also return an administrative ESN via the V8 interface, if one is included in the routing information associated with the caller's location.

5.10.2 Messages

A Request/Response message pair is defined here to allow a VPC to send a routing query to an ERDB that contains information describing the emergency caller's location (or to allow an ERDB to forward a routing query received from a VPC to another ERDB), and to support the return of the associated routing information by the ERDB. XML messages are used to support this information exchange, with NENA tags utilized for conveying Civic and Geo-location information to the ERDB.

5.10.2.1 ERDBRequest – Request Routing Information

For the query, the ERDBRequest is expected to contain either geographical coordinates, civic address information or both civic and geographical location information. The ERDBRequest can be to a local ERDB that contains the ESZ information nation wide or it can be a remote ERDB that serves a specific geographical area. The location information provided to the ERDB in the query is derived from the LO obtained by the VPC.

Table 5-28 - ERDBRequest Parameters

Parameter	Condition	Description
message-id	Mandatory	This parameter uniquely identifies the query at the VPC
source	Mandatory	Identifies the node directly requesting routing information from the ERDB
vpc	Conditional	Identifies the VPC that originally requested the routing information
geolocation	*Conditional	WGS84 coordinates derived from LO
civiclocation	*Conditional	Validated address passed in LO
datetimestamp	Optional	The datetimestamp parameter carries the date and time of the message generation described using UTC
destination	Optional	Identifies the ERDB from which routing information is being requested

* One of these must be present, it is possible that both these elements may be present

message id – The Message ID parameter uniquely identifies the query at the VPC
The <*source*> element identifies the node directly requesting emergency call routing information from the ERDB over the V8 interface. It includes the source node (hostname), a NENA administered identifier (nena-id) a 24x7 contact number (contact), and an optional uri (cert-uri) provide a link to the provider's VESA issued certificate. The <*source*> must be a trusted entity of the ERDB.
source format:

```
<source>
        <organization-name> Noname VPC</organization-name>
    <hostname>cs34.example.com</hostname>
    <nena-id>nena1</nena-id>
    <contact>tel:+398348975439823</contact>
    <cert-uri>https://vpc34.example.com/certificate.crt</cert-uri>
</source>
```

The <nena-id> and <contact> fields are mandatory while all the other fields of the <source> element are optional.

The <vpc> element identifies the VPC that is requesting the routing information from the ERDB. In cases where the routing request is steered from one ERDB to another, the <vpc> element would identify the VPC requesting the routing information whereas the <source> element would identify the ERDB that is steering the request.

vpc format:

```
    <vpc>
        <organization-name> No Name VPC </organization name>
    <hostname> vpc.example.com</hostname>
    <nena-id> NENA911</nena-id>
    <contact>tel:+398348975439823</contact>
    <cert-uri>https://vpc.example.com/certificate.crt</cert-uri>
</vpc>
```

The <nena-id> and <contact> fields are mandatory while all the other fields of the <source> element are optional

geolocation – The ERDB requires WGS 84 format so this may require the VPC to convert the coordinate information, if received, to WGS84. The two other coordinates systems discussed to date are NAD 83 and NAD 27 (HARN). Altitude, if included in the location, is not included in the query to the ERDB. When present in the location, it is used to obtain the routing information, even when both parameters exist.

civiclocation – The Civic Location format is currently defined in the PIDF-LO. The mapping of PIDF-LO parameters to NENA format may be required. The Civic Location is expected to be in form that will enable the ERDB to transform the address into a MSAG-valid formatted address.

datetimestamp – The datetimestamp parameter carries the date and time of the message generation described using UTC.

The <*destination*> element identifies the ERDB from which routing information is being requested. It includes the source node (hostname), a NENA administered identifier (nena-id) a 24x7 contact number (contact), and optional parameters for the organization's name and uri (cert-uri) for the operator's VESA issued certificate.. The <*destination*> must be a trusted entity of the VPC/ERDB. Destination format:

```
<destination>
      <organization-name>ERDB Provider</organization-name>
      <hostname>erdb34.example.com</hostname>
      <nena-id>nena1</nena-id>
      <contact>tel:+398348975439823</contact>
      <cert-uri>https://erdb.example.com/certificate.crt</cert-uri>
</destination>
```

5.10.2.2 ERDBResponse – Routing Response

The response message assumes the responding ERDB has been determined.

Table 5-29 - ERDBResponse Parameters

Parameter	Condition	Description
message id	Mandatory	Uniquely identifies the query at the VPC
source	Mandatory	The identifier of the node directly responding to the routing query over the V8 interface
erdb	Conditional	The identifier of the ERDB that is the original source of the routing information
esrn	Conditional	Routing number to ESGW and correct trunk group. Expected E.164 format.
routingesn	Conditional	Identifies the ESN to be used in routing the emergency call to the correct PSAP
adminesn	Conditional	Identifies the administrative ESN associated with the LO in the query
crn	Conditional	Contingency 24x7 E.164 phone number to use when unable to route using the ESRN.

alternateerdb	Conditional	Indicates the address of the ERDB which might have the routing information being requested
msagvalidcivicaddress	Conditional	Carries the MSAG valid formatted civic address provided by the ERDB
result	Mandatory	Indicates the success or error in responding to the query
datetimestamp	Optional	The datetimestamp parameter carries the date and time of the message generation described using UTC
destination	Optional	The identifier of the node requesting the routing information

message id – The Message ID parameter uniquely identifies the query at the VPC
The <*source*> element identifies the node directly responding with emergency call routing information over the V8 interface. It includes the source node (hostname), a NENA administered identifier (nena-id) a 24x7 contact number (contact), and an optional uri (cert-uri) provide a link to the provider's VESA issued certificate.
source format:

```
<source>
        <organization-name> Noname ERDB</organization-name>
    <hostname>erdb34.example.com</hostname>
    <nena-id>nena1</nena-id>
    <contact>tel:+398348975439823</contact>
    <cert-uri>https://erdb34.example.com/certificate.crt</cert-uri>
</source>
```

The <*erdb*> element identifies the node that is the source of the routing information. In some cases the <erdb> element will be coded with the same information as the source element. In cases where ERDB steering occurs, the <erdb> element will be coded with the identity of the ERDB from which the routing information was obtained. It includes the source node (hostname), a NENA administered identifier (nena-id) a 24x7 contact number (contact), and an optional uri (cert-uri) provide a link to the provider's VESA issued certificate.

erdb format:

```
    <erdb>
        <organization-name> No Name 1 ERDB </organization name>
    <hostname> erdb1.example.com</hostname>
    <nena-id> NENA911</nena-id>
    <contact>tel:+398348975439823</contact>
```

```
        <cert-uri>https://erdb1.example.com/certificate.crt</cert-uri>
</erdb>
```

esrn – This is the number used to route the call to the appropriate SR over the correct trunk group from the ESGW. The format in i2 is expected to be an E.164 PSTN number

routingesn – The routing ESN is associated with a particular ESZ for a given PSAP that has a unique combination of Police, Fire and Medical emergency responders. This ESN will ultimately be used by the SR to identify the appropriate PSAP for the emergency call. The format is expected to be an integer, 5 digits in length.

adminesn - The Administrative ESN parameter is coded with the administrative ESN that is associated with the location information that is received in the query, when this information is available. It is associated with a particular set of English Language Translations for an ESZ in a PSAP that are stored by the ALI Database.

crn – This is the PSAP 24 x 7 emergency number that can be used to route the call in times of network failure. The format is expected to be an E.164 PSTN telephone number.

alternateerdb – This parameter allows the ERDB to indicate the address of an alternate ERDB when it does not have the routing data being requested but knows the address of the ERDB where the routing data can be found. This parameter is expected to be in the form of a uri.

msagvalidcivicaddress – This parameter carries the MSAG-valid formatted civic address provided by the ERDB. As previously described, the ERDB is expected to convert a received civic address into an MSAG valid format that can be presented at the PSAP. This parameter is expected to be sent only if a civic location is received in the ERDBRequest message.

result - The result parameter carries an indication of whether the ERDB was able to provide routing information and the means by which routing information was determined. If no routing information was provided, this parameter could be used to determine the cause of the problem. Table C lists and describes the codes that should be used.

datetimestamp– The datetimestamp parameter carries the date and time of the message generation described using UTC.

The <*destination*> element identifies the node that directly requested emergency call routing information . It includes the source node (hostname), a NENA administered identifier (nena-id) a 24x7 contact number (contact), and optional parameters for the organization's name and uri (cert-uri) for the operator's VESA issued certificate. The <*destination*> must be a trusted entity of the VPC/ERDB.
Destination format:

```
<destination>
      <organization-name>vpc Provider</organization-name>
```

```
      <hostname>vpc.example.com</hostname>
      <nena-id>nena1</nena-id>
      <contact>tel:+398348975439823</contact>
      <cert-uri>https://vpc.example.com/certificate.crt</cert-uri>
</destination>
```

Table 5-30 - Result Codes

Value	Name	Description
200	SuccessGeodetic	This value indicates that the ERDB was successful in determining routing information using the received Geo Location information
201	SuccessCivic	This value indicates that the ERDB was successful in determining routing information using the received Civic Location information
400	ErrorBadLocation	This value indicates that the ERDB was unable to provide routing information because the received location information was bad
401	ErrorNoLocation	This value indicates that the ERDB was unable to provide routing information because the no location information was received in the query
402	ErrorAlternateERDB	This value indicates that no routing information exists for the location provided but indicates the address of an alternate ERDB that might contain the appropriate routing information is being returned
403	ErrorBadMessage	This value indicates that routing information was not provided because the query received was corrupted

404	ErrorAuthorization	This value indicates that routing information was not provided because the query failed authentication
500	ErrorGeneral	This value indicates that a general error occurred and the ERDB is unable to return routing information

5.10.3 Security

The V8 interface will need to operate in a variety of network environments, some trusted, and some not as described in previously. V8 is a XML-based interface and should be used with a suitable security mechanism as defined in Section 3. When the connection between the VPC and the ERDB is not a trusted network, both the VPC and ERDB are expected to be protected with IPSEC or TLS, and thus require a certificates rooted in VESA. Even in a trusted network, TLS protection is advisable. Mutual authentication is required when cryptographic security is deployed.

6 Roles and Responsibilities

The organizational components of the i2 solution refer to those entities, commercial or public, which operate the various network elements in this architecture. For example, there are those entities that are responsible for the operation of a Call Server, those entities that are responsible for the operation of an ESGW, and those entities that are responsible for the operation of a Selective Router. In practice these entities may have responsibility for one or more instances of these network elements and may have a scope which is considerably larger than just the operation of i2 defined network elements. Thus, the entities defined here are logical ones – the key in recognizing whether any of the roles associated with these entities apply to any given real world party, is whether that party has specific ownership and responsibility for the effective operation of the corresponding network entity. Similarly the implementation of a specific logical network element may be such that various components of the implementation are shared by more than one entity. In this case the owning entities are jointly responsible and individually answerable for the effective operation of the network element constituted by that implementation.

- **Caller** – Operates the device from which the call is made and initiates the call to emergency services.
- **VoIP Service Provider (VSP) –** Operates the network equipment that provides call processing for subscribers.
- **Redirect Operator –** Operates redirect server(s).
- **Proxy Operator –** Operates proxy server(s).
- **LIS Operator** – Operates the LIS associated with the IP access network used by the callers.
- **ESGW Operator** – Operates emergency service gateway(s).
- **SR Operator** – Operates the Selective Router(s) corresponding to specific local exchange areas.
- **PSAP Operator** – Operates the Public Safety Answering Points in a particular county, state, or other regional jurisdiction.
- **ALI Operator** – Operates the Automatic Location Identification infrastructure used to provide caller information associated with a pANI offered in a query from a PSAP.
- **VPC Operator** – Operates VPC network element(s).
- **Credential Authority** – An authority responsible for supporting the infrastructure to assign and revoke electronic digital certificates to i2 network entities.
- **Routing Number Authority (RNA)** – An authority responsible for distributing ranges of numbers to network operators for the purposes of call routing and query steering.
- **MSAG Source** – Is responsible for defining, maintaining and publishing the master street address guide for a given coverage area.

- **Validation Database (VDB) Operator** – An operator that provides location information validation services to LIS operators and other users.
- **Emergency Service Zone (ESZ) Routing Database (ERDB) Operator** – An operator that supports the real time routing server that can resolve location information to emergency service zone route at the request of a VPC.
- **Root Discovery Operator (RDO)** - The operator that supports the well known root database from which the URI of the correct VDB or ERDB can be determined based on regional location information.

The different organizational entities, overlaid on their corresponding functional entities, are shown in the following diagram.

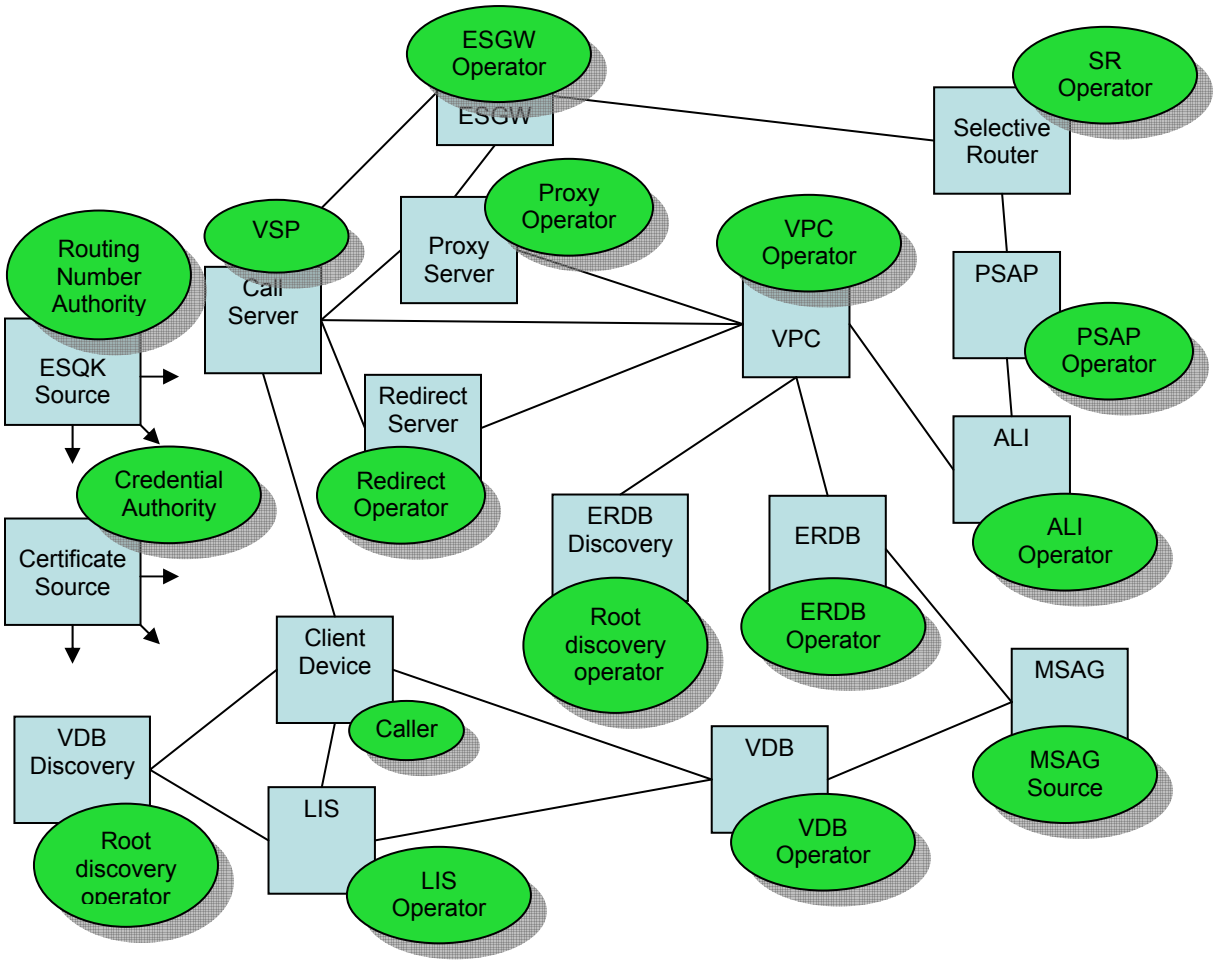


Figure 6-1 i2 Organizational Entities

6.1 Responsibilities

6.1.1 Caller

The caller is responsible for initiating the emergency call by inputting the appropriate emergency service number (e.g., "9-1-1"). For the call to be correctly routed and have location presented to the operator, the caller is responsible for utilizing a combination of access network and device which can ensure that location information, which is validated to the necessary level, is made available to the i2 network for processing. Arbitrary VoIP devices utilized on arbitrary access networks may not provide sufficient functionality to be properly supported by the i2 network and last resort routing, or even failure to deliver the call to any emergency operator, may occur. This requirement applies whether the caller is an individual on a public network or calling from within a managed enterprise.

The caller may also be known as the subscriber. The caller is the individual initiating the actual emergency call. The subscriber is the individual who nominally owns the device and service subscription. The subscriber, regardless of individual caller, has the responsibility to ensure that a properly equipped device as described above is available. The terms "caller" and "subscriber" may be used relatively interchangeably in the document text depending on context.

6.1.2 Voice Service Provider

The voice service provider (VSP) operates the call server which is directly utilized by the caller to initiate the emergency call on the V1 interface. It is the VSP's responsibility to ensure that their call server(s) can appropriately identify that an emergency call has been invoked by the caller and to initiate appropriate call handling. This appropriate handling will be one of the following

- Identify and query an appropriate VPC to obtain routing information for the call and direct the call to the ESGW indicated by that routing information through support of the V2 and V4 interface definitions.
- Identify an appropriate redirect server and direct the call toward it and subsequently route it as determined by that redirect server utilizing the V5 and V4 interfaces.
- Identify an appropriate proxy server and direct the call to that server utilizing the V6 interface.

The VSP is responsible for ensuring that its call server(s) are correctly configured to identify the correct VPC, ESGW, redirect, or proxy servers depending on options used. VSPs are responsible for ensuring their call server(s) have access to the other network entities, whichever options are used, such that all geographic areas from which their callers can initiate calls and which are accessible via the i2 architecture, are serviced. This may be by their own means or by the establishment of commercial or other arrangements with the operators of VPC, redirect, proxy, and ESGW server entities.

6.1.3 Redirect Operator

The redirect operator maintains redirect server(s) and provides access to authorized call servers which are in receipt of an emergency call using the V5 interface definitions. The redirect operator is responsible for ensuring that redirect server equipment has access to VPC functionality that can provide routing direction for all areas from which their VSP user base can originate calls.

6.1.4 Proxy Operator

The proxy operator maintains proxy server(s) and provides access to authorized call servers which are in receipt of an emergency call using the V6 interface definitions. The proxy operator is responsible for ensuring that it can determine the appropriate routing information by accessing relevant VPC functionality, and that it has access to the necessary ESGW infrastructure to deliver calls for those areas.

6.1.5 LIS Operator

This operator is associated with a particular IP network access area. The LIS operator is responsible for providing an operating infrastructure which supports requests for location information by individual end user devices (UA) and/or properly credentialed network elements (e.g. VPC) over the V0 and V3 interfaces respectively. The LIS operator is also responsible for providing technologies and processes which ensure that the geographical location information provided with respect to users is correct to within a specified range of accuracy. Where the location is effectively constrained to a specified range, as determined by other standards, regulatory rulings, contract, etc, LIS operators are responsible for providing a Civic Address corresponding to that location when one is applicable. LIS operators are responsible for ensuring that this Civic Address information is properly and independently validated with an appropriate VDB to ensure successful resolution of destination when that address is used to route emergency calls.

6.1.6 ESGW Operator

The ESGW operator provides the equipment to interface between the IP network and the legacy circuit switch-based emergency network. The ESGW operator is responsible for providing sufficient and reliable capacity for the delivery of emergency calls to the Selective Router network elements in their area of coverage. ESGW operators are responsible for ensuring that calls are placed on the correct trunks based on the ESRN provided in emergency call setup signaling and in accordance with the guidance of the corresponding SR operator as to which trunks correspond to which values of routing information. ESGW operators are responsible for ensuring that the call server operators to whom they provide service are informed which ESRNs are applicable to which ESGW instances that they operate. The ESGW operator is also responsible for ensuring that the infrastructure that they operate provides the correct default, contingency, and congestion routing mechanisms as specified by the selective router operators, PSAP operators or other authorities as applicable to the area of service. ESGW operators are also responsible for maintaining a call record system which, upon request from the selective router operator, will allow them to identify the call server operator from which a given

call originated, identified by time and ESQK. They must support the necessary mechanisms to block delivery of calls from specific call server operators to specific destinations at the request of selective router operators.

6.1.7 Selective Router (SR) Operators

These operators provide the infrastructure to deliver calls arriving on trunks from ESGW network elements to the correct serving PSAP based on the routing information in the call setup signaling. They provide the equipment to adapt to the signaling and voice bearer media (e.g. CAMA) used by the PSAP CPE. This equipment maintains the call state between the SR and the PSAP and responds appropriately to mid-call commands such as call transfer requests to emergency responders. The SR operator is responsible for ensuring that correct default, contingency, and congestion call routing functions are configured for all incoming ESGW trunks. They are responsible for ensuring that ESQK entries in the Selective Routing Database (SRDB) are configured to support call delivery to the correct PSAP, selective transfer, etc. based on the correct ESN associations. SR operators are responsible for working with the VPC operator either directly or through the MSAG administrator to ensure that ESQK block assignments are correctly associated with the appropriate ESRN/ESN combination. SR operators are responsible for providing the correct information associated with unique routing data to ESGW operators that connect to the SR(s) such that those operators can provision the correct trunk, default, contingency, and congestion routing data against each ESRN in their systems.

6.1.8 PSAP Operators

PSAP operators provide the call center resources which take and assess emergency calls to determine appropriate handling of the call. They are responsible for connecting the caller to the correct first responder organizations when necessary. They are responsible for ensuring that they operate the necessary CPE with associated staffing capacity and reliability to serve the volume of calls originating in their serving area. They are responsible for ensuring that they have the necessary CPE to query ALI equipment and receive and display call related information including the caller's location.

PSAP operators provide direction in terms of the correct default routing for calls that the network needs to support. They may also have a role in specifying the necessary ESQK block allocation sizes on a per ESZ basis.

6.1.9 ALI Operator

ALI operators provide the infrastructure to PSAP operators to retrieve the location, ESN information, and other call related information based on the query key that was provided for the call.

The ALI operator is responsible for providing an electronic query interface to PSAP operator CPE. All valid query keys presented on that interface must be matched to the related call information, including location, and presented back to the PSAP. In the case of i2 related requests, the local ALI operator must ensure that the request is steered to the

appropriate VPC over the V-E2 interface. ALI operators are responsible for providing a reliable real-time infrastructure which can identify the correct VPC to which to steer the query based on the presented ESQK, format a valid ESPOSREQ message and to receive and process the esposreq response. The ALI operator is responsible for ensuring that the ALI database maintains correct ESQK to VPC steering data such that any valid ESQK presented as a query key can be matched to an appropriate VPC. The steering data must be sourced from the VPC operator. ALI operators are responsible for maintaining records of queries to facilitate historical analysis including identification of calls by time and ESQK assignment, and content and status of request/response messages as they occurred.

ALI operators are responsible for ensuring that the responses received from the VPC are correctly formatted and presented to the PSAP CPE.

6.1.10 VPC Operator

The VPC operator provides robust infrastructure which allows the routing information for a given emergency call to be determined based on the location of the caller, and maintains the call information, caller location information, and corresponding ESN information, based on the information received from the Call Server/Proxy via the V2 interface, from the ERDB via the V8 interface, and from the LIS via the V3 interface (if applicable). The VPC operator will be responsible for having mechanisms in place to respond to ALI queries for location information. VPC operators will also be responsible for ensuring that any MSAG-valid formatted civic location information received from the ERDB in response to a routing query is included in the response to the ALI database. In addition, they are responsible for ensuring they have the infrastructure in place to direct location queries to any applicable LIS interface when presented with a location key.

The VPC operator is responsible for ensuring that the VPC equipment supports compatible E2 interface capabilities to support ALI queries. The VPC operator must ensure that the necessary processes and mechanisms are in place to obtain ESQK allocations from the RNA, to determine the correct ESRN to ESQK sub-block associations, and to make the E2 interface connections accessible from authorized ALI operators. Where it is required to do so, the VPC operator must also ensure that the ESQK allocations appropriate to each of its VPC instances is communicated to the ALI operator in order that they can maintain a correct VPC steering database.

VPC operators are responsible for ensuring that any PSAP policies on call handling are applied with respect to default routing when location information source cannot be verified, or where location information type (geodetic and/or civic) or content is limited. The VPC operator is responsible for ensuring that last resort routing data is defined and that equipment is configured to provide this information in response to V2 interface queries when no more applicable route can be identified for the call.

VPC operators are responsible for maintaining 24x7 telephone response service such that PSAP operators can contact them for details of a particular call in the event of failure of

an ALI query or in order to determine the identity of the originating call server operator and to facilitate communication with that operator in the event of needing assistance with making contact with the caller. The VPC operator is also responsible for maintaining historical records of all calls such that similar investigations can be conducted at arbitrary points in the future.

6.1.11 Credential Authority

The credential authority is responsible for providing certificates to appropriately qualified call server, VPC, ESGW, LIS, ERDB, SR and VDB operators. These digital certificates are to be provided as and when they are needed to ensure that authentication can occur over the i2 defined interfaces and so that location information can be digitally signed and checked for source of origin by network elements within the i2 architecture.

It is the responsibility of credential authorities to ensure that certificates are securely generated, distributed, and maintained. Where necessary, they are also responsible for the withdrawal and cancellation of certificates.

Two types of credential authority are defined – VESA and the delegate authorities.

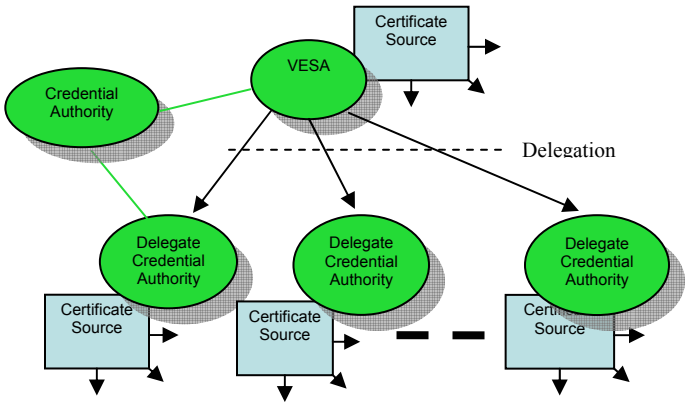


Figure 6-2 Organizational Decomposition – VESA and Delegate Credential Authorities

6.1.11.1 Valid Emergency Services Authority (VESA)

This organization is the root source of all certificates. It is responsible for identifying and issuing certificates either directly to end using entities or through delegate credential authorities. It is responsible for ensuring that any delegate credential authority that it identifies is properly qualified and operating with sufficient security and legitimacy to perform this role. Where VESA issues certificates directly to end users, it also has the responsibilities of a delegate credential authority in those cases.

VESA is also responsible for maintaining a master revocation list for all end entities that have had their certificates revoked for any reason. It must provide a means for the delegate credential authorities to populate the list. This list must be made available electronically to all organizational entities which need to validate data based on VESA root certificates.

6.1.11.2 Delegate Credential Authorities

A delegate credential authority issues certificates, which are derived from VESA certification. It is responsible for issuing certificates to the operators of network entities that utilize VESA certificates for the exchange of authenticated data on the i2-defined interfaces.

Delegate credential authorities are responsible for ensuring that the organizations involved in the i2 architecture are properly equipped in infrastructure and operating processes to meet the demands of reliable emergency call delivery and processing from VoIP networks before issuing certificates. They should operate an appropriate process of assessment and renewal audit, in order to assess these organizations and validate their suitability to participate in the i2 network. Part and parcel of this responsibility is the generation and provision of electronic digital certificates which are required for the purposes of authentication and authorization between the various network entities comprising the i2 architecture.

Delegate credential authorities are also responsible for identifying when a given certificate needs to be revoked (where an entity no longer meets the requirements of eligibility for the certificate – for example, when it ceases operation). When a certificate is identified as being revoked or expired, this information must be communicated to the VESA so the certificate can be included in the master revocation list.

Examples of delegate credential authorities may be PSAP operators, state emergency authorities, or regional 9-1-1 service providers.

6.1.12 Routing Number Authority (RNA)

The RNA is responsible for distributing ranges of numbers from a reserved number space to properly credentialed network element operators for the purposes of call routing and query steering.

The RNA issues multiple discrete blocks of ESQK allocations to VPC operators from a reserved numbering space defined for this purpose. The routing number authority is responsible for ensuring the uniqueness and correctness of the numbers allocated and the corresponding information associated with each number. They are responsible for ensuring that the VPC instances against which allocations are made are properly credentialed and approved to provide emergency call routing service. They are also responsible for polling these organizations to ensure that they are still credentialed and, where necessary, for reclaiming ESQK allocations from VPC operators as VPCs go out of service.

6.1.13 Master Street Address Guide (MSAG) Source

The MSAG source represents the organizational components that are responsible for performing the division of an emergency coverage area into the individual emergency service zones (ESZ), and the association of ESN lists to those zones. The ESZ must be defined in terms of civic address boundaries incorporating the necessary postal and 9-1-1 field formatting. The definitions may further support the division by geo-spatial boundaries[20]. The MSAG source is required to make this information available to authorized ERDB operators, VDB operators, PSAP and SR operators and any other concerned parties who require this fundamental information. The MSAG source is expected to have the necessary infrastructure in place to ensure that the MSAG data is kept current and that updates are made available in an electronic form to authorized parties in a timely fashion. The MSAG source can be devolved into two specific organizational entities.

20 Note that in order to support future devices that may only be able to be provide location as a geodetic location (e.g., devices that support IETF RFC 3825 or mobile wide area wireless Internet access devices), there needs to be a geospatial boundary equivalent of the MSAG. As in the case of cellular, the logical ESZ boundary may be of lower resolution, for example it may be the PSAP boundary, in which case the ESN associated with this logical ESZ would indicate "query caller" as it does for cellular telephony access.

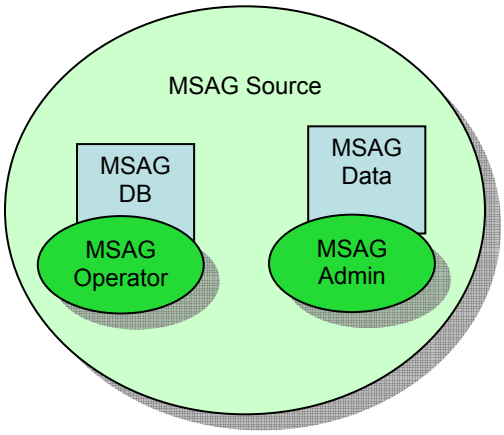


Figure 6-3 Organizational Decomposition - MSAG Source

6.1.13.1 MSAG Administrator

The MSAG administrator is the component of the MSAG source that is responsible for determining, documenting, and maintaining the actual MSAG data. This includes the local level activities to understand ESZ boundary break downs and associated ESN lists. The MSAG Administrator is responsible for maintaining the civic data in the MSAG. The MSAG Administrator is also responsible for creating and maintaining the geo-spatial representation of ESZ boundaries. They are responsible for liaising with the SR operators in the area of coverage to assist the SR operators in determining which ESRN values correspond to the ESZ allocations. They provide the data to the MSAG operator for the actual electronic storage and distribution of the MSAG data.

6.1.13.2 MSAG Operator

The MSAG operator maintains the database equipment and infrastructure that supports the access and retrieval of the MSAG data by authorized parties. They must provide the necessary infrastructure for the MSAG administrator to ensure that the data can be updated. They must ensure that the database itself remains reliable, uncorrupted, and secure from unauthorized access. The MSAG Operator that provides access to the civic data of the MSAG may be different from the MSAG Operator that provides access to the geo-spatial ESZ boundary data for the MSAG.

6.1.14 Validation Database (VDB) Operator

The VDB operators are responsible for providing the service by which LIS operators and other authorized categories of users in their area of operation can submit access network location information over the V7 interface for validation. Validation checks will ensure that the location information will successfully key into the current MSAG in support of call routing. VDB operators are responsible for providing an effective electronic means of performing validation and providing assistance in correcting non-valid information. They must ensure that the validation occurs against the current version of the MSAG.

They are responsible for ensuring that the root discovery operator is informed of the availability of their service and the regional coverage it provides to support reliable discovery by users. When changing the URI of their infrastructure, they are responsible for ensuring that old URIs are maintained for an overlap period and the RDO is informed of the associated expiry and activation times.

The VDB operator should liaise with neighboring operators and resolve areas of overlap based on regional coverage as identified in the root discovery information (see section on RDO). That is, where ambiguity may arise in the root discovery data because of sub-municipality splits in VDB operator coverage, the operator should make arrangements to proxy validation requests or return the identity of the alternate for these areas of overlap.

6.1.15 Emergency Routing Database (ERDB) Operator

The ERDB operators are responsible for ensuring that reliable infrastructure with the necessary performance to support real time routing queries over the V8 interface is available to authorized VPC operators. They must ensure that the routing queries can occur using either the civic address or geodetic boundary information contained in the MSAG that corresponds to the location in the query.

The ERDB operator is responsible for working with SR operators, PSAP operators and other parties as necessary to ensure that ESZ boundaries are associated with correct ESRN values that will be used as the basis of call routing and that the correct ESRN is provided in response to a routing request. They are responsible for ensuring that the US postal address format for civic address keying of the routing database has a corresponding correct MSAG format for providing to the VPC in the V8 interface routing response.

They are responsible for ensuring that the root discovery operator is informed of the availability of their service and the regional coverage it provides in order that they can be reliably discovered by users. When changing the URI of their infrastructure, they are responsible for ensuring that old URIs are maintained for an overlap period and the RDO is informed of the associated expiry and activation times.

The ERDB operator should liaise with neighboring operators and resolve areas of overlap based on regional coverage as identified in the root discovery information (see section on RDO). That is, where ambiguity may arise in the root discovery data because of sub-municipality splits in ERDB operator coverage, the operator should make arrangements to proxy routing requests for these areas of overlap. The ERDB operators are responsible for maintaining records of all routing requests including results and status against time and the identity of the requesting VPC entity.

6.1.16 Root Discovery Operator (RDO)

This is a singleton organizational entity in the architecture. That is, it is assumed that the functions supported by this entity can be accessed by a single well known network

address (URI). The RDO is responsible for maintaining and making available the identities of the key VDB and ERDB functions in the network. This information is to be maintained as current and made available to all requesting entities. The RDO is responsible for ensuring that updated versions of the data with specific activation and expiry times are available. New versions of data must always be made available before current versions expire. The RDO is not responsible for discovering ERDB and VDB operators itself, but it is responsible for providing the means to have discovery information reliably communicated by those entities in an electronic form. The RDO is responsible for consolidating the discovery information as received by all VDB and ERDB operators, negotiating coordinated activation and expiry intervals, and making this consolidated information available for access over the V9 interface. The RDO can be organizationally devolved into the ERDB RDO and the VDB RDO as these functions have discrete user bases and separate root URI values may be assigned to each function.

7 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-05

[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] TIA-TSB-146, *IP Telephony Support for Emergency Calling Service*

[11] NENA 02-010, *NENA Standard Format and Protocols For ALI Data Exchange, ALI Response and GIS Mapping*

[12] Internet draft, *Requirements for Session Initiation Protocol Location Conveyance*, October 2004, draft-ietf-sipping-location-requirements-02

[13] NENA 05-001, *Implementation of the Wireless Emergency Service Protocol E2 Interface*

[14] IETF RFC 2313, *PKCS #1: RSA Encryption, Version 1.5,* March 1998

[15] IETF RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, April 2002

[16] FIPS PUB 197, *Advanced Encryption Standard*, November 2001

[17] IETF RFC 2401, *Security Architecture for the Internet Protocol*, November 1998

Appendix A -ALI Changes

Purpose

Provide list of potential system changes required for implementing I2 solution.

Overview

The initial I2 deployment will be similar to Wireless Wireline Compatibility Mode as specified in J-STD-036. The VoIP provider will deliver an ESQK into the 9-1-1 Network. The PSAP will query the local Emergency Services Message Entity, the ALI system, with the ESQK. Once the ESME receives the ESQK from the PSAP it will query the VoIP Positioning Center, VPC, using the E2+ message format as implemented over the V-E2 interface. This implementation approach may necessitate software changes to an ESME that is currently supporting an E2 NCAS deployment only.

The E2 NCAS deployment allows for the delivery of the Call Back Number and Emergency Services Routing Digit to the PSAP (Format B within J-STD-036-B). In the E2 NCAS deployment the caller's geo location is obtained from the Mobile Positioning Center and the data associated with the Emergency Services Routing Digits, as stored within the ESME, is used for the cell site address. This differs from a deployment that uses the E2+ message format. When the E2+ message format is used the VPC is responsible for delivery of the Call Back Number and will place the civic address of the VoIP caller into tagged fields of the E2+ Location Description parameter.

Potential Changes Required to Support i2 Solution

The following list is informative. The Pubic Service Agency should consult with their 911 System Service Provider to obtain an analysis of the potential changes required for implementing I2 solution. This text is meant to be used for discussion between the PSAP and the ALI provider.

- Implement E2+ query based on ESQK. ESQK shall be placed into the ESRK field of Emergency Services Protocol message. Since the ESQK will have the same form and function as the ESRK, there will be no change to the existing ESRK field.

- Implement parsing of tagged fields in the E2+ Location Description parameter into the ALI format.
    - Determine if any E2+ fields should not be used.
    - Determine approach for using ESN returned in E2+ response and how agency names will be displayed.
    - Review the <LOC> tag and any data elements delivered in this field.
        - Determine if any conflict exists with existing ALI format.
    - Determine if there are any embedded labels in the ALI format that may need to be accounted for when parsing the VoIP data.

- Review VoIP Class of Service values and determine if any changes need to be made in call detail reports or Computer Aided Dispatch systems.
- Determine if the E2+ Position Source or ALI ESQK shell record shall be used to create a VoIP Class of Service.
    - Ensure that the VoIP Position Source value(s) are NOT interpreted as wireless values.
- Determine if the existing ALI format has any conflicts for displaying Geo Location and Civic Location fields at the same time. This may be an issue if your existing ALI format has multi use fields.
    - Determine if a VoIP position source or Class of Service can be used to prioritize when a Geo Location or Civic Location should be displayed.
- Determine if there is a need for additional ALI text messages.
    - ESME should have the ability to distinguish when steering is done to a MPC or a VPC. This will be necessary to ensure wireless text messages are not created for VPC responses.

Appendix B Rules for Address Abbreviation

Resources for Abbreviation Matching

USPS Publication 28 can be found at the following link:
http://pe.usps.gov/cpim/ftp/pubs/Pub28/pub28.pdf
The Canadian Postal Guide can be found at the following link:
http://www.canadapost.ca/business/offerings/address_management/pdf/addressing_guide-e.pdf

The following table is excerpted from USPS Publication 28 to show variations in Street Suffix Abbreviations. The suffix name of AVENUE was picked for illustration purposes only.

Primary Street Suffix Name	Commonly Used Street Suffix or Abbreviation	Postal Service Suffix Abbreviation
AVENUE	AV AVE AVEN AVENU AVENUE AVN ANVUE	AVE

Table 1: Street Suffix Abbreviation (taken from USPS Pub 28, Appendix C for illustration purposes)

The VDB MUST be able to translate AV, AVE, AVEN, AVENU, AVENUE, AVN and ANVUE to the USPS accepted abbreviation of AVE.

Address received over the V7	Result Code	Address contained in the MSAG and returned over V-E2	Address returned over the V7
OAK AVE	100 (Success)	OAK AVN	OAK AVE
OAK AV	102 (Alt returned)	OAK AVN	OAK AVE
Oak Ave	102 (Alt returned)	OAK AVN	OAK AVE
OAK AVE.	102 (Alt returned)	OAK AVN	OAK AVE

Table 2: Examples of Street and Street Suffix Names as input/outputs over V7

Additional Validation Functionality

The VDB may optionally do more than matching based on a standardized list. For example, if a VDB receives "AVINU", it could decide to associate and return AVE in the V7 response. The limit of this VDB functionality should be incumbent on the specific implementation.

Appendix C – MSAG to Postal Address Comparison

This appendix is provided for informational purposes only. The intent of the appendix is to illiustrate the fact that postal addresses and MSAG addresses are very often different and it is the MSAG address which is required to ensure proper dispatch at the PSAP.

Information for VDB Developers

Example using actual MSAG data; postal addresses were looked up at http://www.satorisoftware.com/US/addresscheck/AddressCheck.asp.

These are just some customer address examples pulled at random from MSAGs around the country (no searches were done to find examples likely to not match to Postal addresses). Based on this tiny sample it appears that conformity to Postal addresses is going to vary widely from MSAG to MSAG with most MSAGs being very different from the Postal.

Variations of Andover in MSAG (each of these variations will have a different set of valid streets and addresses associated with them):

Community	County	State
ANDOVER BORO	SMST	NJ
ANDOVER BORO	SUSX	NJ
ANDOVER TWP	SUSX	NJ

MSAG Address	Postal Address	Comment
18 AMBLER LANE ABERDEEN TWP, NJ	18 Ambler Ln Matawan NJ 07747-1225 County name: Monmouth	Note that Postal City does not match MSAG City. Postal lookup failed if zip not supplied using city name ABERDEEN TWP; worked without zip if TWP omitted.
1 CLIFFSIDE WAY ANDOVER TWP NJ	1 Cliffside Way Andover NJ 07821-5042 County name: Sussex	Note that Postal City does not contain TWP. Postal lookup failed if zip not supplied using city name ANDOVER TWP; worked without zip if TWP omitted.
400 US HWY NO 206 ANDOVER NJ	Lookup failed with or without zip	Mapquest returned: You searched for "400 us hwy no 206, andover, nj 07860", MapQuest did not find this exact address, but found one very

		similar: "400 Us Highway 206 S, Newton, NJ 07860-6002".
301 W 1ST AVE BARRINGTON BORO NJ	301 W 1st Ave Barrington NJ 08007-1206 County name: Camden	Postal lookup failed if zip not supplied using city name BARRINGTON BORO; worked without zip if BORO omitted.
17 AVENUE A ST NEWARK CITY NJ	17 Avenue A Newark NJ 07114-2661 County name: Essex	Note that Postal City does not contain CITY
2184 AZALEA AVE WALL TWP NJ	2184 Azalea Ave Sea Girt NJ 08750-2401 County name: Monmouth	Note that Postal City does not match MSAG City. The MSAG has a few streets in it for Sea Girt, NJ – Azalea Ave is not one of them. Postal lookup failed if zip not supplied using city name WALL TWP; worked without zip if TWP omitted.
10 ACADEMY DR E HANOVER TWP NJ	10 Academy Dr E Whippany NJ 07981-1801 County name: Morris	Note that Postal City does not match MSAG City. Whippany, NJ is not in the MSAG Postal lookup failed if zip not supplied using city name HANOVER TWP; worked without zip if TWP omitted
2948 HIGHWAY 72 E ABBEVILLE, ABB, SC	2948 Highway 72 E Abbeville SC 29620-5258 County name: Abbeville	
4216 TAYLOR CREEK RD AFTON, ALB, VA	4216 Taylor Creek Rd Afton VA 22920-2159 County name: Albemarle	
105 E HOLLAND ARCHBOLD, FUL, OH	105 E Holland St Archbold OH 43502-1210 County name: Fulton	
921 LIGHTHOUSE CHURCH RD BAKER, OKA, FL	Lookup failed with or without zip	Mapquest returned: You searched for "921 LIGHTHOUSE CHURCH RD, BAKER, FL 32531", MapQuest did not find this exact address, but found one very similar: "Baker, FL 32531".
132 BANDERA CIR BANDERA BAY, HEN, TX	132 Bandera Cir Mabank TX 75156-8920 County name: Henderson	Note that Postal City does not match MSAG City.
31496 330TH ST BARNARD, NOD, MO	31496 330th St Barnard MO 64423-8240 County name: Nodaway	

139 SAWYERS CREEK RD CAMDEN, CAM, NC	139 Sawyers Creek Rd Camden NC 27921-7507 County name: Camden	
32995 TERRACE VIEW RD CAPE KIWANDA, TIL, OR	Lookup failed with or without zip	Mapquest returned: You searched for "32995 Terrace View Rd, Cape Kiwanda, OR 97135", MapQuest did not find this exact address, but found one very similar: "Pacific City, OR 97135".
493 SIMCOE MTN RD CENTERVILLE, KLI, WA	493 Simcoe Mountain Rd Centerville WA 98613-2906 County name: Klickitat	
8620 N CR 800 E DECATUR, WLS, IN	Lookup failed with or without zip	Mapquest returned: You searched for "8620 N CR 800 E, DECATUR, IN 46733", MapQuest did not find this exact address, but found one very similar: "8620 N 800 E-90, Decatur, IN 46733-9202".
34 DUNKARD CHURCH RD DELAWARE TWP, HUNT, NJ	34 Dunkard Church Rd Stockton NJ 08559-1405 County name: Hunterdon	Note that Postal City does not match MSAG City.
1463 RD 51 E DIX, KIM, NE	1463 Road 51 E Dix NE 69133-8920 County name: Kimball	
1720 SCIOTO RD ELIZABETHTON, UNI, TN	1720 Sciota Rd Elizabethton TN 37643-1904 County name: Carter	Street name changed – counties are different; this is probably not a match Mapquest returned: You searched for "1720 SCIOTO RD, ELIZABETHTON, TN 37643", MapQuest did not find this exact address, but found one very similar: "Elizabethton, TN 37643-1904".
2261 COMERS ROCK RD ELK CREEK, GRA, VA		street number or box number out of range Mapquest returned: Map of the address
13228 US 24 EMERALD TWP, PAU, OH	13228 US 24 Cecil OH 45821-9401 County name: Paulding	Note that Postal City does not match MSAG City.

Appendix D – Issues under Investigation

This Appendix provides a list of issues that are still under consideration in the VoIP Migratory Work Group. The resolution of these issues may result in revisions to the i2 solution document. The issues that are currently on the VoIP Migratory group agenda as potential topics for further investigation are as follows –

- Delivery of ESQK and CBN to SR (20-digit delivery)
- Signaling of Geodetic information to the SR
- VDB/ERDB discovery mechanism using geodetic information
- Allowing VDB to return MSAG formatted address to LIS
- Requirements on VESA operator
- Requirements on ERDB/VDB discovery operator
- Delivery of Class of Service over V-E2 interface
- V0 Interface to Call Server
- Support of Layer 3/Layer 7 mechanisms for location acquisition.