# NENA Requirements for Location Information to Support Emergency Services

**DRAFT**

NENA Requirements for Location Information to Support Emergency Services
NENA 08-<to be assigned (tba)>, Issue 0, May 30, 2006 (DRAFT)

Prepared by:
National Emergency Number Association (NENA) VoIP Location WG

Published by NENA
Printed in USA

DRAFT

One Nation 9-1-1 One Number

## NENA STANDARDS

## NOTICE

The National Emergency Number Association (**NENA)** publishes this document as a guide to be used by designers, manufacturers and implementers of systems that will be used to provide location information needed for 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** recommends that members 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 shall not 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

DRAFT

Acknowledgments:

The National Emergency Number Association (NENA) VoIP Technical Committee Location WG developed this document.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

| **Members:** | **Company** |
|---|---|
| Nadine Abbott, WG leader | Telcordia |
| Deb Barclay | Lucent Technologies |
| Tim Barry | AT&T |
| Marc Berryman | Greater Harris County 9-1-1 |
| Guy Caron | Bell Canada |
| Marlys Davis | King County E9-1-1 Program |
| Martin Dawson | Andrew Corporation |
| Bob Gojanovich | HBF Group |
| Anna Hastings | Ameritech |
| Gary Hutchins | Intrado |
| Dick Khan | AT&T |
| Kim Leigh | Qwest |
| Marc Linsner | Cisco |
| Selena MacArthur | Time Warner Cable – Digital Phone |
| Roger Marshall | TeleCommunication Systems |
| Ken Maynard | Bexar Metro 9-1-1 Network District |
| Patti McCalmont | Intrado |
| Peter McHale | Verizon Wireless |
| David Morris | Verizon |
| Brian Rosen | Neustar |
| Edward Shrum | BellSouth |
| Barbara Stark | BellSouth |
| Nathan Wilcox | microDATA |
| James Winterbottom | Andrew Corporation |

DRAFT

# TABLE OF CONTENTS

**1 EXECUTIVE OVERVIEW ..... 6**

1.1 PURPOSE AND SCOPE OF DOCUMENT ..... 6
1.2 REASON TO IMPLEMENT ..... 7
1.3 BENEFITS ..... 7
1.4 OPERATIONAL IMPACTS SUMMARY ..... 7
1.5 DOCUMENT TERMINOLOGY ..... 8
1.6 REASON FOR ISSUE ..... 8
1.7 REASON FOR REISSUE ..... 8
1.8 DATE COMPLIANCE ..... 8
1.9 ANTICIPATED TIMELINE ..... 8
1.10 COSTS FACTORS ..... 8
1.11 COST RECOVERY CONSIDERATIONS ..... 8
1.12 ACRONYMS/ABBREVIATIONS ..... 9

**2 OVERVIEW ..... 9**

**3 TERMINOLOGY AND ASSUMPTIONS ..... 10**

3.1 TERMINOLOGY AND DEFINITIONS ..... 10
3.2 ARCHITECTURE ..... 12
3.3 ASSUMPTIONS ..... 13

**4 REQUIREMENTS ..... 14**

4.1 LOCATION DETERMINATION AND ACQUISITION ..... 14
4.2 LOCATION REPRESENTATION ..... 14
4.3 LOCATION SECURITY AND DEPENDABILITY ..... 15

**5 ADDITIONAL EVALUATION CRITERIA ..... 15**

**6 BIBLIOGRAPHY OF RELATED NENA DOCUMENTS ..... 16**

**7 EXHIBITS -- EXAMPLE SCENARIOS AND USE CASES ..... 18**

7.1 RESIDENTIAL CONFIGURATIONS ..... 18
*7.1.1 Residential/Mass Market Scenario – Location Capable IP Access Network ..... 19*
7.1.1.1 Use Case: User with Location-Capable IP Endpoint ..... 19
7.1.1.2 Use Case: User with Location-Incapable/Unaware IP Endpoint ..... 19
*7.1.2 Mass Market Scenario – Multiple Service Providers and LISs, Including Wireless Access Points ..... 20*
7.1.2.1 Use Case: User with Wireless Access Location-Capable IP Endpoint ..... 21
7.1.2.2 Use Case: User with Wireless Access Location-Incapable/Unaware IP Endpoint ..... 21
7.1.2.3 Use Case: User with Wireless Access Location-Measurement-Capable IP Endpoint ..... 21
7.2 ENTERPRISE CONFIGURATIONS ..... 21
*7.2.1 Scenario: VoIP- and Location-Capable Enterprise — Provides VoIP Services and Operates LIS(s) ..... 22*
7.2.1.1 Use Case: On-Site User with Location-Capable IP Endpoint ..... 23
7.2.1.2 Use Case: On-Site User with Location-Incapable/Unaware Endpoint ..... 23
7.2.1.3 Use Case: On-Site User with Wireless Access Location-Capable IP Endpoint ..... 24
7.2.1.4 Use Case: On-Site User with Wireless Access Location-Incapable/Unaware IP Endpoint ..... 24
7.2.1.5 Use Case: On-Site User with Wireless Access Location-Measurement-Capable IP Endpoint ..... 24
*7.2.2 Scenario: VoIP & Location-Capable Enterprise — Remote Staff Served by Location-Capable IP Access Network (with LIS) ..... 24*



DRAFT

7.2.2.1 Use Case: Remote VPN Users with Location-Capable IP Endpoints ..... 25
7.2.2.2 Use Case: Remote VPN Users with Location-Capable but Unaware and Location-Incapable IP Endpoints.. 25
*7.2.3 Scenario: Enterprise — Remote VPN Users Served via Location-Capable Wireless Access Points .....26*
*7.2.4 Scenario: VoIP & Location-Capable Enterprise — Remote Staff Served by IP Access Network without Location Services (no LIS).....26*
*7.2.5 Scenario: Enterprise – Operates a LIS, but Uses Hosted VoIP Services for Emergency Calling .....27*
7.2.5.1 Use Case: On-Site User with Location-Capable IP Endpoint ..... 28
7.2.5.2 Use Case: On-Site User with Location-Incapable/Unaware IP Endpoint..... 28
7.2.5.3 Use Case: On-Site User with Wireless Access Location-Incapable/Unaware IP Endpoint..... 29
7.2.5.4 Use Case: Remote VPN User with Location-Capable IP Endpoint Served by Location-Capable IP Access Network (with LIS) ..... 29
7.2.5.5 Use Case: Remote VPN User with Location-Incapable IP Endpoint Served by Location-Capable IP Access Network (with LIS) ..... 29
7.2.5.6 Use Case: Remote VPN User Served by IP Access Network without Location Services (no LIS) ..... 29
*7.2.6 Scenario: Enterprise – Does Not Operate a LIS .....30*

DRAFT

# 1 Executive Overview

## 1.1 Purpose and Scope of Document

This Technical Reference document provides the NENA requirements for providing location information to support emergency calling. It also provides example scenarios and use cases that need to be supported. This is being provided to support organizations that are defining solutions for determining, acquiring and conveying location information to support emergency calling.

Location information is extremely important to Enhanced 9-1-1 (E911) Services for two reasons:

1. In North America, the caller's location is used to determine the routing of the emergency call to the appropriate Public Safety Answering Point (PSAP).
2. The PSAP generally uses the caller's location to assist in the dispatch of the appropriate emergency response resources to the site of the emergency.

Historically, wireline callers have been identified by Telephone Numbers (TNs); static location data correlated with the TN has been entered and maintained in special-purpose databases. Dedicated facilities from the originating switch direct emergency calls to an appropriate Selective Router. During an emergency call, the Automatic Number Identification (ANI) passed with the call is used to look up location information associated with the TN. This location information is used to route the call to the proper PSAP. The systems and interfaces handling this information are dedicated and secure. The location information is as current and accurate as the records maintained in the database.

Wireless calling has been supported with a phased approach. In Phase I, a Pseudo-ANI (pANI) has been associated with each wireless carrier cell site/sector and is passed with the emergency call. The emergency call is routed to the PSAP associated with that pANI. The pANI allows the PSAP call-taker to determine a wireless caller's location information but only in relation to a cell site/sector. Phase II supports measuring a caller's location. The wireless carrier provides the caller's number and a pANI (associated with the call rather than cell site/sector) that can be used as lookup keys for routing and to support queries to a Mobile Positioning Center for the caller's location. Again, the systems and interfaces to signal information are dedicated and secure and the caller's location is as accurate as the device used to record or to measure it.

New IP-based technologies further separate the tether between the identifiers for an emergency caller and the current location of the caller. New mechanisms are being considered to determine and acquire location information for a given emergency call. These mechanisms must support static, nomadic and mobile users. The general approach being supported in the IETF is to determine and acquire location information at the point of origin in the access network. Location information is conveyed with the call so that both can be routed and delivered to the appropriate PSAP.

It is expected that the mechanisms for actually determining location might make use of either or a combination of wiremap information and measurement methods, depending on the type of access architecture and the access provider.

The primary purpose of this document is to provide a set of requirements that can be used by industry forums and standards bodies in the development of standard mechanisms for devices to acquire location information from their service providers. However, when devices must acquire location information from a service provider, rather than self-measuring, it is desirable to minimize the number of methods that devices must support to acquire location information from various service providers. Any given method will only work if every access network can support it, and these methods will only be interoperable if standards are defined and used. It is hoped that interoperable standards will allow IP endpoints to move between locations and access networks and still be able to acquire their location for emergency calling at a reasonable cost. It is also important that location information for IP endpoints be as accurate and dependable as the location information available for existing wireline and wireless users.

This document also recognizes that some devices will not be location-capable; in some cases network elements may need to acquire location information on behalf of these devices. Optional mechanisms for service providers to support this capability for their customers is also desired.

A Presence Identity Data Format – Location Object (PIDF-LO) has been defined as a protocol-independent mechanism to carry location information-by-value in the form of a civic street address or geographical coordinates. Mechanisms are also being considered for carrying a location-by-reference that provides a Uniform Resource Identifier (URI) pointer to the actual location information. This mechanism is recommended by NENA as the form in which location information will be conveyed to the PSAP via Session Initiation Protocol (SIP), once it has been acquired.

## 1.2 Reason to Implement

In the past, a comprehensive, coherent set of requirements from NENA has not been available to standards development organizations (SDOs). Solutions have been driven by legislation and based on technical input primarily from equipment vendors. This document should be of assistance to SDOs as they develop solutions and protocols for emerging technologies to determine, acquire, convey, and deliver location information for supporting emergency calling in North America.

## 1.3 Benefits

Use of this document model will:

Provide guidance to SDOs
Enable proposed solutions to be evaluated to determine if they meet the requirements of NENA.
Encourage a more uniform approach to standards for location information.

## 1.4 Summary of Operational Impacts Summary

The way in which location information is determined, acquired, and conveyed will impact its use in location-based routing. The availability and integrity of this information will impact the number of calls that are misrouted or otherwise affect the ability of a PSAP to handle emergency calls. The availability and integrity of location information will also affect the ability of the PSAP and other agencies to dispatch appropriate resources for the emergency call.

## 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 serves as input to the Emergency Services Interconnection Forum and other SDOs for development of standards and solutions to support location information for emergency services.

## 1.7 Reason for Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in this paragraph.

This is the first issue of this document.

## 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 or equivalent.

## 1.9 Anticipated Timeline

Deployment or implementation will take place as required to support location information in emerging technologies.

## 1.10 Costs Factors

All proposed solutions will have tradeoffs. Cost factors have been identified as one additional criteria that may affect evaluation of any particular proposed solution for location determination by the access network, acquisition by the endpoint or other network element on its behalf, conveyance with the call, and delivery to the PSAP. Costs affect rate of adoption and implementation.

This document will not provide specific application of cost factors to any solution, but rather will identify this as a factor that will need to be considered.

## 1.11 Cost Recovery Considerations

Cost recovery mechanisms need to be determined.

DRAFT

### 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: | |
|---|---|
| AIP | Access Infrastructure Provider |
| ALI | Automatic Location Identification |
| ANI | Automatic Number Identification |
| ANSI | American National Standards Institute |
| ATIS | Alliance for Telecommunications Industry Solutions |
| CLEC | Competitive Local Exchange Carrier |
| CPE | Customer Premises Equipment |
| E9-1-1 | Enhanced 9-1-1 |
| ILEC | Incumbent Local Exchange Carrier |
| | |
| LAN | Local Area Network |
| LIS | Location Information Server |
| LO | Location Object |
| MSAG | Master Street Address Guide |
| PIDF | Presence Information Data Format |
| PIDF-LO | Presence Information Data Format – Location Object |
| PSAP | Public Safety Answering Point |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| VLAN | Virtual LAN |
| VoIP | Voice over Internet Protocol |
| VPC | VoIP Positioning Center |
| VSP | Voice Service Provider |
| VPN | Virtual Private Network |
| WAP | Wireless Access Point |
| WNC | Wireless Network Controller |

## 2 Overview

Section 3 of this document provides background terminology, definitions, architecture, and assumptions.

wiretrace provisioning process (including location validation)
location determination by the access network
location acquisition by the endpoint or by another network element on its behalf
conveyance of location with the call
delivery of location information to the PSAP.



DRAFT

Section 4 of this document provides the requirements for mechanisms for:

- wiretrace provisioning process (including civic location validation)
- location determination by the access network
- location acquisition by the endpoint or by another network element on its behalf
- location updates
- location dependability
- testing plans.

Section 5 lists additional criteria which might be used in evaluation of a particular solution for implementation.

Section 6 provides references.

Section 7 of this document provides example scenarios and use cases. Not all solutions may be applicable to all scenarios. In particular, location determination may depend on the characteristics of the technology and the expected mobility of the endpoint.

# 3 Terminology and Assumptions

## 3.1 Terminology and Definitions

***IP Access Network***: The network in which the first publicly routable IP address is assigned to an end-point. For residential broadband networks the creation and supply of an access network may require the co-operation of several different providers. For example an ISP may lease lines and DSLAM capacity from an existing telephony provider; in such a circumstance both entities are necessary to provide an access network.

***Definitive Civic Address***: An address that can be resolved into a local MSAG-valid address and will yield a route to the correct PSAP when used to route an emergency call and is bound to a specific VEP.

***Network Location Determination***: Refers to the mechanism and data that a network entity can use to ascertain the whereabouts of a terminal in the access network such that the location can be specified in a valid PIDF-LO.

***Enterprise Network***: A large, privately owned and run, diverse network connecting major points in a company or other organization.

***Location Acquisition***: Refers to the way in which a network-determined location is made available to the network entity responsible for inserting the location information into the context of an emergency call. The network entity may be the terminal or it may be some other routing node such as a proxy or call-server.

***Location Conveyance***: Refers to the act of transporting location information with an emergency call.



DRAFT

***Location Dependability***: Reflects the level of trust that a receiving node has in the quality and authenticity of the location information being provided.

For location information to be useful to a recipient it requires three key characteristics:

1. It must be attributed to the Target that the recipient wishes to locate
2. It must be in a form and to a suitable precision to be of use to the recipient
3. It must have characteristics 1 and 2 at the time it is provided to the recipient

The ability or level of trust that a location recipient has that the location information accurately exhibits all three of these characteristics is referred to as location dependability.

***Location Validation***: Refers to the action of ensuring that a civic address can be used to discern a route to the appropriate PSAP. Location validation is outside of the scope of this document.

***Nomadic***: A user is said to be nomadic if they are constrained within an access network such that their location can be represented as a definitive civic address for that network attachment. The user may move from one network attachment to another but cannot maintain a session during that move. If the user is able to move outside the definitive civic address without losing network attachment then the user is considered to be mobile, not nomadic.

***Mobile***: A user is said to be mobile if they are able to change access points while preserving all existing sessions and services regardless of who is providing the access network; and their location may be definitively represented by a geographic co-ordinates but only indicatively represented by a civic address.

***Fixed/Static***: Refers to an IP end-point that cannot move, is always in same location and always accesses a network from the same point.

***Location-capable***: Used to describe IP endpoint devices that are capable of requesting, acquiring, and storing location information as well as including this information in a Presence Identity Data Format – Location Object (PIDF-LO) when originating an emergency call.

***Location-aware***: used to describe IP endpoint devices that are location-capable and that have acquired location information, either with network assistance or by self-determination.

***Location-unaware***: used to describe IP endpoint devices that are location-capable but that have not been able to successfully acquire location information, either with network assistance or by self-determination.

***Location-incapable***: used to describe IP endpoint devices that are not capable of requesting, acquiring, or storing location information. This includes most existing IP endpoints today.



One Nation 9-1-1 One Number

***Location Recipient:*** A location recipient is the consumer of location information. This may be the Target, the PSAP, the VPC or any other node that uses location information when it is provided.

## 3.2 Architecture

Figure 1 describes the architectural elements and interfaces for determining, acquiring, conveying, delivering and updating location information for location-capable endpoints.

**Figure 1 Location Information Architecture – Location-Capable Endpoints**

Figure 2 describes the architectural elements and interfaces for determining, acquiring, conveying, delivering and updating location information for location-unaware endpoints.

**Figure 2 Location Information Architecture – Location-Unaware Endpoints**

The following definitions are also used in this document.

Access Location Element (ALE) – the network elements in the access infrastructure that determine the position of a device.

Location Information Server (LIS) – repository of mappings between identifiers (known to the ALE) and the location information that describes the physical geographical location associated with that identifier, e.g., geo-coordinates or civic street address.

LIS Directory/Discovery – identifies the LIS that serves a given IP domain.

Location Validation Function (LVF) – that function which an endpoint, LIS, or ASP can query to determine whether a given civic street address has the appropriate data elements to uniquely identify a location-appropriate PSAP by the Emergency Call Routing Function.

Emergency Call Routing Support – includes network elements like proxies, call signaling control functions, etc., that perform location-based routing queries.

### 3.3 Assumptions

To be determined.

# 4 Requirements

## 4.1 Location Determination and Acquisition

**DA1**– The access network shall provide a mechanism for determination and acquisition of location information, and support queries for location.

**DA2** – The location estimate used shall be that associated with the physically (wire, fiber, air) connected network.

**DA3** – Location may be requested at any time. Location information must be associated with the device at the time the location is requested.

**DA4** – Location acquisition should be provided by a consistent method across all network configurations.

**DA5** – Location determination and acquisition mechanisms should be applicable to emergency calling; they may also be applicable to a wide range of value-added location-based services.

**DA6** – Location determination and acquisition techniques shall support both NENA i2 and i3 network architectures.

**DA7** – When measurement-based location determination mechanisms fail, the most accurate location information available should be provided. Examples include: For mobile, the Wireless Service Provider might provide tower/Access Point location, last known fix, etc. For wireline, a LIS might provide a civic location that defines the serving area of an access point, e.g., the State of Texas.

**DA8** – Location determination and acquisition must have minimal impact on call setup time in the event that location is not known ahead of time.

**DA9** – Where a device is not location aware, the network should have the ability to assert a location estimate on behalf of the device.

**DA10** – Location acquisition methods should not require modification of hardware/firmware in home-routers/modems.

**DA11** – A location determination method must exist that does not require network hardware replacement in the core network.

## 4.2 Location Representation

**Rep1**– Location information may be provided by-value or by-reference; the form is subject to the nature of the request.

**Rep2** – Location determination and acquisition mechanisms must support all location information fields defined within a PIDF-LO.

**Rep3** – Location acquisition mechanisms must allow for easy backwards compatibility as the representation of location information evolves.



DRAFT

**Rep4** – All representations of location shall include the ability to carry altitude and/or floor designation. This requirement does not imply altitude and/or floor designation is always used or supplied.

### 4.3 Location Security and Dependability

**LocSec1**– Location information shall only be provided to authenticated and authorized network devices. The degree of authentication and authorization required may vary depending on the network.

**LocSec2** – Location determination and acquisition methods should preserve privacy of location information, subject to local laws and regulations applicable to the endpoint's geographic location.

**LocSec 3** – The location or location estimate of a caller should be dependable.

**LocSec4** – The location acquisition protocol must support authentication of the Location Information Server, integrity protection of the Location Information, and protection against replay.

**LocSec5** – The location source shall be identified and should be authenticated. This includes manually entered locations.[1]

**LocSec6** – Where a location is acquired and cached prior to an emergency call, it SHOULD be refreshed at regular intervals to ensure that it is as current as possible in the event location information cannot be obtained in real time.

**LocSec 7** – Where location by-reference is used, the appropriate privacy policies MUST be implemented and enforced by the LIS operator.

## 5 Additional Evaluation Criteria

You may wish to consider the following additional criteria in evaluating your location acquisition and delivery mechanisms:

EC1 – How/when can location information be determined/refreshed?

EC2 – What network/user elements are affected by the determination method?

How long does it take to do?

Who is involved in doing it?

Who needs to invoke it?

EC3 – What network/user elements are affected by the location acquisition method?

EC4 – What is the likelihood of universal acceptance and availability for location determination?

[1] Manual entry is not the preferred method. If the Location Information is configured into the Emergency Caller's Device by manual entry, such entry SHOULD require authentication and authorization of the person providing the entry.



One Nation 9-1-1 One Number

Worldwide

North America

EC5 – What is the likelihood of universal acceptance and availability for location delivery?

Worldwide

North America

EC6 – Relative complexity versus benefit?

EC7 – What is the maturity of the supporting standards?

EC8 – What are the determination technique's advantages? (e.g. precision, speed to location etc.)

EC9 – What are the delivery technique's advantages?

EC10 – What are the vulnerabilities of the determination technique?

EC11 – What are the vulnerabilities of the delivery technique?

EC12 – Failure modes, when applied to the scenarios, must be supported.

Number of failure modes

Degree of impact

Likelihood of occurrence

Recovery

EC13 – How/when does the method support location validation? Other methods to determine accuracy?

EC14 – Location dependability

EC15 – Interoperability between acquisition and determination mechanisms

EC16 – Interoperability between different location determination mechanisms.

EC17 – Interoperability between different location acquisition mechanisms. Can they co-exist without causing confusion?

# 6 Bibliography of Related NENA Documents

[1] NENA 08-502, *NENA Generic E9-1-1 Requirements*, Issue 1, July 23, 2004

[2] NENA 08-001, *Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)*, Issue 1, 2005

[3] NENA 08-751, *NENA i3*, Technical Requirements Document, to be published



DRAFT

[4] NENA (to be assigned), *NENA VoIP Recommended Method(s) for Determining Location to Support Emergency Calling* Technical Information Document (TID)– DRAFT

DRAFT

# 7 Exhibits -- Example Scenarios and Use Cases

The following sections describe the key operating scenarios that have been identified as either existing or likely, with regards to requiring location information for the purposes of making an emergency call. The scenarios encompass a range of attributes including the access environment, service provider environment, and device capabilities. For ease of use, the scenarios are broken into two main categories: residential and enterprise.

## 7.1 Residential Configurations

Residential or mass market services in this TRD refer to services that are offered to home or small business users. These services may be offered over a number of access technologies, including xDSL broadband, cable broadband and a variety of wireless access technologies.

An Enterprise without its own Enterprise network might also have Enterprise sites that appear as mass market customers to the IP access provider from the point of view of location technology.

The following variables contribute to characterizing the use cases that are considered in residential/mass market scenarios.

IP endpoint device capabilities

- Location-capable and aware
  - Capable of self-determination of location
  - Capable of acquiring location from the network
  - Capable of receiving user entry of location.
- Location-capable but unaware
- Location-incapable

Ability of IP endpoints to Change Location

- Static/fixed location only
- Static or Nomadic or Mobile

Various combinations of these variables may serve to characterize use cases to be considered in evaluating proposed solutions for location determination and location acquisition in the residential/mass market environment scenario.

For purposes of this TRD it has been acknowledged that the case of static/fixed location IP endpoints can be accommodated with conventional pre-IP approaches (i.e., pre-population of routing and location databases with Telephone Number-based records). However, most IP endpoints will be capable of being moved from location to location, so the focus of this TRD is on the case of nomadic users—solutions for nomadic users will also be able to accommodate static/fixed location devices.

Some wireless access scenarios have also been included for completeness.

### 7.1.1 Residential/Mass Market Scenario – Location-Capable IP Access Network

An example scenario is illustrated in Figure 3. In the figure, residential and small-to-medium (SMB) business locations are provided access to the Internet directly via a public IP access network. A VoIP Service Provider (VSP) application provides voice services to IP endpoints. In this figure, a LIS is included in the IP access network to illustrate the entity that is used by entities to acquire location information.

**Figure 3 Residential/Mass Market Scenario – Location Capable IP Access Network**

Two use cases are considered for this basic scenario.

Residence

#### 7.1.1.1 Use Case: User with Location-Capable IP Endpoint

This use case is expected to apply to residences/small businesses equipped with new IP devices/applications that are location-capable and must either use the method supported by the IP access network for acquiring its location information from the service provider's LIS, or must be capable of measuring/determining its own location.

Mall location

Once location information is acquired, the IP device must be capable of constructing and sending its location information in PIDF-LO on emergency calls.

#### 7.1.1.2 Use Case: User with Location-Incapable/Unaware IP Endpoint

This use case applies for existing residential equipment/applications that are not capable of acquiring, storing location information or constructing a PIDF-LO. It also applies for IP devices that



SMB

do not support the location acquisition method(s) that are supported by the IP access network provider.

In this use case, if the VoIP Service Provider's call server can identify the caller's IP access network, the call server may cooperate with the IP access network LIS to estimate the caller's location on-behalf-of the IP device.

### 7.1.2 Mass Market Scenario – Multiple Service Providers and LISs, Including Wireless Access Points

This example scenario is provided to illustrate the increased complexity involved in IP access network architectures where there may be more than one service provider and more than one LIS involved in relaying location information, as illustrated in Figure 4. From the point of view of the entity that is acquiring location information, solutions are needed that hide this complexity.

**Figure 4 Mass Market – Multiple Service Providers and LISs, Wireless Access Points**

The use cases that apply in this scenario are not appreciably different from the previous scenario from the point of view of the entity that is acquiring location. This scenario is included primarily to highlight IP access network architectures that will have an impact on location determination solutions by requiring communications among multiple LISs, and to consider the case of wireless access points.

Coffee Shop

Residence

Laptop

Wireless Access Point 1

#### 7.1.2.1 Use Case: User with Wireless Access Location-Capable IP Endpoint

This use case applies when IP devices use wireless access points to originate emergency calls. For location determination, the wireless access points must support the association of a "connected" IP device with the geographic location of the wireless access point. The wireless access points may also support a location acquisition mechanism provided by the IP access network for its IP devices.

#### 7.1.2.2 Use Case: User with Wireless Access Location-Incapable/Unaware IP Endpoint

This use case applies when the IP device using a wireless access points to originate an emergency call is location-incapable or does not support the method(s) for location acquisition that are supported by the IP access network. However, in this use case, the wireless access points may support the association of its "connected" IP devices with the geographic location of the wireless access point to support acquisition of location information on-behalf-of the IP device by a VoIP Service Provider. This optional capability is only possible if the VSP is able to determine the IP access provider serving the IP device.

#### 7.1.2.3 Use Case: User with Wireless Access Location-Measurement-Capable IP Endpoint

This use case applies when IP devices use wireless access points to originate emergency calls. This use case differs from the previous ones in that the IP device measures its own location, with or without the assistance of the IP access network.

### 7.2 Enterprise Configurations

A number of variables contribute to characterizing the Enterprise scenarios that should be considered.

IP endpoint device capabilities

- Location-capable and aware
  - Capable of self-determination of location
  - Capable of acquiring location from the network
  - Capable of receiving user entry of location
- Location-capable but unaware (cannot acquire location)
- Location-incapable

Enterprise IP endpoint device location

- On-site/on-Enterprise LAN
- User at remote site
- Remote user—road warrior (at a different Enterprise location, e.g., hotel)
- Remote user—telecommuter (at a residential/mass market customer site)



DRAFT

Enterprise support of location technology

- Enterprise supports local LIS on Enterprise LAN
- Enterprise does not support local LIS

Enterprise support of VoIP Services

- Enterprise supports VoIP services with Enterprise Call Server/Proxy
- Enterprise uses hosted/carrier VSP for access to PSTN and E9-1-1 emergency services calling

For remote users, the remote IP access network's support of location technology

Various combinations of these variables serve to characterize scenarios and use cases to be considered in evaluating proposed solutions for location determination and location acquisition in the Enterprise environment.

As in the residence/mass market scenarios, the focus in the current issue of this TRD is on solutions to support nomadic users, in the expectation that this will also meet the needs of static/fixed users. Support for wireless access points is included.

### 7.2.1 Scenario: VoIP- and Location-Capable Enterprise — Provides VoIP Services and Operates LIS(s)

In this example Enterprise scenario, the Enterprise may have one or more office locations interconnected by an Enterprise network. This is illustrated in Figure 5. The Enterprise provides its own call servers/proxies that support emergency calling from users on the Enterprise network. The Enterprise operates a LIS that is capable of cooperating in the determination of the physical geographic location of users on its corporate LANs. (It is possible that one or more LISs might be involved, but coordination among these is not considered here). The Enterprise may use a public access network for access to the Internet, as shown in the figure, or it may act as its own ISP.

DRAFT

**Figure 5. Multi-Site Enterprise—VoIP Service and Location-Capable**

Several use cases will be considered for this same basic scenario.

#### 7.2.1.1 Use Case: On-Site User with Location-Capable IP Endpoint

This use case is expected to apply to Enterprise staff equipped with new IP devices/applications deployed by the Enterprise on its LANs. In this use case, the user's IP device that is connected to the Enterprise LAN(s) must be location-capable and must either use the method supported by the Enterprise for acquiring its location information from the Enterprise LIS, or must be capable of measuring/determining its own location.

Once location information is acquired, the IP device must be capable of constructing and sending its location information in PIDF-LO on emergency calls.

#### 7.2.1.2 Use Case: On-Site User with Location-Incapable/Unaware IP Endpoint

This use case applies for older Enterprise equipment/applications. It may also apply to visitors to the Enterprise with IP devices that either do not support location or that support location acquisition methods not supported by the Enterprise LAN.

In this use case, the Enterprise network's call server may cooperate with the Enterprise LIS to estimate the caller's location on-behalf-of the IP device.

#### 7.2.1.3 Use Case: On-Site User with Wireless Access Location-Capable IP Endpoint

This use case applies when the Enterprise provides wireless access points in its Enterprise network and when IP devices use these wireless access points to originate emergency calls. The Enterprise wireless access points must support the association of a "connected" IP device with the geographic location of the wireless access point. The Enterprise wireless access points must also be able to support the location acquisition mechanism used by the Enterprise for its IP devices.

#### 7.2.1.4 Use Case: On-Site User with Wireless Access Location-Incapable/Unaware IP Endpoint

This use case applies when the Enterprise provides wireless access points in its Enterprise network and allows IP devices that are location-incapable or that do not support the Enterprise methods for location acquisition. However, in this use case, the Enterprise wireless access points must support the association of its "connected" IP devices with the geographic location of the wireless access point to support acquisition of location information on-behalf-of the IP device by the Enterprise's VoIP services.

#### 7.2.1.5 Use Case: On-Site User with Wireless Access Location-Measurement-Capable IP Endpoint

This use case applies when the Enterprise provides wireless access points in its Enterprise network and when IP devices use these wireless access points to originate emergency calls. This use case differs from the previous ones in that the IP device measures its own location, with or without the assistance of the Enterprise network.

### 7.2.2 Scenario: VoIP & Location-Capable Enterprise — Remote Staff Served by Location-Capable IP Access Network (with LIS)

This example Enterprise scenario is an extension of the previous scenario that considers the use cases of remote staff connected to the Enterprise via a Virtual Private Network (VPN). This is illustrated in Figure 6. The Enterprise provides its own call servers/proxies that support emergency calling from users on the Enterprise network. The Enterprise operates a LIS for location determination and acquisition on its own network. The Enterprise may use a public access network for its access to the Internet, as shown in the figure, or it may act as its own ISP.

For remote VPN users, the capabilities of the IP access network serving the remote user must also be considered. In this example Enterprise scenario, the remote IP access network is Location-Capable; that is, it operates a LIS and supports method(s) for determining and acquiring location information.

**Figure 6. Enterprise—Remote VPNs—Remote IP Access Network is Location-Capable**

Several use cases will be considered for this same basic scenario.

#### 7.2.2.1 Use Case: Remote VPN Users with Location-Capable IP Endpoints

This use case is expected to apply to Enterprise staff equipped with location-capable IP devices/applications connected to the Enterprise network via a VPN. The IP endpoint must not only be location-capable, but must be able to use the method supported by the remote IP access network for acquiring its location information from the location-capable IP access network, or must be capable of measuring/determining its own location.

Once location information is acquired, the IP endpoint must be capable of constructing and including its location information in PIDF-LO on emergency calls originated over the VPN.

#### 7.2.2.2 Use Case: Remote VPN Users with Location-Capable but Unaware and Location-Incapable IP Endpoints

This use case applies for remote VPN users equipped with IP endpoints that either do not support acquisition of location or that support location acquisition methods that are not supported by the remote IP access network.

In this use case, the Enterprise network's LIS or call server may cooperate with the remote user's IP access network LIS to estimate the caller's location on-behalf-of the IP endpoint.

DRAFT

### 7.2.3 Scenario: Enterprise — Remote VPN Users Served via Location-Capable Wireless Access Points

The example Enterprise scenario in Figure 7 is a variation of the previous scenario, where the IP endpoint remote access is provided from a wireless access point.

**Figure 7. Enterprise—Remote VPNs—Remote IP Access Network Provides a Location-Capable Wireless Access Point**

The use cases for this scenario are similar to the use cases for the wired access scenario, with the exception that the Wireless Access Point (WAP) must be capable of supporting location determination, and possibly acquisition of location information by the wireless IP endpoints using it for access.

### 7.2.4 Scenario: VoIP & Location-Capable Enterprise — Remote Staff Served by IP Access Network without Location Services (no LIS)

This example Enterprise scenario is a variation of the Enterprise scenario that considers the use cases of remote staff connected to the Enterprise via a Virtual Private Network (VPN). This scenario is illustrated in Figure 8. The Enterprise provides its own call servers/proxies that support emergency calling from users on the Enterprise network. The Enterprise operates a LIS that is capable of cooperating in the determination of the physical geographic location of users on its corporate LANs. The Enterprise may use a public access network for access to the Internet, as shown in the figure, or it may act as its own ISP.

However, in this scenario the remote IP access network (e.g., a hotel Enterprise network) is not capable of supporting Location Services and does not operate a LIS.

**Figure 8. Enterprise—Remote VPNs—Remote IP Access Network Does Not Support Location Services**

For this scenario, the use cases of location-capable, location-capable/unaware, and location incapable IP endpoints are essentially indistinguishable, in that location cannot be determined nor location information acquired automatically for any of them at the point where they access the network. This is true whether the access is provided via wireline connections or wireless access points.

### 7.2.5 Scenario: Enterprise – Operates a LIS, but Uses Hosted VoIP Services for Emergency Calling

In this example Enterprise scenario the Enterprise operates a LIS that is capable of cooperating in the determination of the physical geographic location of users on its corporate LANs. The Enterprise uses a hosted VSP solution to support emergency call originations from users on the Enterprise network as well as from remote VPN users as shown in Figure 9. With respect to the remote users connected to the Enterprise network via VPNs, in this scenario it is assumed that the remote IP access network is location capable (i.e., operates its own LIS).

DRAFT

**Figure 9. Enterprise—Location Capable but Uses Hosted VoIP Services**

Use cases including both on-site and remote users are included together for this scenario for brevity. Use cases include both remote user IP access networks that operate a LIS and that do not support location services.

#### 7.2.5.1 Use Case: On-Site User with Location-Capable IP Endpoint

From the point of view of the location information for emergency calling, this use case is the same as described in Section 7.2.1.1 for wireline connected IP endpoints and the same as described in Sections 7.2.1.3 and 7.2.1.5 for wireless access IP endpoints. IP endpoints connected to the Enterprise LAN must use the method supported by the Enterprise for acquiring location information.

#### 7.2.5.2 Use Case: On-Site User with Location-Incapable/Unaware IP Endpoint

This use case applies for older Enterprise equipment/applications. It may also apply to visitors to the Enterprise with IP endpoints that either do not support location or that support location acquisition methods not supported by the Enterprise LAN.

In this use case, the VSP's call server may cooperate with the Enterprise LIS to estimate the caller's location on-behalf-of the IP endpoint.

DRAFT

#### 7.2.5.3 Use Case: On-Site User with Wireless Access Location-Incapable/Unaware IP Endpoint

This use case applies when the Enterprise provides wireless access points to its Enterprise network and allows IP endpoints that are location-incapable or that do not support the Enterprise methods for location acquisition. However, in this use case, the Enterprise wireless access points may optionally support the association of its "connected" IP endpoints with the geographic location of the wireless access point to support optional acquisition of location information on-behalf-of the IP endpoint by the hosted VoIP services.

#### 7.2.5.4 Use Case: Remote VPN User with Location-Capable IP Endpoint Served by Location-Capable IP Access Network (with LIS)

This use case is expected to apply to Enterprise staff equipped with location-capable IP endpoints/applications connected to the Enterprise network via a VPN. From the point of view of the location information for emergency calling, this use case is the same as described in Section 7.2.2.1 for wireline connected IP endpoints and the same as described in Sections 7.2.3 for wireless access IP endpoints.

The IP endpoint must not only be location-capable, but must be able to use the method supported by the remote IP access network for acquiring its location information from the location-capable IP access network, or must be capable of measuring/determining its own location.

Once location information is acquired, the IP endpoint must be capable of constructing and including its location information in PIDF-LO on emergency calls originated over the VPN.

#### 7.2.5.5 Use Case: Remote VPN User with Location-Incapable IP Endpoint Served by Location-Capable IP Access Network (with LIS)

This use case applies for remote VPN users equipped with IP endpoints that either do not support acquisition of location or that support location acquisition methods that are not supported by the remote IP access network.

In this use case, if the Enterprise network's LIS or the hosted VSP's call server can identify the LIS that serves the remote user, by mutual agreement they may optionally cooperate with the remote user's IP access network LIS to estimate the caller's location on-behalf-of the IP endpoint.

#### 7.2.5.6 Use Case: Remote VPN User Served by IP Access Network without Location Services (no LIS)

This use case applies for remote VPN users equipped with IP endpoints that support location acquisition methods that are not supported by the remote IP access network.

For this scenario, the use cases of location-capable, location-capable/unaware, and location-incapable IP endpoints are essentially indistinguishable, in that location cannot be determined nor location information acquired automatically for any of them at the point where they access the network. This is true whether the access is provided via wireline connections or wireless access points.



DRAFT

### 7.2.6 Scenario: Enterprise – Does Not Operate a LIS

In this scenario, the Enterprise does not operate a LIS, but makes use of the IP access network's LIS to automatically obtain location information for each of its access entry point into the serving IP access network.

By using a different access point for each site, the Enterprise can obtain a different location object for different sites. From the point of view of the IP access network, each entry point is indistinguishable from any other access point for location determination. Therefore, an office site may have no more detailed location information than an individual endpoint. This scenario is assumed to be addressed in the mass market scenarios described in Section 7.1.

DRAFT