Report for Ofcom

Assessment of VoIP location capabilities to support emergency services

28 June 2011

Ref: 19374-263

analysys mason

Contents

Analysys Mason Limited
Bush House, North West Wing
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)845 600 5244
Fax: +44 (0)20 7395 9001
london@analysysmason.com
www.analysysmason.com
Registered in England No. 5177472

1 Executive summary

This document is the final report of a study conducted for Ofcom by Analysys Mason into the ND1638 architecture designed by the Network Interoperability Consultative Committee (NICC) to provide location information for emergency calls made by VoIP users. The objective of this study is to help Ofcom to develop its understanding of the NICC architecture, including:

- describing the capabilities and any limitations of the architecture
- identifying the challenges of implementing the architecture
- quantifying the implementation and on-going running costs.

The ND1638 architecture has been developed to meet a specific requirement to provide real-time emergency service location capability for VoIP users contacting UK emergency services from DSL access points via the existing architecture used by the stage one Public Safety Answering Points (PSAPs). The architecture achieves this specific requirement and remains, where possible, compatible with international interface standards, namely those developed by the National Emergency Number Association (NENA) in the United States and the Internet Engineering Task Force (IETF). In a European context, ND1638 represents the most detailed work that has been done to address a specific national requirement. ND1638 is, as a result, well placed to influence the Europe-wide initiative by the European Emergency Number Association (EENA) that is due to progress towards specifying VoIP emergency location standards during 2011 (although a common pan-European approach is unlikely due to variation in emergency service architectures between countries).

However, ND1638, which only addresses DSL, is just the first stage in the development of the emergency services location architecture to meet the developing needs of users. The use of different means of VoIP access (e.g. cable, Wi-Fi hotspots, private networks) as well as other next-generation services (e.g. text, images and video) are not currently covered. Work is continuing on addressing these issues in the NICC working group, and it needs to be ensured that the initial implementation of ND1638 is compatible with its on-going development. Our investigations suggest that this is likely to be the case, as for example the ND1638 architecture does not exclude an evolution from a network-centric to an end-device-centric, physical location request model which may be more appropriate to all-IP networks in the future.

To date, there has been very little (if any) progress towards implementation of ND1638 in the UK, and there remain considerable challenges in achieving this. During the study we spoke with a number of UK-based ISPs, VoIP service providers (VSPs) and emergency handling authorities (EHAs), which raised several concerns about the current architecture, relating to:

- **Range of access types supported** – only DSL is supported, and not other access types such as Wi-Fi hotspots, cable networks or private networks.
- **Alignment with other standards** such as those defined by NENA and IETF, rather than being a UK-specific standard.

- **Need for additional implementation guidance** to ensure consistent and robust implementation.
- **Costs of implementation** – significant investment is likely to be required.
- **Challenge of managing the implementation across so many VSPs and ISPs** – the UK has a large number of VSPs and ISPs.
- **Ensuring the participation of the ISP and access network provider (ANP) community** – there may be reluctance to participate, particularly amongst ISPs and ANPs not providing VoIP services directly themselves.

The engagement of ISP and ANP organisations is particularly important to the success of the project, as their participation is required to implement the Location Information Server (LIS), which is required to determine the physical geographical address of the VoIP 999 caller. As ISPs and ANPs are not currently involved in emergency calling, and as VoIP callers will in many cases not be their taking a voice service directly from them, this may prove difficult (as economic incentives are misaligned). It is of note that in the United States, where an LIS has been included in the NENA i2 architecture for some time, actual LIS implementation is very sparse: the usual method for determining the location of callers is still to rely on the non-real-time registration of this information by end users, as in the current UK situation (pre-ND1638). The large number of VSPs, ISPs and ANPs in the UK will also provide a challenge in terms of implementation programme management.

The lack of progress towards implementation has also made it difficult to establish definitive costs for implementation across different entities, including EHAs, VSPs, ISPs and application service providers (ASPs). Cost estimates provided by the industry vary widely: estimates of capital costs by study participants ranged from £200 000 to £1 million plus, while for operating costs, estimates varied from £2000 to £200 000 per annum. The wide discrepancies in the cost estimates provided reflect both a certain lack of focus on this area to date, as well as the different starting positions of the various organisations. However, it is apparent that significant investment will be required by a large number of parties.

While it appears that ND1638 provides a viable way forward for VoIP emergency location, the progress of EENA standardisation and the on-going consultation by the US Federal Communications Commission (FCC) on the NENA i3 “next generation 911” architecture should be closely monitored. Both are due to report during 2011. EENA should provide a clear indication of the position of the ND1638 architecture in the context of European compatibility, while the level of NENA architecture implementation that the FCC mandates in the United States may provide some guidance on what can reasonably be expected to be implemented in the UK.

2 Introduction

2.1 Background

Voice calls to emergency services are accompanied by location information when this is technically feasible. Location information is used both for call-routing purposes, to ensure the call is delivered to the appropriate emergency authority, and also for dispatching personnel to the location of the incident once the call is delivered. European Directive 2009/136/EC regarding universal service and users' rights states: *"In particular, undertakings should make caller location information available to emergency services as soon as the call reaches that service independently of the technology used."* As a result of this Directive, Ofcom has issued modifications to its General Conditions under section 48(1) of the Communications Act 2003.[1] The requirement of the Directive presents a significant challenge to service providers if the caller is using VoIP technology. Many implementations of VoIP allow the caller to use the service from any location with Internet connectivity (it is a "nomadic service"). This can make it difficult to locate the caller accurately as there is not a fixed relationship between the calling line identity (CLI) of the caller and their physical location, unlike in the case of traditional landline services.

In the UK, the NICC has taken steps to address this issue by developing the ND1638 standard. This provides the ability to determine the location of a VoIP subscriber when making an emergency call in real time by obtaining the relevant data from the network. If implemented, this would replace the current practice of relying on the subscriber to provide their location to their VoIP service provider (VSP) which then passes it on to the emergency authorities by data file transfer.

2.2 Objectives

The objective of this study is to help Ofcom to develop its understanding of the NICC architecture, including:

- describing the capabilities and any limitations of the architecture
- identifying the challenges of implementing the architecture
- quantifying the implementation and on-going running costs.

In addition, Ofcom wishes to understand other solutions being developed elsewhere in the world to address this issue and how they compare to the NICC solution.

2.3 Scope

This study is intended to provide Ofcom with a status report on developments in VoIP location for emergency service calling, to inform its future policy decisions in this area.

[1] http://stakeholders.ofcom.org.uk/binaries/consultations/gc-usc/statement/Annex_2.pdf

2.4 Document layout

The remainder of this document is laid out as follows:

- Section 3 provides an introduction to the UK emergency services calling environment
- Section 4 describes the ND1638 architecture
- Section 5 reviews the ND1638 architecture
- Section 6 provides details of emergency service location initiatives in other parts of the world
- Section 7 summarises the key conclusions of the study.

A list of the abbreviations used is provided in Annex A.

3 UK emergency services calling environment

3.1 Development of UK emergency calling services

3.1.1 Service history

The UK's 999 emergency service calling service was the first in the world when it was launched in 1937,[2] and it was extended to all major towns and cities by 1948. The service was further extended to mobile users in 1986. In recent years, the growth in the use of VoIP services that can call ordinary fixed and mobile numbers has created another class of user of the emergency calling service – the VoIP subscriber.

3.1.2 Basic conventional fixed line service architecture

The UK takes a centralised, national approach to the routing of emergency service calls, as shown in Figure 3.1. When the caller dials 999 (or 112), the call is connected by the service provider to a national Stage 1 public safety answering point (PSAP). There are two Stage 1 PSAPs, which are run by the two emergency handling authorities (EHAs) BT and C&W. Each PSAP handles emergency calls for the whole of the UK, so routing does not need to be dependent on the location of the caller. This is different to architectures in other countries such as United States and France where PSAPs are deployed to service a particular geographical area.

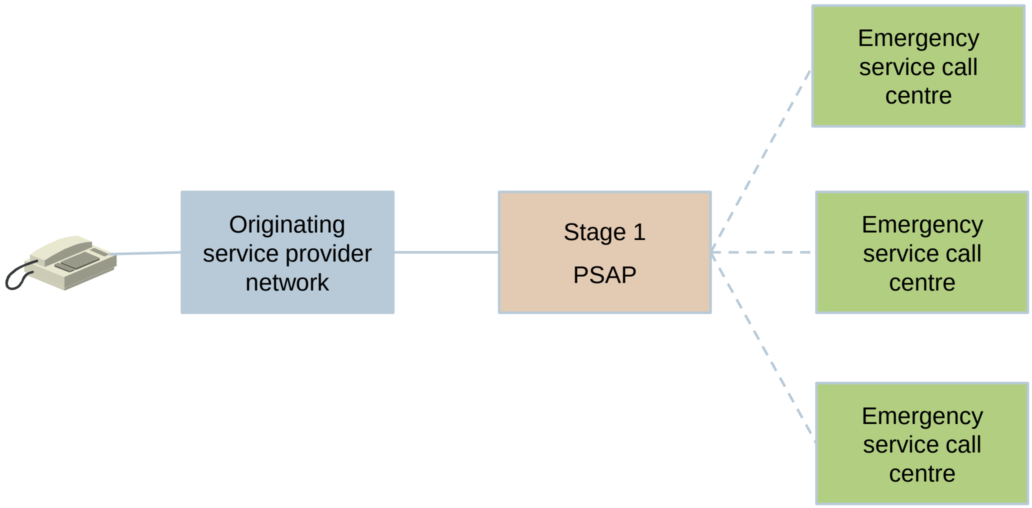

Emergency service call centre
Originating service provider network
Stage 1 PSAP
Emergency service call centre
Emergency service call centre

Figure 3.1: Conventional fixed line emergency call path [Source: Analysys Mason]

The call is answered by an agent at the PSAP and routed onward based on the location of the caller and the service they request (e.g. police, fire, ambulance, etc.). The location is found by associating the CLI of the caller with a physical geographical address provided by the originating

[2] "Regulation of VoIP services: Access to emergency services", Ofcom consultation, 26 July 2007.

service provider to the EHA or, in the absence of this information, by interrogating the caller. Identifying the physical location of the caller is generally straightforward as long as the service provider has reliable processes in place to map the CLI to a physical address and provide the information to their relevant EHA. This is helped by the fact that the service provider is also the access provider, and the CLI is directly associated with the physical telephone line at the user's location and cannot be used at other locations.

3.2 Importance of location in emergency service calls

The ability to provide a location for the caller is a key element of the emergency calling service. It is vital for helping the emergency services to provide a rapid response. This information is used for routing the call from the PSAP to the emergency service, so that the call is presented to the right organisation to respond, and is also used by the emergency service to despatch the most appropriate resources to the right location

Caller location information can also be of critical importance in dealing with the small percentage of situations where the callers are not able to give an accurate indication of their location. These may include calls from very young children, medical emergencies where the caller is incapacitated, or cases in which the caller needs to remain hidden and/or silent. For conventional fixed lines, the caller's location information can usually be provided to the emergency services relatively easily and accurately. However, calls from certain lines – such as corporate telephony networks, mobile networks, as well as (potentially nomadic) VoIP users – pose additional difficulties.

In mobile networks, the issue has been addressed by the introduction of mobile network location technologies. They can range in precision from the identification of the cell location at the basic level, to using techniques involving timing and uplink/downlink measurement to provide a more accurate location of the caller within the cell.

The introduction of VoIP services, and particularly nomadic voice services – where the user can potentially make calls from any location with Internet access – provides a greater challenge in providing the location of the caller. We discuss these challenges below.

3.3 Challenges of establishing the location of a VoIP caller

The VoIP service subscriber does not have to use a VoIP service provided by its ISP or its access network provider (ANP). Indeed, it is likely that the ISP and/or ANP will not know that the VoIP subscriber is using a service from a VSP at all. Also, it is likely that the VSP will not know which ISP and/or ANP its VoIP service subscriber is using. As the ANP (which may or may not also be the ISP) is the only organisation that can provide the location of the subscriber, it can be seen that both the VSP and the ISP/ANP need to be involved in the process of identifying the location of a particular call to the emergency services. In addition, the fact that VoIP services are can be nomadic means that the ISP/ANP could change on a call-by-call basis as the subscriber uses the service from different locations, for example other people's access connections, Wi-Fi hotspots, or even the network of their employer or other organisations.

With VoIP, the service delivery model has changed from the conventional landline model where a service provider is responsible for the complete service – application, active transport layer and physical network. In the VoIP model, the service may be provided by three different organisations: VSP (application), ISP (active transport layer) and ANP (physical network access). This is illustrated in Figure 3.2.

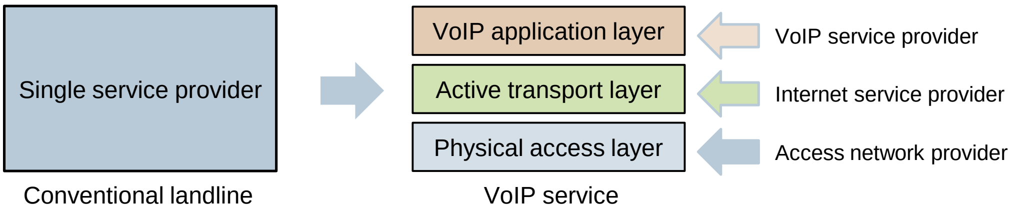


Figure 3.2: *Comparison of VoIP and conventional landline service delivery models [Source: Analysys Mason]*

Note that it is still possible that the VSP, ISP and ANP could be the same organisation, but even then it is quite possible that internal systems will not be integrated sufficiently to be able to align the VoIP CLI with its physical address.

3.4 VoIP location implementation to date

In the UK, solutions implemented to date have not been able to establish the location of the subscriber by actions within the network: they rely on the subscriber providing their location to the VSP themselves and the VSP passing on the details. This has required the mapping of each CLI to the location provided by the end-user to the VSP in a simple computer CSV file.[3]

For some VSPs, the address provided to the EHA will be that provided by the subscriber to the VSP on registration, while some VSPs also provide the subscriber with the facility, usually via a web page, to update their address as they move from location to location. However, this is far from ideal as:

- it relies on the end-user always remembering to update their address details before they use the service from another location
- there is a delay between the subscriber updating their address on the VSP's system, the updated file being sent to the EHA, and the update of the EHA systems. It is not a dynamic real-time system.

Note that in the United States, where the location of VoIP subscribers is also mandated for emergency services, the solution implemented by service providers in the majority of cases has

[3] Comma Separated Values – a simple file format for exchanging data.

also relied on a manual process of the subscriber providing their location details. This is described in more detail in Section 6.2.1.

Standards have been developed that will allow the automatic determination of a subscriber's location on a real-time basis. In the UK, this has been via the NICC group work, and in the United States via the work of NENA. In both cases, the step to implement the architecture has yet to be taken, but Analysys Mason's investigations suggest that the work undertaken by NICC and NENA are the most developed initiatives in this area; NENA i2 is already deployed in the United States.

3.5 The UK VSP and ISP market

3.5.1 VSP market

The UK VSP market is still relatively young, and it is fair to say that the numbers of VoIP subscribers have not reached the levels anticipated a few years ago. VoIP has been used primarily as a secondary line service as BT, the major local loop unbundling (LLU) players (e.g. TalkTalk, Sky, C&W) and Virgin Media continue to provide a conventional POTS voice landline service (in terms of the interface offered, even if the service uses an NGN core network). Such services are unsuitable for nomadic use. Over-the-top (OTT) or access-agnostic services such as Skype and Vonage have also played a role, but conventional fixed voice still continues to dominate the fixed market. In 2010, Analysys Mason estimated that retail VoIP[4] and OTT VoIP[5] accounted for 12% of the total number of fixed voice lines in the UK, as shown in Figure 3.3 below. We forecast that this situation will gradually change over the next five years, and predict that retail VoIP and OTT VoIP will account for 25% of fixed voice connections by 2015, with OTT VoIP accounting for 20% of the total.

The VSP market is very fragmented: the UK's VSP industry body, the Internet Telephony Service Provider Association (ITSPA), has nearly 50 members that offer VoIP services.

[4] Retail VoIP includes residential and connections to small businesses sold in a similar way to residential services, but not connections to larger businesses.

[5] OTT VoIP includes subscriptions via a mobile handset.

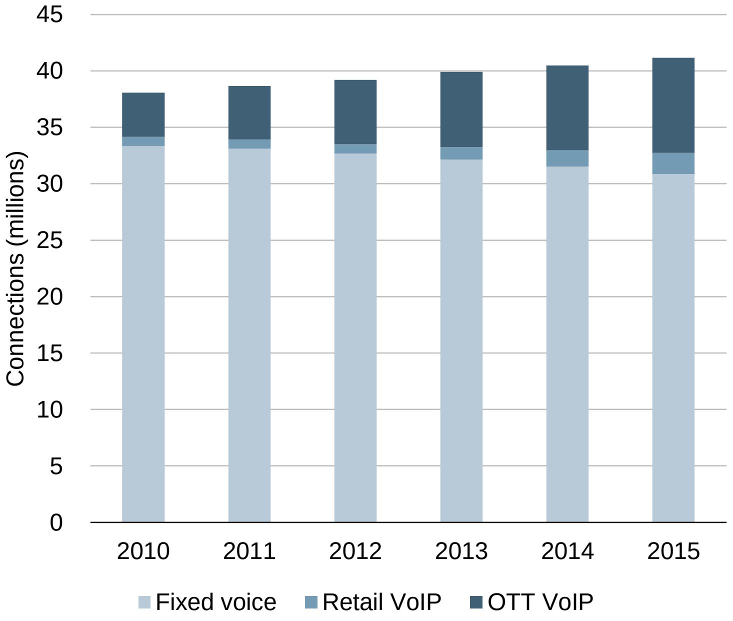


Figure 3.3: UK fixed connections (2010-15) [Source: Analysys Mason]

3.5.2 UK ISP market

The UK residential ISP market is dominated by six major players (BT, TalkTalk, Virgin Media, Sky, Orange, O_2), but there is a plethora of other medium-sized and smaller ISPs offering services to the residential, and particularly the business, markets. In addition, there are wholesalers that provide services to other ISPs. There are more than 130 ISPs[6] focused on the fixed broadband market and a further 20 or so fixed wireless broadband operators.[7] While some of these are virtual ISPs whose infrastructure is managed by a wholesale ISP, there are still a significant number of players in the UK market. This complexity is important, as we shall see below.

3.5.3 Implications for emergency VoIP location

Both the VSP and ISP markets in the UK are fragmented although there is some overlap between the VSP and ISP market, with VSPs also offering ISP services. However, it is apparent that to ascertain VoIP location according to the ND1638 architecture, described in Section 4, a significant number of VSP and ISP organisations are going to need to provide real-time data to the EHA managing the stage 1 PSAPs.

[6] Source: ISPReview website (May 2011).

[7] Source: ISPReview website (May 2011).

3.6 UK emergency service call volumes

The number of VoIP 999 calls received by the BT EHA is a very small proportion of the overall emergency service call volumes. BT estimates that currently only 10 000 per month, or 0.45% of calls, originate from a VoIP end-point, as shown in Figure 3.4. This is a much smaller proportion than would be expected based on the total number of VoIP connections: this reflects the use of VoIP as a secondary line and also a possible reluctance to use VoIP connections for emergency service calls.

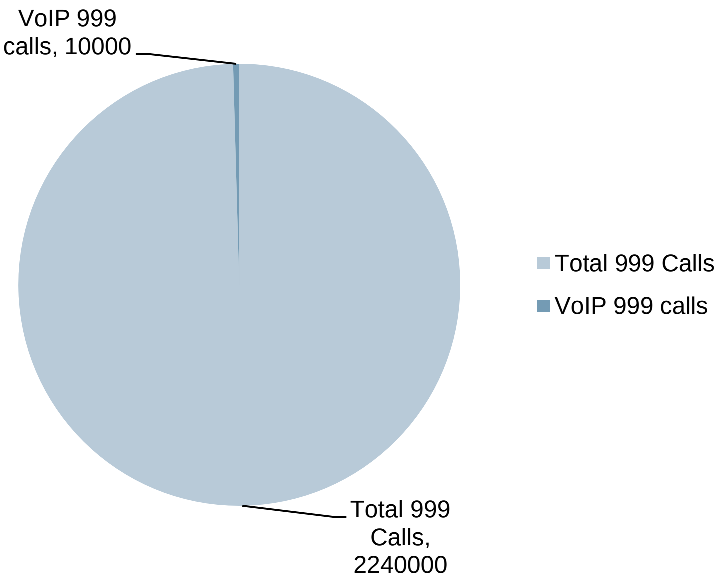


Figure 3.4: Typical monthly emergency service calls via the BT EHA (2011) [Source: BT]

Of the 4000 VoIP calls per month that are actually passed through to emergency services, 250 are classified as silent calls, where the caller did not identify a service or location. It is likely that only a small proportion of these are genuine emergencies, rather than people inadvertently dialling 999. However, the absence of location information means that it is not possible for the emergency services to deal with such calls, and this could lead to genuine emergency situations not being dealt with properly.

4 NICC solution architecture

Work has been on-going for a number of years to develop a UK national standard architecture to identify the physical locations of VoIP callers in real time, and provide that information to the EHAs. In March 2010, the first stage of this work culminated in the release of the ND1638 NICC document[8] by the NICC Emergency Location Working Group. This section summarises the key aspects of the architecture, and is intended to aid the understanding of subsequent sections that review the architecture and describe other initiatives by other organisations in different parts of the world.

4.1 Scope of the architecture

The initial version of the ND1638 architecture has been developed to enable the automatic routing of VoIP calls to a UK EHA operating the present TDM[9]-based infrastructure, where calls are presented to it via a TDM-based IUP[10] or UK-ISUP[11] interface. It focuses on VoIP calls made from DSL access lines, which is the most prevalent case in the UK.

4.2 Architectural elements and operating principles

4.2.1 Overview

The basic VoIP emergency call process, which involves a series of organisations, each of which is responsible for an element of the ND1638 architecture, is summarised in Figure 4.1 and described below.

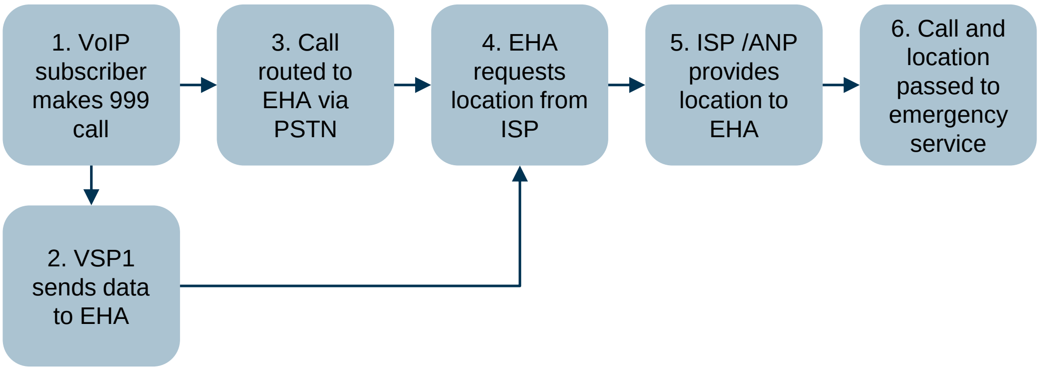

1. VoIP subscriber makes 999 call
3. Call routed to EHA via PSTN
4. EHA requests location from ISP
5. ISP /ANP provides location to EHA
6. Call and location passed to emergency service
2. VSP1 sends data to EHA

Figure 4.1: ND1638 emergency call set-up overview [Source: Analysys Mason]

[8] NICC Document ND 1638 Issue 1.1.2 (2010-3) VOIP – Location for Emergency Calls (Architecture).

[9] Time Division Multiplex.

[10] Interconnect User Part – see NICC Document ND1006 Interconnect User Part.

[11] UK-Integrated Services User Part – see NICC Document ND1007 ISDN User Part (UK-ISUP).

1. The user makes an emergency service 999 call using the VoIP service they subscribe to, which is provided by **VSP1**.

2. **VSP1** also passes CLI and IP address information out-of-band to the EHA to allow the physical address to be requested.

3. The call is now routed over an SS7 interconnect to the PSTN. This may be done by **VSP1** if it controls its own PSTN-IP Gateway (PIG), or the call may be passed to another service provider (**VSP2**) to achieve this. The call may be routed to the EHA directly, or via one or more **PSTN network operators**.

4. The **EHA** is responsible for the Stage 1 PSAP role, answering the 999 call and requesting the location of the VoIP subscriber

5. The **ISP** is responsible for providing the physical location of the VoIP caller to the emergency services to via the EHA in association with an ANP if the physical access network is provided by a different provider, for example if the ISP is taking a bitstream wholesale service from an ANP that has deployed .

   The access network provider – **ANP –** is responsible for providing the physical address of the VoIP caller to the ISP. In many cases, the ISP will be the same organisation as the ANP, but there are also many other cases where the ISP will be taking a bitstream wholesale access service from another ANP that has deployed DSL access infrastructure.

6. Finally, the EHA passes on the call and location information to the relevant emergency service.

4.2.2 Functional entities

There are a number of functional entities in the solution, each of which is the responsibility of one of the organisations described above, as shown in Figure 4.2 below.

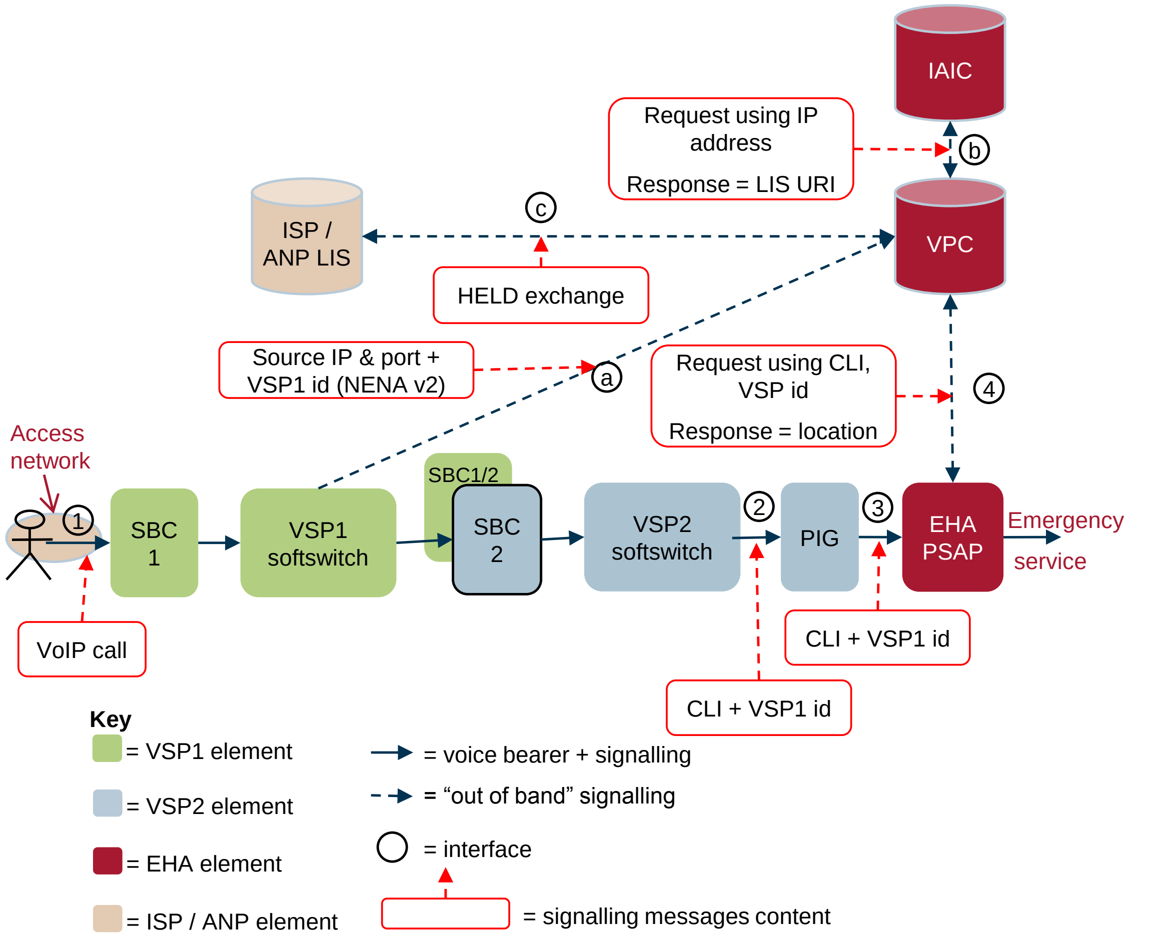


Figure 4.2: ND1638 architecture [Source: NICC/ Analysys Mason]

VSP1

- **Softswitch (or call server)** – the network element that hosts the VoIP subscriber and is the initial element responsible for routing the call to the EHA. In ND1638, this softswitch is also responsible for capturing the source IP address and port of the subscriber. This information along with the CLI and a unique identity of the VSP1 is passed to the EHA's **VoIP positioning centre** (VPC) (interface (a) in Figure 4.2 above). Note that this information may be passed to the EHA via VSP2 to ease adoption for small VSPs.

- **Session Border Controller** (SBC) – an enhanced firewall that protects the perimeter of a service provider's network from malicious attack and topology discovery. The SBC may exist between the caller and the VoIP service provider (SBC1 in Figure 4.2 above) and between VSP1 and VSP2[12] (SBC2). The SBC performs IP address translation that prevents downstream entities in the call set-up process from discovering the IP address of the subscriber. This means that the VSP must provide a mechanism for accessing the public IP address of the subscriber so that it can pass it over interface (a).

[12] VSP1 and VSP2 may each have their own SBC at their interconnect interface.

VSP2[13]

- **Softswitch (or call server) –** controls the transit of the 999 call from VSP1 to the EHA. As the interface to the PSAP of the EHA is TDM-based, this softswitch needs to control a PSTN–IP Gateway.

- **PSTN – IP Gateway** (PIG) – converts the 999 call from VoIP to TDM so that it can be accepted by the existing Stage 1 PSAPs, which currently use TDM-based technology.

- **Session Border Controller** (SBC) **–** may be implemented at the interface between VSP1 and VSP2.

EHA

- **Stage 1 PSAP** – essentially a call centre where the agents answer the 999 calls and decide which emergency service to pass the call on to. A key element of this process is knowing the location of the caller. In ND1638, the PSAP requests the location of the VoIP caller from the VPC.

- **Voice Positioning Centre** (VPC) – responsible for providing the location information that will allow the VoIP 999 call to be routed to the correct emergency service call centre. It should provide enough location information to allow the emergency service to respond quickly to the call, particularly when the caller is unable to clearly identify their location.

- **IP Address to ISP Converter** (IAIC) – used to identify the ISP hosting the 999 caller, by mapping the IP address provided by VSP1 or VSP2 to an ISP identity.

ISP or ANP

- **Location Information Server** (LIS) **–** responsible for providing location information about a particular IP address when it receives a request from the VPC. If the ISP uses an ANP for providing the physical access to its customers, it will be necessary to interact with that ANP, which will also need to have an LIS, to obtain the physical address of the 999 caller. Each ISP that has IP addresses allocated to it will require an LIS, as will each ANP.

4.3 Emergency call set-up and location information transfer

The key elements of the process to obtain location information for a VoIP emergency call in the context of the ND1638 architecture are summarised below. Lettered steps have been added to the architecture diagram in Figure 4.3 to aid the understanding of the steps.

[13] Note that VSP1 and VSP2 could be the same organisation, and so the VSP1 and VSP2 elements are combined. There can also be interim VSPs between VSP1 and VSP2.

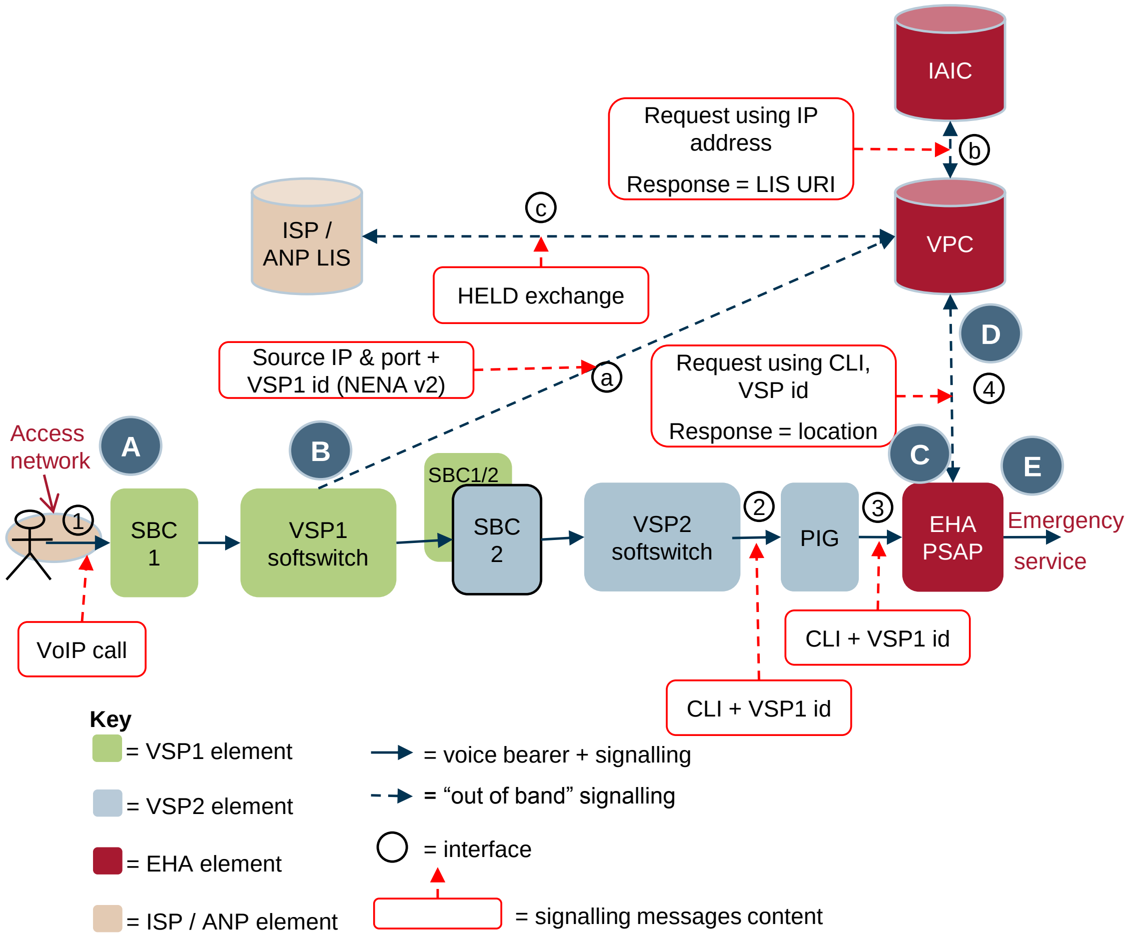


Figure 4.3: ND1638 architecture call set-up and location data transfer [Source: NICC / Analysys Mason]

Step A

The VoIP subscriber makes an emergency service 999 call.

Step B

1. The VSP1 softswitch identifies the call as an emergency service call and captures the source IP address and port of the caller, and forwards it along with its CLI and the VSP1 ID to the VPC. This information may be “proxied” to the VPC via VSP2.

2. VSP1 routes the call towards its chosen EHA either via its own PSTN-to-IP gateway, or via VSP2 which has such a gateway. The call path may involve multiple other VSPs or PSTN operators.

Step C

The emergency call arrives at the stage 1 PSAP via a TDM interface after conversion at the PSTN-to-IP gateway. The signalling message contains the CLI of the caller and the VSP1 ID.

Step D

1. The VPC receives the source IP address and port of the caller as well as the CLI and VSP1 ID, and initiates a request for the physical location of the IP address.
   a. The VPC queries the IP Address to ISP Converter which identifies the ISP that the IP address belongs to. The ND1638 architecture defines that this can be done by using Border Gateway Protocol or Domain Name System methods.
   b. Once the ISP is determined, a message is sent to the LIS of the ISP requesting the physical location of the IP address.
2. The PSAP requests the location of the caller from the VPC, providing the VPC with the CLI and ISP ID.
3. The VPC matches the requests from the VSP1 and the PSAP for the physical address.
4. When the LIS responds with the physical address, the location is passed back to the PSAP.

Step E

The PSAP agent forwards the call to the appropriate emergency service based on the location data returned from the VPC and discussion with the caller.

4.4 Interfaces

The ND1638 architecture has defined and provided guidance on the interfaces required between the elements defined in its solution. The interfaces are identified in Figure 4.4 and summarised in Figure 4.5.

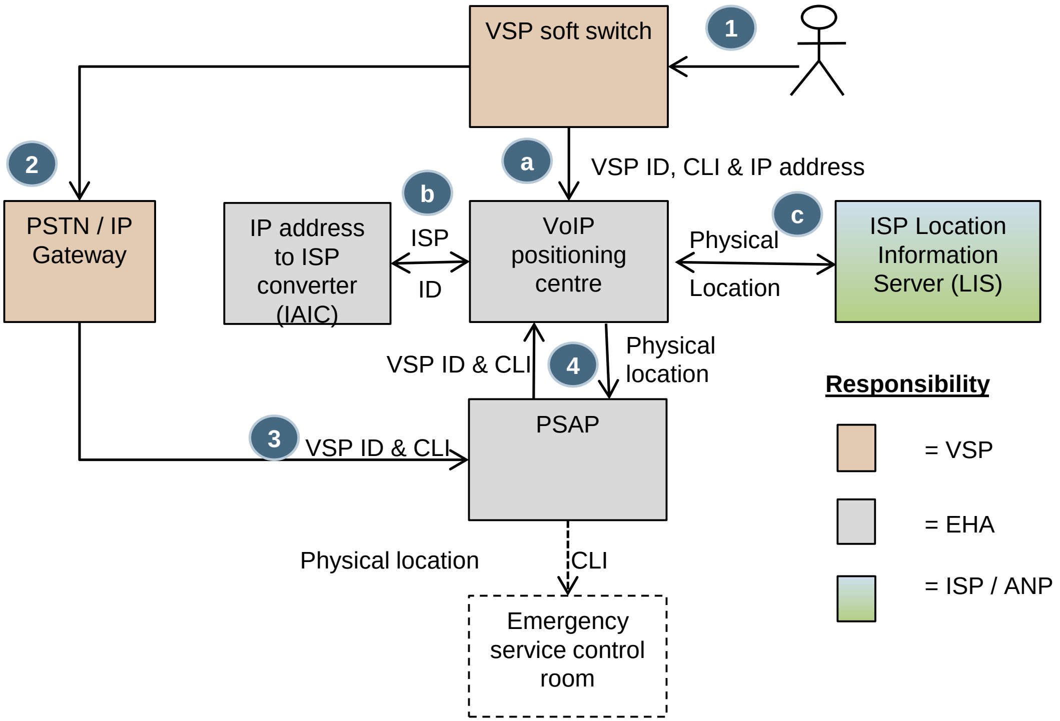


Figure 4.4: Data exchange protocols in ND1638 architecture [Source: Analysys Mason, NICC]

Interface ID	*Interface description*
1, 2	VSP defined, probably SIP
3	ND1006 (IUP) / ND1007 (ISUP)
4	EHA implementation choice
a	Based on NENA i2 V2 (but IP address replaces PIDF-LO in LIE field)
b	EHA implementation choice
c	Based on RFC5985 (HTTP Enabled Location Delivery (HELD)) and RFC5139 (Provided Civic Location Format for PIDF-LO)

Figure 4.5: Defined interfaces of ND1638 [Source: NICC, Analysys Mason]

Interfaces (1), (2) and (3) refer to the 999 call set-up interfaces used by the signalling messages that set up the voice bearer for the call. Interfaces (1) and (2) are in the VoIP environment and will typically use Session Initiation Protocol (SIP), although other signalling protocols could be used. The choice of signalling protocol is at the discretion of the ISP as long as the VSP identification (VSP ID) and CLI can be passed in the signalling messages. Interface (3) is the TDM domain interface between the VSP and the PSAP and be one of the UK SS7 interconnect standards – IUP (ND1006) or UK-ISUP (ND1007).

Interfaces (a), (b), (c) and (4) are the out of band interfaces used to determine the physical location of the 999 caller by interrogation of the LIS at the ISP. Interface (a) is based on the i2 V2 interface defined by NENA, which is responsible for developing VoIP emergency service specifications in the United States. This approach has been taken to ensure that the interface that provides location information to the VPC from the VoIP subscriber follows international standards as much as possible. However, there is one key difference. In the NENA implementation, the location information element (LIE) of the emergency services routing request contains the presence information data format – location object information, essentially the physical address information, whereas in the ND1638 implementation, the LIE contains the source IP address and port number. This is because in the NENA implementation it is the responsibility of the calling-device to request the physical location from the LIS, as this information is needed for routing to the most appropriate PSAP.

As described in Section 3.1.2, because the UK has a national stage 1 PSAP, it is not necessary to know the location of the 999 caller for PSAP routing and so it has not been necessary to put this responsibility onto the calling device. However, it should be noted that ND1638 specifically states that this approach does not preclude the LIE from being used to provide physical location data in the future.

Interface (b) is the interface between the VPC and the IAIC for determining the ISP that the 999 caller’s IP address belongs to. This interface is an EHA implementation choice as it is within the EHA and could be a proprietary interface.

Interface (c) is between the VPC and the LIS in the ISP network. This interface uses the IETF RFC5985 (HTTP Enabled Location Delivery (HELD)) protocol to request the physical location of the VoIP subscriber based on the IP address. The physical location is returned using the UK profile for the PIDF-LO (Presence Information Data Format Location Object), which is based on IETF RFC5139 (Revised Civic Location Format for PIDF-LO).

Interface (4) is between the PSAP and the VPC. As both elements are under the control of the EHA, the details of the interface are to be defined by the EHA and it can be a proprietary interface.

4.5 Other key architectural elements

4.5.1 Security

ND1638 chooses to provide general guidance on security rather than a prescriptive solution, but concedes that the number of organisations of varying sizes involved likely make it impractical for all external interfaces between organisations to be via private circuits or virtual private circuits. It specifies that the key security measures should:

- impose a minimal performance overhead as speed is critical for 999 operation
- be robust and reliable
- be widely known and easy to use for all organisations
- include authentication to prevent any attacks aimed at data corruption or interception of data for financial gain
- ensure all communications are protected from interception
- make it possible to authenticate that communications are from authorised sources
- prevent denial-of-service attacks
- be able to detect any tampering with messages by third parties.

ND1638 suggests that Transport Layer Security mechanisms may be appropriate as a low cost option for smaller operators, but it acknowledges that this may be seen as inappropriate by larger operators. Internet Protocol Security (IPSec) may be considered as another possibility.

4.5.2 Message response times

It is a general requirement of ND1638 that the response time to information requests needs to be short, to meet the requirements of the emergency service environment. For example, querying the IAIC can involve querying the domain name server (DNS) of the ISP. ND1638 proposes that the maximum network delay for DNS response should be 200ms. After that the result of the BGP4 route collector should be used to determine the ISP hosting a particular IP address.

A further example recommends the time allowed for the LIS to respond to a HELD request for a physical location should be 500ms. ND1638 does not specify an overall (end-to-end) time limit for physical location details to be provided after the receipt of a request.

4.5.3 Summary of the key aspects of the ND1638 architecture

The key aspects to note about the ND1638 architecture when comparing it to other solutions are as follows:

1. **Incorporation of other standards** – The approach of the ND1638 working group has been to follow the mature NENA i2 architecture where possible, particularly for the interfaces between VPC, VSP and ISP which will need to be implemented by a multitude of VSPs and ISPs. This should ensure some compatibility with solutions in other jurisdictions.

2. **Network-centric approach** – ND1638 takes a network-centric approach to the determination of the physical location of the 999 caller. The location of the subscriber is determined within the network based on its IP address as provided to the VPC by VSP1.

   This approach is possible because the UK uses the single stage 1 PSAP approach, where the PSAP that the call is routed to is the same for all parts of the UK. Therefore, the location of the caller is not required before call set-up. In the full NENA i2 implementation, the 999 caller's end-device is involved in the determination of its location, by initiating the interrogation of the Location Information Server and then providing that data for use in the call routing process. This is described in more detail in Section 6.2.1.

3. **Focus is on DSL access only** – The current version of ND1638 focuses on the emergency location of subscribers using a DSL access. While this is the most common access mechanism in the UK market, it needs to be noted that this approach excludes other access mechanisms such as cable networks, Wi-Fi hotspots and private networks (including VoIP subscribers using a corporate VPN).

4. **No other next-generation services are addressed** – ND1638 focuses specifically on VoIP services and not on other next-generation services such as text (SMS, messaging and real-time text), images and video, which have, for example, been included in the NENA i3 specification development (see Section 6.2.1).

4.6 Working group – plans for future work

Since version 1.1.2 of ND1638 was released in March 2010, the NICC Emergency Location Working Group has continued to work on developing the architecture further. This has included work on considering other access mechanisms such as cable networks, private networks and Wi-Fi hotspots, which are not covered specifically in the initial version of ND1638. We understand that the work to extend the architecture to cable networks is straightforward and largely complete. Other use cases for Wi-Fi hotspots and private networks have been examined. It is likely that the NICC will release separate use case documents for the different access mechanisms, but no formal date for release of this has been provided.

The working group has also recently been asked to start considering how next-generation services may be incorporated into the UK emergency service calling environment.

5 Review of proposed NICC architecture

In this section we discuss issues raised in our interviews with a number of stakeholders in the area of VoIP emergency services, held as part of this study. After summarising the participants' views of the ND1638 initiative (both positive and negative), we then discuss their estimates and concerns regarding the costs of implementing ND1638, and their views on its reliability, as well as a range of other issues. Finally, we summarise the progress that has been in ND1638 implementation.

5.1 Review approach

Analysys Mason has conducted a number of interviews with stakeholders in VoIP emergency services, covering UK-based organisations and other organisations involved in standards development in this area in the United States and Europe. We have received input from 13 individuals or groups of people from the following areas (note that some interviewees can be classified into more than one category):

- UK EHA
- Member of the NICC Emergency Location Working Group
- Internet Telephony Service Provider Association
- Small sized integrated VSP and ISP
- Medium sized integrated VSP and ISP
- OTT VSP
- Large ISP
- System vendor
- Representative of IETF
- Representative of NENA
- Representative of EENA.

The remainder of the document will not specifically identify participants, in order to protect the confidentiality of their comments, but Analysys Mason wishes to thank everybody for their participation and the useful insight they provided.

It should be noted that we attempted to gain greater participation, specifically from other members of the ISP community, but the businesses we contacted either declined to take part or did not respond to our requests.

5.2 Study participants comments on the ND1638 architecture and implementation

There was general support amongst participants that a better solution is required to providing location. Presently, the onus is on the end-user to update their location, which is passed to the EHA via a periodic file transfer process. This is unsuitable as a robust solution for use by nomadic voice users. All participants considered the ND1638 architecture to be technically feasible to implement. However, there was variation in the strength of their support, with many participants highlighting issues that concerned them in the ND1638 architecture. A summary of the points raised is provided below.

5.2.1 Comments in support of the architecture

Positive comments in support of the architecture are summarised as follows:

- A good solution meeting UK network requirements and the respondent plans to seek budget for 2012/13 implementation.
- A robust solution included as part of the development strategy of the operator.
- A location database with real-time capability as defined in ND1638 is the way to go.
- It is based on the very mature NENA i2 architecture developed for North America.
- It can easily be migrated to support IP-enabled emergency call centres.
- Architecture development has involved direct stakeholders such as small VSPs and ISPs to ensure the architecture is practical and deployable.
- Current access networks (fixed and mobile) require the access network to provide emergency location, so it follows that ISPs/ANPs need to provide the location for VoIP emergency services as defined in ND1638.

5.2.2 Comments questioning aspects of the architecture and process

However, there were a number of comments questioning the architecture in a number of areas:

- cost of implementing the architecture
- reliability of the solution in determining location
- range of access types supported
- alignment with other standards
- support across international borders
- support for VSP subscribers without PSTN CLI
- need for further implementation guidance.

We report the comments below, and deal with the issues arising in subsequent sections

Cost of implementing the architecture

- The requirement of providing real-time reconciliation of CLI, IP address and reconciliation will require a significant investment. This architecture will be difficult to implement for smaller ISPs with small capital budgets.

- The current solution is balanced in favour of smaller VSPs, with in-house or open source softswitch/call server platforms. The cost implications of upgrades to vendor-supplied softswitch/call server platforms have not been considered by the working group developing the architecture.

Reliability of solution in determining location

- ND1638 may not deliver the physical location in 100% of cases, due to difficulties that may arise in managing large, dynamic real-time databases, and so give a false level of security to the end-user.
- It does not support other methods for determining location, such as by the end-device itself via mechanisms such as the Global Positioning System (GPS).

Range of access types supported

- The architecture needs to cover a wider access base, e.g. cable networks, corporate networks and Wi-Fi hotspots.
- In some cases (e.g. within private networks, Wi-Fi hotspots) it may be difficult to determine the IP address of the caller.

Alignment with other standards

- ND1638 is UK-centric and may be superseded by European or other international standards.
- Other standards are “more open-ended and aimed at the future” with consideration being given to next-generation emergency services that include using text, images or video.

Support of architecture across international borders

- The solution does not address callers using a non-UK-based service provider, as VSPs in other jurisdictions do not have an association with UK VPCs.
- Due to the scarcity of IPv4 addresses, IP addresses are becoming less closely associated with particular countries, and ISPs ‘import’ addresses from countries with larger supplies. While a well-maintained IAIC function will be able to handle this in the ND1638 implementation, it may become an issue if an end-device needs to adjust its behaviour based on the country it is in, and uses the IP address to determine the country.

Support for VSP subscribers without PSTN CLI

- Not all VSPs associate a CLI with the VoIP subscriber, which causes an issue with ND1638 as CLI is required.

Need for further implementation guidance

- Additional implementation guidance, specification and description are required to support ISP integration of location servers in a consistent manner.
- Security for accessing the LIS should be carefully defined.

- Message response times, specifically the HELD protocol physical location response time from the LIS (500ms), are too short and should allow repeat requests for the data.
- If left alone, the industry probably could not make the implementation work as too many links could break down. Overall programme management is required to ensure consistency and robustness.

In the following three sections we consider these concerns raised by stakeholders in more detail and, where appropriate, describe how they may be addressed. We have divided the issues into (a) concerns about implementation costs, (b) doubts about the reliability of the solution, and (c) other issues.

5.3 Estimated costs of implementing the architecture

5.3.1 Summary

As part of our engagement with the study participants, we asked them to estimate the costs of implementing the ND1638 solution and on-going operational support. None of the VSPs, ISPs and EHAs we asked has reached the stage of producing a detailed costing that would be suitable for obtaining investment approval from their business. However, they were able to provide estimates for the key elements based on high-level assessments. These are shown in Figure 5.1.

Element	*Development cost range*
EHA	c. £200 000 – £800 000
VSP softswitch / call server	c. £50 000 (in-house) c. £100 000 – £250 000 (vendor-supplied upgrade)
LIS	c. £50 000 – £1 million
Integrated VSP / LIS development	c. £200 000 – £2+ million

Figure 5.1: Estimated development costs – summary [Source: Analysys Mason, study participants]

Study participants were more reluctant to estimate on-going operational costs, but estimates ranged from “minimal” to 5% of capex investment. Some concern was shown as to the knock-on impact of upgrades to the network on emergency VoIP location elements.

5.3.2 Breakdown of development costs and business impact

Capital expenditure

Figure 5.2 below provides a list of the development costs identified by stakeholders that can be expected to be counted as capital expenditure, together with a brief description of the development required and an indication of the impact of such costs on the business.

Participant	*Area*	*Description of development*	*Estimated capital cost*	*Business impact on participant*
1	EHA	In-house development of VPC and IAIC systems and interfaces	c. £200k	Project will need to demonstrate it can break even
2	EHA	Development of VPC and IAIC systems and interfaces as a standalone system by external developer	c. £700k – £800k	Larger than annual EHA budget.
3 (large VSP/ISP)	VSP	Development of vendor supplied softswitch to provide CLI / IP address data	c. £100k – £200k	VSP plus ISP development would be "low end of large budget item"
	ISP	Development of LIS including provisioning development, APIs, implementation, laboratory set-up, carrier-grade NAT compatibility, testing, security solution	c. £1mn	
4 (small VSP/ISP)	VSP / ISP	Development of VSP interface (a) and real time interaction between voice and customer database to meet LIS requirements	c. £200k	30% of annual capital expenditure budget
5 (medium ISP/ VSP)	VSP / ISP	Development of VSP interface (a) and LIS, implementing real-time interrogation capability requiring a substantial network re-design – network includes a number of disparate elements due to business expansion by network acquisition	c. £1mn – 2+mn (c. £500k hardware plus development of £500k – £1.5+mn)	Annual capital expenditure historically £500k
6 (medium VSP/ISP)	VSP / ISP	Development of VSP interface (a) and LIS (interface to RADIUS solution) plus SBCs for logical routes[14] (relatively new ISP network)	Own softswitch: c. £50k; vendor softswitch: c. £250k; system development: c. £75k; SBCs: £80k	Total is 15% of capital expenditure budget

Figure 5.2: Breakdown of estimates of development costs by participant [Source: Analysys Mason / study participants]

The costs quoted show a large variance between the different organisations. This can be attributed to the following factors:

- **Approach to development** – for example, the cost differential between in-house and bought-in solutions.
- **Current design strategy and needs of the current business** – for example, the stakeholder's current business may not have a requirement to link IP addresses to real addresses in real time, and the network may need to be re-designed significantly to support this. As another example,

[14] The participant suggested the implementation of specific logical routes for 999 calls that would allow 999 calls to pass through SBCs without translating the 999 caller end-device IP address.

an ISP that has expanded by acquisition may have a responsibility for a number of disparate networks that have yet to be integrated. The requirement to interface the LIS to a number of different platforms within the same network will increase integration costs (e.g. Participant 5 in Figure 5.2), whereas a relatively new ISP that has expanded organically may have a much simpler integration task (e.g. Participant 6 in Figure 5.2).

- **Future design strategy** – for example, the introduction of carrier-grade NAT (Network Address Translation) to conserve IPv4 address ranges may address a specific problem, but it also brings additional complexity to mapping IP addresses to physical addresses in real time.
- **Size of network** – for example, the LIS function can become more complex in a large network using many access networks, and also possibly needs to address integration issues in cases where a network has grown through acquisition of other networks. In the case of the LIS, the system integration costs are likely to outweigh the in-house development costs or the purchase costs of the LIS itself.
- **High-level nature of cost estimates** – can lead to discrepancies as both under- and over-estimating is fairly likely to occur.

While we have not been able to establish definitive costs, it is clear that the capital expenditure will be a significant investment for all businesses that have provided cost information.

Operational expenditure

Study participants were generally less forthcoming in the detail they provided on operational expenditure. In general, they preferred to reserve judgement. However, in the comments that were made, there were variations. A couple of participants considered that on-going costs would be small or minimal, as the process would be largely automated – a figure of 1% of the capex investment was quoted in one case.

Two other participants were less optimistic. One suggested an additional senior support engineer would be required (with overall annual support costs of £200 000), and the other questioned whether on-going process could be entirely automated and thought significant effort would be required to accommodate network changes and their associated testing prior to implementation.

It is reasonable to say that those participants that had most concerns about the cost of implementation also were also more concerned about the on-going operational costs.

5.4 Reliability of the solution in determining location

There are four key factors that will determine the reliability of the ND1638 in ensuring UK network coverage of VoIP emergency location is determined for each VoIP 999 call: (a) access technology, (b) EHA implementation, (c) VSP implementation and (d) ISP/ANP implementation. These factors are summarised in Figure 5.3. Each can potentially limit the coverage of the solution and hence the proportion of VoIP calls to the emergency services for which the real-time location of the 999 caller can be determined using ND1638 architecture. The issues are discussed below.

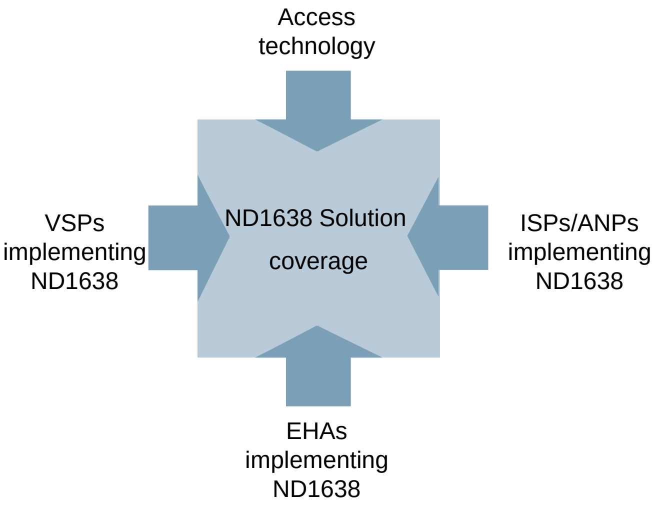


Figure 5.3: Factors impacting coverage of ND1638 solution [Source: Analysys Mason]

5.4.1 Access technology

The current version of the ND1638 architecture is targeted at supporting a DSL-based architecture. This is a sensible first step as nearly 80% of broadband connections are delivered over DSL in the UK (see Figure 5.4).

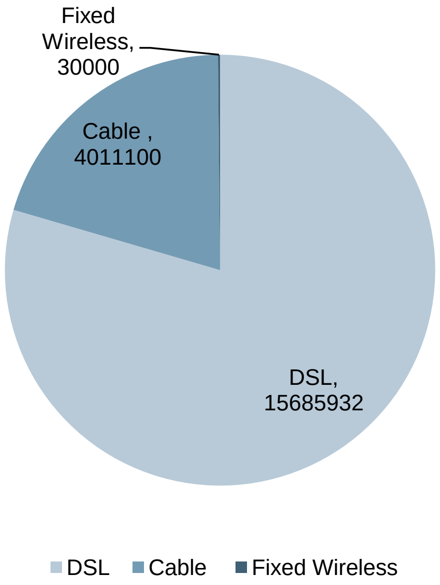


Figure 5.4: UK retail broadband connections by technology (end-2010) [Source: Analysys Mason]

We understand that the NICC working group has made good progress in developing a cable network use case, and this will allow very nearly 100% of retail access connections to be addressed. It is also likely that the architecture could be extended to fixed wireless relatively straightforwardly if priority is given to this within the NICC.

It should be noted that the connections in Figure 5.4 do not take into account of

- the connections of companies, not using DSL or cable modem access, who have a growing number of VoIP users, who will not be within the scope of the ND1638 architecture
- a much smaller but growing number of users using VoIP service at Wi-Fi hotspots.

5.4.2 EHA implementation

Clearly, for the architecture to be supported it must be implemented by at least one of the two primary EHAs. However, if one of the EHAs decided it did not wish to implement ND1638, it should be possible for VSPs, ISPs and ANPs to work with the EHA offering service, although some VSPs would inevitably need to change their emergency service provider.

5.4.3 VSP implementation

There are 46 full members of the ITSPA providing VSP services in the UK (see Figure 5.5), and there may be other VSPs offering services.

Aql QMA	BT	Birchills Telecom Limited	Ciptex Ltd
CommsSolutions	Coms plc	Easy-Dial Ltd	Gamma Telecom
Ghost Telecom	Gradwell Dotcom Ltd	Inclarity Ltd	Inspiredtel
Localphone Ltd	Loho Ltd	Lyndos.net	Magrathea
Nationwide Telephone Assistance Ltd	Netplan Internet Solutions LTD	Node4 Limited	Ok Telecoms
Orbis Telecom	Orbtalk Ltd	Phonecard Services Ltd	Poundbury Systems Ltd
Simwood eSMS Limited	Solutios Limited	Sota Solutions Limited	Spitfire Network Services Ltd
Stripe 21 Ltd	SureVoIP	Telappliant	TeleWare Telecom
Timico Ltd	Truphone	VIVA Telecommunications	Voicenet Solutions Ltd
VoIPon Solutions	Voxbone	VoiceHost	Voxhub
Voipfone	VoIP User	VoIPtalk	Vonage Limited
WI-Manx Limited	Zen Internet		

Figure 5.5: UK service providers that are members of ITSPA, May 2011 [Source: ITSPA website]

While BT is the largest member, in general members are small and medium sized businesses – reflecting the fragmented nature of the VSP market in the UK. Many of the providers also offer ISP services, either as an ISP themselves or via a white-label service from another service provider. There are other businesses offering VoIP services that are not ITSPA members: Skype is probably the most widely used service provider that is not a member.

While ITSPA members such as BT, Gradwell and Magrathea have taken a prominent role in developing ND1638, we understand that there are members that have not followed ND1638 developments closely, and that have concerns about implementation costs. This may mean there is reluctance from some VSPs to implement the ND1638 solution. However, this issue could be eased to some extent by the ND1638 architecture allowing VSPs to "proxy" data to the VPC via a VSP2 – this approach could reduce implementation costs for some VSPs.

Analysys Mason estimates suggest that at end-2010, there were around 800 000 retail VoIP subscribers (residential plus small businesses) purchasing "residential-like" managed voice-over-broadband services. Many of these subscribers are likely to be customers of ITSPA members. If some VSPs did not implement ND1638 then there would be a corresponding impact on the number of VoIP subscribers that had a VoIP emergency location capability open to them.

In addition, at the end of 2010 there were nearly 4 million users of OTT VoIP (e.g. Skype and Vonage). Although such services are often used as a "second line" and may not be most users' first choice for making 999 calls, these still represent a significant number of subscribers, even if many of these (in the case of Skype) may not have signed up for the ability to make calls to E.164 numbers.

5.4.4 ISP/ANP implementation

The UK retail broadband DSL market is dominated by six major players which together account for nearly 94% of the market (see Figure 5.6).

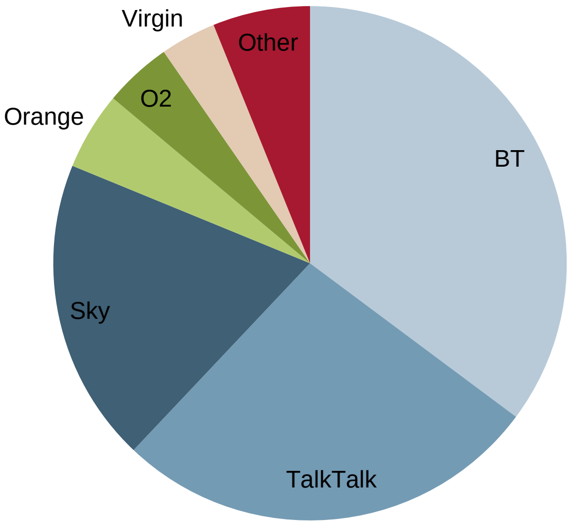


Figure 5.6: UK DSL market connections by operator, end-2010 [Source: Analysys Mason]

From one perspective, to achieve maximum DSL coverage for the ND1638 solution, it is important that these top six providers implement the solution. However, other ISPs still account for nearly 1 million DSL connections, and it also needs to be considered which ISP VoIP subscribers are most likely to use.

For the 4 million OTT VoIP users, we expect that their propensity to use a particular ISP is in line with the general market share of the UK market. However, a significant number of the 800 000 retail VoIP residential and small business customers taking a managed service are likely to be using a broadband service also provided by their VSP. This may be provided directly by the VSP or as wholesale product from another ISP. In these cases, the ISP may not be a top-6 provider, but another provider specialising in providing wholesale broadband services to resellers. This may result in a disproportionate number of retail VoIP subscribers using a broadband service other than from one of the top 6, which makes it important to ensure a wider range of ISPs participate in ND1638 implementation.

It should also be noted that the UK ISP market is very fragmented outside of the top 6 providers. As stated in Section 3.5.2, there are in excess of 130 fixed broadband ISPs in the UK market, and only 6 of the ISPs on that list are also members of the ITSPA. Providing maximum coverage for ND1638 implementation will therefore require the co-operation and co-ordination of a large number of service providers. Further analysis is required to ascertain how many providers are virtual ISPs and VSPs reselling services from other providers' networks – this could result in a simplification of the interaction needed between VSPs, ISPs and the EHA. However, it is still likely to be challenging to maximise coverage by ensuring as many VSPs and ISPs deploy the architecture as possible.

5.5 Discussion of other comments questioning aspects of the architecture

5.5.1 Range of access types supported

ND1638 has been developed specifically to support the DSL access use case. It therefore does not define how VoIP emergency location should be supported for other access types such as cable networks, private networks (such as those deployed by businesses and other organisations) and Wi-Fi hotspots. The key issue here is how to ensure that the VSP is able to provide the VPC with a public IP address that can be used to interrogate an LIS that provides the physical address. In the case of cable networks, primarily Virgin Media's network, we understand that a clear method for accommodating them into the ND1638 architecture has been established, but not yet published.

ND1638 acknowledges the potential difficulties in the private network environment, where the VSP1 may attempt to provide a private address which is not unique to that location and cannot be linked to a physical location by an ISP/ANP's LIS. It suggests that in this case, where an enterprise is effectively acting as a VSP1, it could be required to provide a public IP address to the VPC and also provide its own "enterprise LIS" function. ND1638 indicates that further details will be the subject of a future issue of the document. However, it needs to be considered whether it is reasonable for all sizes of private network to take on this additional requirement of an "enterprise

LIS". Issues such as defining the physical location within a large building or campus to a level that is useful to emergency services without putting an unreasonable administrative overhead on the "enterprise" will need to be examined. This issue is being considered as part of the NENA implementation in United States, including examining the capture of location within a building or campus.

The NICC working group has also spent time considering the issue of Wi-Fi hotspots, and has used the BT Openzone set-up as a case study for ensuring location can be determined in line with ND1638 requirements. We understand that its results are encouraging, although they have not yet been formally released into a use case. It also needs to be considered whether the location of the Wi-Fi base station provides the location at a sufficient level of granularity[15]. It needs further investigation as to whether, in this case, combining this data with location data from the user device would be more appropriate. In addition, similar techniques to those used within a mobile network to provide location data, or techniques such as triangulation between Wi-Fi base stations, might be considered to provide a more reliable result – though they may be challenging to put into practice. The cost and viability of implementing a common approach will be key considerations.

5.5.2 Alignment with other standards

Some participants expressed concern that the ND1638 approach has been devised to meet specific UK requirements, but is not compatible with other standards. At present, the main specification that ND1638 can be compared to is the NENA i2 specification (which is discussed further in Section 6.2.1). ND1638 does include the same key architectural elements such as the VPC and the LIS. In addition, the key external interfaces – Interface (a) and Interface (4) are based on NENA and IETF standards, as described in Section 4.4, providing significant alignment with standards overall. However, some issues remain, as discussed below.

Location from end-device versus location from the network

The different PSAP architectures in the UK and the United States have resulted in a different approach to obtaining the physical location. In the United States, the end device of the 911 caller is responsible for obtaining its physical location from the LIS so that the information can be used to ensure the call routes to the correct PSAP – in the Unites States, PSAPs are implemented on a local or regional basis. As the UK takes a single, national stage 1 PSAP approach, this "early" knowledge of physical location is not required and has not been implemented. This does mean that the end-device will need to operate differently in a NENA environment to the ND1638 environment, which will cause issues for end-device developers which operate in both markets, as they will need to support different versions of their products. Overall, there are advantages in both implementations – the balance will depend on the particular network circumstances, as shown in Figure 5.7 below.

[15] It is possible that the Wi-Fi hotspot could cover an area large enough for the location of the access point to be insufficiently precise for the emergency services.

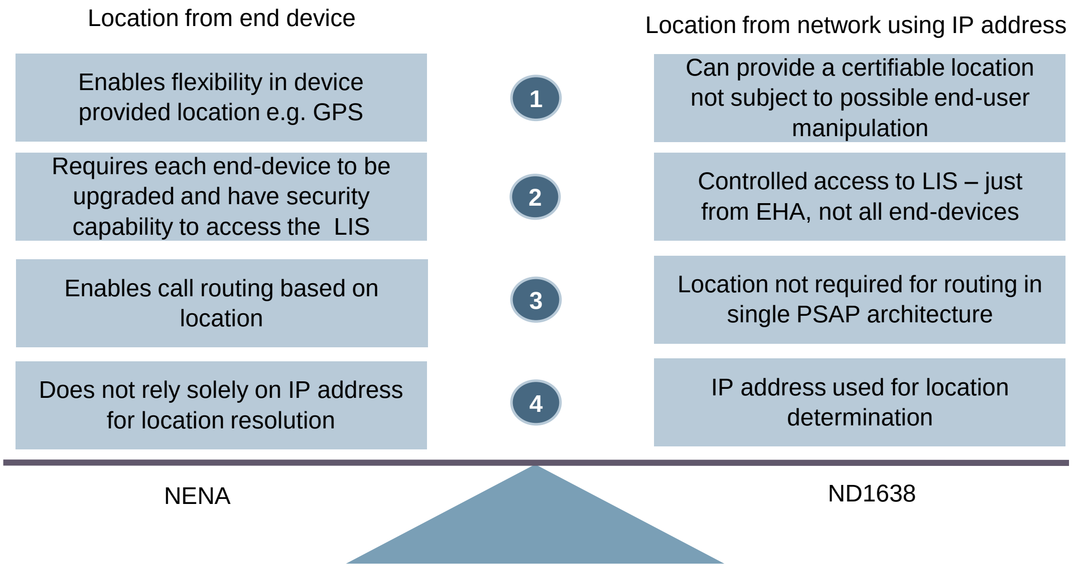

Location from end device
Location from network using IP address
Enables flexibility in device provided location e.g. GPS
1
Can provide a certifiable location not subject to possible end-user manipulation
Requires each end-device to be upgraded and have security capability to access the LIS
2
Controlled access to LIS – just from EHA, not all end-devices
Enables call routing based on location
3
Location not required for routing in single PSAP architecture
Does not rely solely on IP address for location resolution
4
IP address used for location determination
NENA
ND1638

Figure 5.7: Comparison of NENA and ND1638 location request mechanisms [Source: Analysys Mason]

Each of the four numbered issues covered in Figure 5.7 are covered below:

1. If the end-device is already used to determine physical location, this makes it easier to include other location mechanisms such as GPS within the device, which can provide an input to location determination. It can also be argued that locating the caller based on the IP address makes it less likely that there can be any manipulation that may cause the end-device to provide an incorrect location. Whilst it is to be hoped that nobody would want to manipulate location information that is to be used for emergency calling purposes, use of the LIS for other purposes might lead to greater levels of concern on this point.

2. The NENA implementation requires the end-device to have the functionality and sufficient security capability to be able to access the LIS in a secure manner. This will require each end-device to support the architecture (i.e. new end-devices), whereas in ND1638 no such upgrade is required. In addition, ND1638 provides more controlled and manageable access to the sensitive data contained in the LIS, as only the VPC will have access, rather than all end-devices.

3. The NENA implementation does enable routing based on the location, but in the UK this is not required due to the implementation of a national stage 1 PSAP.

4. ND1638 as currently defined relies on the passing of an IP address to the VPC for physical address resolution. The use of the end-device in the NENA implementation makes it easier for other mechanisms such as handset GPS location to be used, which may provide greater reliability of results in some circumstances where the location from IP address could be a wide area (e.g. Wi-Fi hotspot). However, while ND1638 does currently stipulate the passing of the IP address in the location information field of the emergency services routing request over Interface (a), it also states that in the future it could contain physical location information in the form of the PIDF-LO.

Incorporation of next-generation emergency service capability

The remit of the NICC Emergency Location Working Group in developing ND1638 has been to focus on VoIP emergency location assuming the EHA elements of the network remain in a TDM environment. This is reflected in the architecture that has been formulated. However, the working group has recently been asked to start considering aspects of next-generation service (text, images and video). This is still in its early stages.

5.5.3 Support of architecture across international borders

The support of VoIP emergency location services across international borders presents a challenge from a number of perspectives. For example, if a 999 caller in the UK does not have a UK-based VSP, then it may well not have an association with a UK VPC, making it impossible to establish location details.

An end-device that expects to be used across international borders could try to establish the country it is in from the public IP address it is connected to. However, the increasing tendency for ISPs to use address ranges from other countries (due to the scarcity of IP addresses in their own country) makes this increasingly complex, and likely to result in errors.

There has been not been any significant effort to date to address these issues, but it is likely to gain greater attention as EENA embarks on Europe-wide emergency VoIP location standardisation (further details are given in Section 6.3).

5.5.4 Support for VSP subscribers without PSTN CLI

Some service providers offer VoIP subscribers the ability to make calls to the PSTN without the caller having their own CLI. This causes a basic problem with the ND1638 solution, as the CLI is used to identify the subscriber at the EHA, to allow the physical location to be requested for the call. The ND1638 solution will therefore not work for such a scenario. This issue could be addressed in three ways to meet the requirement to be able to dynamically determine the physical location of the subscriber:

1. Require that every subscriber with capability to call emergency services has to be allocated a CLI. This would probably be an interim measure prior to the EHA being IP-enabled. It would cause some additional costs to the VSP.
2. The VSP2 that has PSTN access and a PSTN number range could allocate CLIs on a call-by-call basis and pass the CLI allocated over Interface (3) and Interface (a) to the EHA. This would introduce a new numbering concept at odds with CLI being linked to a specific subscriber, which might cause some difficulties in identifying the subscriber. Some softswitch equipment vendors might find it difficult (and be reluctant) to implement such functionality, as it moves away from the concept of the CLI being a key way to identify a specific subscriber.

3. The EHA could be IP-enabled, probably using a SIP signalling interface, so that forms of subscriber identification other than CLI can be accepted. This is likely to happen in the evolution of the ND1638 architecture, but present indications from stakeholders suggest that this is likely to be two or more years into the future.

5.5.5 Need for further implementation guidance

General

The implementation of the ND1638 architecture will be a complex process, with a large number of organisations being involved. Section 3.5 highlighted that over 50 VSPs and around 150 ISPs may need to get involved in the process to ensure full coverage. As organisations are likely to have varying levels of interest in, and commitment to, the project, strong implementation programme management will be required.

The implementation programme may benefit from a companion document to ND1638 providing more detail on operational issues and the standard technical approach to DSL environments, to encourage deployment standardisation. NENA has taken this approach by developing operational and technical information documents.

LIS development

One participant expressed a need for additional implementation guidance, particularly to ensure the integration of the LIS in a consistent manner. A significant proportion of ISPs use BT IPStream (or its 21CN successor Wholesale Broadband Connect) for their DSL access. The participant specifically requested that BT be mandated standardise the operations of pushing location from cable-plant providers to ISPs. They considered that the mechanism would ensure that the ISP has access to location information when required, ensuring minimal delays or possible failures in the event of an emergency call.

The participant also suggested that the process would benefit from a standard mechanism for the LIS to query the ISPs’ Authentication, Authorisation and Accounting (AAA) servers to obtain data relevant to the process. This is not addressed by ND1638 (or indeed by IETF). It was suggested that this could help reduce the cost of the LIS to ISPs as it would reduce the need for large ISPs to monitor significant traffic, possibly from many datastreams. This is indeed a matter that has been raised by other participants, and appears to be a significant issue in LIS development costs.

Security of data

As described in Section 4.5.1, ND1638 provides guidance on the security considerations for implementing ND1638, particularly related to the security of the data connections. Particular concern has been expressed by one participant that due to the sensitive nature of LIS data (specifically, physical address data), the architecture document needs to be more specific and describe very robust mechanisms to ensure that unauthorised access to data is minimised.

ND1638 does recognise the dangers of data being "…corrupted deliberately or intercepted for financial gain", but effectively leaves the relevant parties to define their preferred implementation based on technology preferences and budgetary constraints. While this provides flexibility and the possibility to match the implementation method to the available budget, some further definition may be of benefit, to ensure some commonality of approach across the large number of VSPs, ISPs and EHAs that will need to consider this.

Message response times

ND1638 makes a recommendation that the response time for a HELD message from the VPC to the LIS for the physical address of a 999 caller should be 500ms. There is also no mechanism for a re-try should the first request be unsuccessful. This relatively short response time and lack of provision for re-try is an acknowledgement of how important it is to get the information in an emergency situation as quickly as possible. It has been suggested that in some circumstances this may be difficult to achieve, particularly if an ISP is implementing carrier-grade NAT[16], which is being considered by UK ISPs to conserve IP address space. Carrier-grade NAT will put a processing strain on keeping the LIS updated in a large network, which may impact the ability of the LIS to respond quickly to EHA requests.

5.6 Progress in ND1638 implementation

NICC work and prototyping

The focus of the NICC working group since the March 2010 publication of ND1638 has been described in Section 4.6. Outside of the working group our discussions with the stakeholders suggest there has been very little (if any) progress towards implementation. For example, nobody has been involved in any prototyping of the architecture, unlike in the case of the NENA implementation in the United States, as described in Section 6.2.1. However, the NENA prototyping will provide some benefit to the ND1638 where the implementations overlap, such as the HELD interface used for interrogating the LIS.

Implementation plans

A number of the organisations we talked to have made some initial high level plans towards implementation, but nobody has yet firmly committed ND1638 to their development plans. It appears that – certainly for larger organisations – the first opportunity for implementation is likely to be FY12/13. It is probably true that if implementation does not gather further momentum in the next few months, then it could be delayed until the year after that due to the budgetary planning cycle. It should also be noted that for two of the VSP/ISPs we talked to, it was the first time that ND1638 had been brought to their attention. If this pattern is repeated, as seems likely, over the

[16] Carrier-grade NAT is used to conserve IP addresses and help with the problem of IPv4 address exhaustion. End-points are not given public addresses, but instead private addresses that are translated to public addresses in the ISP's network. Carrier-grade NAT has been considered in the development of ND1648 and will be considered further during the development of private network use cases.

rest of the VSP and ISP community, then there is a significant education programme that needs to be completed.

Barriers to deployment

There is a widely held view that it will be difficult to get every VSP, ISP and ANP to participate in ND1638 without further "encouragement". Comments made by participants mentioned the following issues:

- There is no incentive to spend money if there is no direct commercial gain and the customer does not buy the service directly. This was mentioned repeatedly in the context of it being difficult to persuade ISPs and ANPs to take part, and it was commented that costs might be particularly difficult to bear for smaller organisations.

- The ISP/ANP community has not previously taken part in emergency calling provision, and it may be difficult to convince them that they should now, although a robust solution to emergency calling location over the Internet does rely on their co-operation. It was commented that experience in other access technologies in the UK and around the world suggests their co-operation may not be secured unless they are compelled to do so. However, it was also highlighted that an effective LIS could be used as the basis for other commercially attractive location-based applications. It was also mentioned that an LIS service managed by a third party provider might provide a more finally attractive option for some ISPs/ANPs.

- Those organisations that see themselves as software application providers rather than voice communications providers may be reluctant to take part.

- Organisations may be reluctant to take part unless they are assured that there is a programme management structure in place to ensure that it can be successfully implemented across enough of the UK network to make it worthwhile.

- Reservations were expressed about how future-proof ND1638 is and whether it may be superseded by another international specification.

- Foreign-based Internet telephony service providers may resist meeting ND1638 requirements as they may not wish to implement country-specific solutions. It was also mentioned that they may be reluctant to pass subscriber data across borders (even CLI to VPC) due to data protection concerns.

The comments expressed here are discussed further in Section 6.2.1 in the context of the experience in the United States.

6 Other VoIP and NG112/911 initiatives

There are a number of organisations working on NG112/911 solutions, including various standards development organisations (SDOs) and public safety associations in Europe and North America. In this section, we consider the work and initiatives being undertaken by the following organisations:

- Internet Engineering Task Force (IETF) – ECRIT and GEOPRIV
- National Emergency Number Association (NENA) – NG911 (i2 and i3) and ICE
- European Emergency Number Association (EENA)
- 3rd Generation Partnership Project (3GPP) – IMS
- Open Mobile Alliance (OMA).

We also look at the Emergency Services Workshop (ESW) series – the ongoing effort in the emergency services community to coordinate global standards and technologies for emergency calling and emergency notification.

6.1 IETF – ECRIT and GEOPRIV

The Internet Engineering Task Force (IETF) is a loosely self-organised group of individuals who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications. The IETF is not a traditional standards organisation, although many specifications that are produced become standards. The IETF has developed ECRIT (Emergency Context Resolution with Internet Technologies) and GEOPRIV (Geographic Location/Privacy).

ECRIT achieves the context resolution of emergency calls placed by the public using VoIP and general Internet multimedia systems, where Internet protocols are used end-to-end.

The GEOPRIV working group’s remit is to develop and refine representations of location in Internet protocols, and to analyse the authorisation, integrity, and privacy requirements that must be met when these representations of location are created, stored, and used. GEOPRIV essentially offers a system for networks to provide location information to subscribers, as shown in Figure 6.1 below, whereby the network advertises a location server and the client requests location information from the server. It also enables third parties (e.g. PSAPs) to ask for subscriber location information.

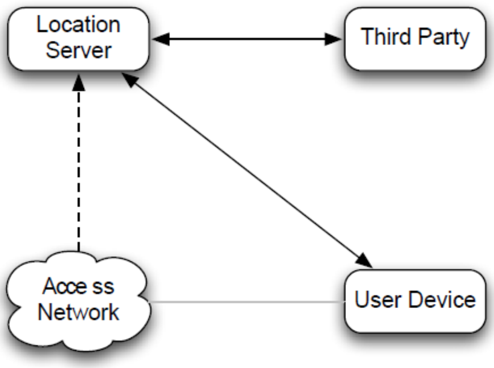
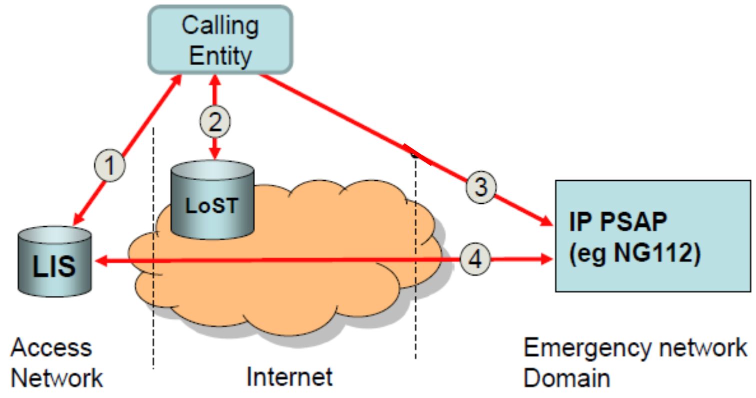


Figure 6.1: Simplified representation of GEOPRIV system [Source: ECRIT / GEOPRIV]

6.1.1 The ECRIT emergency calling model

The ECRIT emergency calling model covers geolocation, call routing and delivery. It is summarised in Figure 6.2 and described below.



1. Calling entity* obtains coarse location and location URI from LIS (directly or via device)
2. Calling entity queries LoST for PSAP URI corresponding to coarse location
3. Calling entity initiates SIP session to PSAP URI –passing coarse location and location URI
4. PSAP uses location URI to query LIS for accurate location information and location updates

(*) Calling entity may be an originating user device or an intervening call proxy, soft switch, etc.

Figure 6.2: The ECRIT emergency calling model [Source: CommScope]

The ECRIT model identifies three critical steps:

i. Determine the caller’s location by interrogating an LIS using the HELD protocol.

ii. Find the proper PSAP – the IETF has developed the LoST (Location-to-Service-Translation) protocol and server for this purpose.

iii. Location conveyance – put simply, a change to the SIP invite message such that it contains a PIDF-LO or Uniform Resource Identifier (URI).

The HELD protocol

HTTP Enabled Location Delivery (HELD) is a Layer 7 Link Control Protocol (LCP) that is used for retrieving location information from a server within an access network. The IETF specification defines an extensible XML-based protocol that enables the retrieval of location information from an LIS by a device. This protocol can be bound to any session-layer protocol, particularly those capable of MIME transport. The IETF draft describes the use of HTTP and HTTP/TLS[17] as transports for the protocol.

Location may be retrieved from the LIS by value, i.e. the end-device may acquire a literal location object describing its location. The device may also request that the LIS provide a location reference in the form of a location URI or set of location URIs, allowing the device to distribute its location information by reference. Both of these methods can be provided concurrently from the same LIS to accommodate application requirements for different types of location information.

In ND1638 it is noted that the HELD specification is targeted for end-devices to obtain location from an associated LIS. In the interim period, until devices are capable of making this request, it is proposed the VPC fetches the location information on behalf of the device from the providing network's LIS, i.e. the VPC is a 'location recipient' making a third-party request from a HELD perspective (see Interface (c) (VPC to ISP LIS) in the ND1638 architecture).

The LoST protocol

The IETF has developed a new Location-to-Service Translation (LoST) protocol that allows end systems and VoIP proxies to map location data into Uniform Resource Locators (URLs) representing either PSAPs or other SIP proxies that perform a more fine-grained mapping.

The IETF has generally assumed that emergency calls use SIP for setting up and terminating calls, as this is probably the most widely-used standards-based VoIP protocol. However, LoST is largely independent of the signalling protocol and would, for example, also work for XMPP, Skype, Jingle and other proprietary VoIP protocols. LoST itself is carried in HTTP messages.

In summary, users placing an emergency call dial either the local or home emergency service number, such as 911 in North America. The user agent recognises the call as an emergency call, inserts a special service Uniform Resource Name (URN), such as urn:service:sos, into the call setup request, and consults an internal table for the PSAP URL it should route the request to. The PSAP URL has been determined earlier by invoking LoST with the current location of the caller.

It is important to note that the United States has 6140 primary and secondary PSAPs and 3135 counties which include parishes, independent cities, boroughs and census areas.[18] In comparison, UK-wide coverage for emergency calls is provided by Stage 1 PSAPs operated by BT (5 PSAPs) and Cable and Wireless (2 PSAPs). In the United States, where PSAPs serve limited areas and

[17] Transport Layer Security.

[18] http://www.nena.org/911-statistics

emergency callers must be directed to the most appropriate PSAP, the design rationale for the LoST protocol is therefore understandable. However, given the much less distributed nature of the emergency call handling architecture in the UK, the use of LoST is less relevant at this stage.

SIP location conveyance

Session Initiation Protocol (SIP) is the IETF’s protocol for establishing real-time application sessions, and is very commonly used for VoIP. It has gained massive popularity in recent years, and is used not just in VoIP software, but also in PBXs from various vendors, open source products such as Asterisk, and a wide range of carrier products. SIP is the base for telephony in next-generation technologies such as Long Term Evolution (LTE), and is a major component of IP multimedia subsystems (IMS). A high percentage of calls being routed today already use SIP.

For these reasons, the IETF has considered a number of ways to embed location information into SIP messages. The current version of the SIP location conveyance specification uses “Content ID” URIs to refer from the new “Geolocation:” header to a MIME body part, which then contains the location embedded in a Presence Information Data Format Location Object (PIDF-LO) Presence/Location document.

PIDF-LO

In ND1638, once the appropriate ISP LIS has been determined through Interface (b), a HELD location request is used to pass the IP address received in Interface (a) to the identified ISP LIS. The ISP LIS responds with a location as a PIDF-LO.

PIDF-LO allows for great flexibility of location types, and can contain civic addresses and extensive privacy rules. However, since the publication of the original PIDF-LO civic specification (IETF RFC4119), it has been found that the specification is lacking a number of additional parameters that can be used to more precisely specify a civic location. IETF RFC 5139 revises the GEOPRIV civic form to include additional civic parameters and introduces a hierarchical structure for thoroughfare (road) identification, which is employed in some countries. New elements are defined to allow for even more precision in specifying a civic location.

Annex C of ND1638 provides guidelines for the creation of civic addresses to meet UK requirements, and the profile used is based on RFC 5139.

6.2 NENA – NG911 and ICE

Next Generation 911 (NG911) refers to an initiative aimed at updating the 911 service infrastructure in the United States and Canada to improve public emergency communications services. In addition to calling 911 from a telephone, it intends to enable the public to transmit text, images, video and data to the 911 PSAP. The initiative also envisions additional types of emergency communications and data transfer, such as VoIP. The National Emergency Number Association (NENA) first identified the need for NG911 in 2000, and started development actions in 2003, and is nearing full definition and standards for NG911. Since 2006, the US Department of Transportation (DOT) has been leading their NG911 Initiative, a research and development project aimed at advancing NG911.

6.2.1 NG911 – the i2 and i3 specifications

NENA has developed its 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. The differences between the i2 specification and the newer i3 specification are largely based on the assumptions being made about the capabilities of the infrastructure available to the PSAP operator. For i2, the PSAP operator receives emergency calls via the PSTN, while for i3 the PSAP operator uses an IP-based emergency services network.

NENA i2 specification

The i2 specification[19] describes the short-term architecture for the 911 system. It deals with the migration of emergency services in cases where the access network is an IP network and the emergency service provider's network (the PSAP's network) is still circuit-switched. Once the caller's location is known, the call is routed towards the appropriate PSAP through an Emergency Services Gateway (ESGW) that translates signalling between both networks. Figure 6.3 illustrates the functional elements and signalling interfaces used to support the i2 solution.

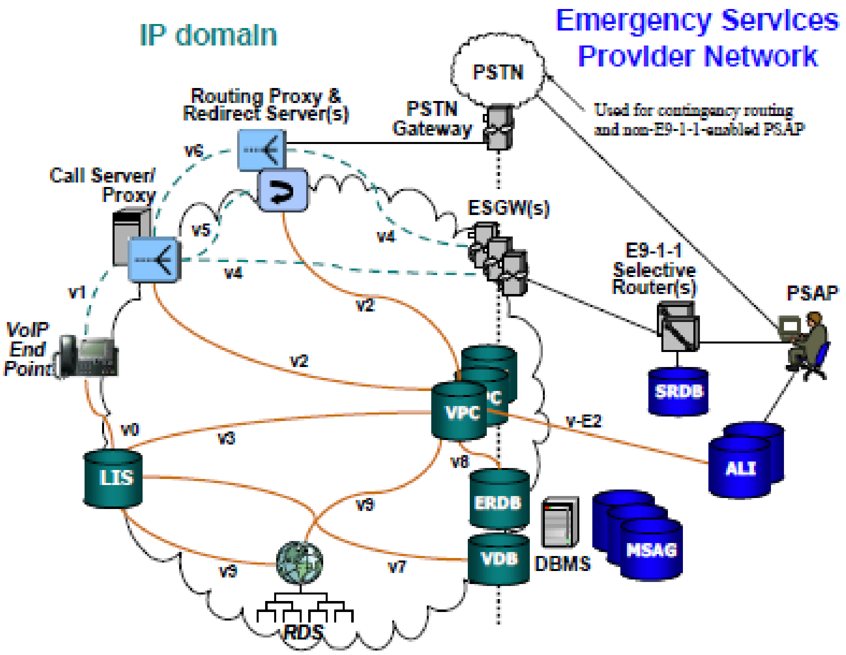

IP domain
Emergency Services Provider Network
PSTN
Routing Proxy & Redirect Server(s)
PSTN Gateway
Used for contingency routing and non-E9-1-1-enabled PSAP
v6
Call Server/ Proxy
v5
v4
ESGW(s)
v4
E9-1-1 Selective Router(s)
v1
v2
PSAP
VoIP End Point
v2
SRDB
VPC
v-E2
v0
v3
ALI
LIS
v8
v9
ERDB
VDB
DBMS
MSAG
v3
v7
RDS

Figure 6.3: NENA i2 – functional elements and signalling interfaces [Source: NENA]

[19] NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2), August 2010 (http://www.nena.org/sites/default/files/20100811_08-001%20v2.pdf)

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 (shown on the right-hand side of the diagram).

A number of protocol interfaces are outside the scope of the 911 system (v0/v1) and several are between elements that are considered to be within the 911 system (v2, v3, v4, v5, v6, v7, v8, v9 and v-E2). The former are specified by other standards organisations, such as the IETF. The latter are defined in the i2 specification.

The ESGW is the signalling and media inter-working point between the IP domain and conventional trunks to the 112/999 Selective Router. The Selective Router delivers calls arriving on trunks from the ESGW to the correct serving PSAP based on the routing information in the call setup signalling.

The LIS is the functional entity that provides locations of endpoints. An LIS can provide location-by-reference, or location-by-value, and, if the latter, in geo or civic forms. An LIS can be queried by an endpoint for its own location, or by another entity for the location of an endpoint. In either case, the LIS receives a unique identifier that represents the endpoint, for example an IP address, and returns the location (by value or reference) associated with that identifier. The administrator/owner of the LIS, for example the ISP, is responsible for creating and maintaining this mapping.

The VoIP Positioning Centre (VPC) is the element that provides routing information to support the routing of VoIP emergency calls. It also cooperates in delivering location information to the PSAP using the existing Automatic Location Identification (ALI) database infrastructure.

For further description of the functional elements shown in Figure 6.3, please refer to the i2 specification document.

NENA i2 deployment and FCC 05-116

Whilst the i2 specification was developed several years ago, it has not been generally deployed in full across the United States. According to a senior NENA representative it has been deployed only in “patches” – there has been no complete implementation of the full specification to date, and LISs are not currently in use.

Figure 6.4 below illustrates how 911 VoIP calls are generally handled in the United States today, alongside an illustration of how calls from traditional, fixed locations are handled.

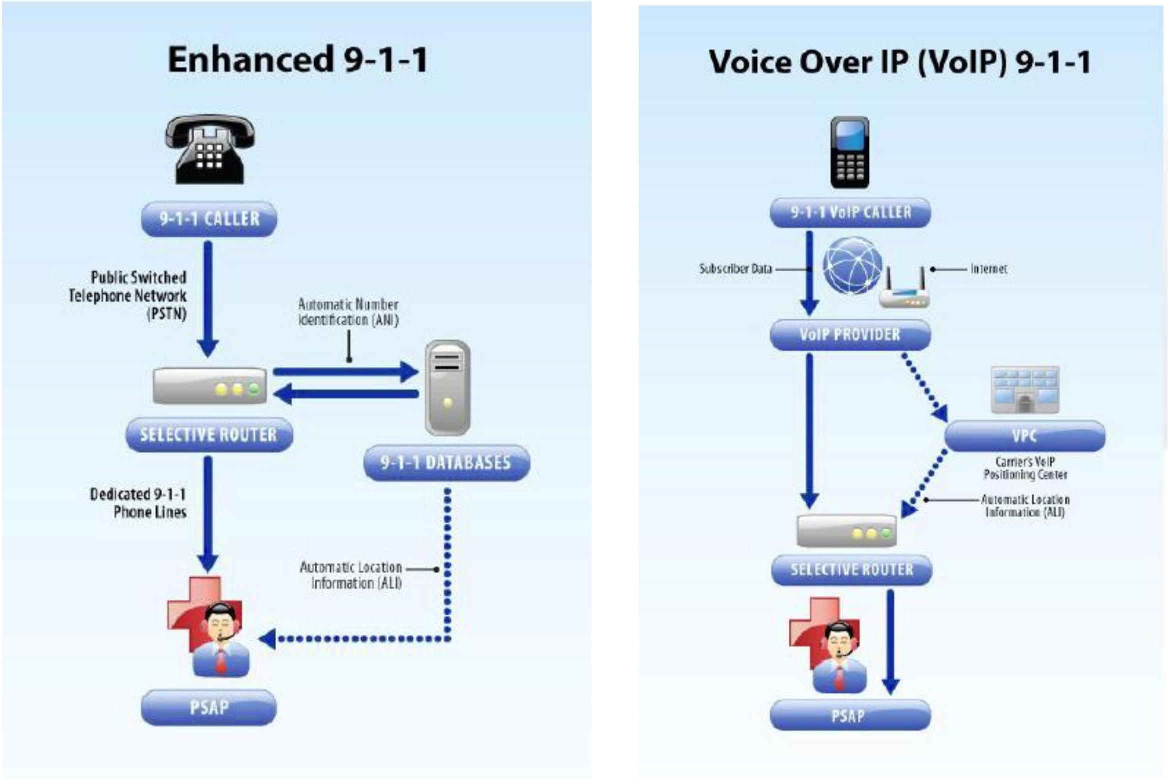

Enhanced 9-1-1
9-1-1 CALLER
Public Switched Telephone Network (PSTN)
Automatic Number Identification (ANI)
SELECTIVE ROUTER
9-1-1 DATABASES
Dedicated 9-1-1 Phone Lines
Automatic Location Information (ALI)
PSAP
Voice Over IP (VoIP) 9-1-1
9-1-1 VoIP CALLER
Subscriber Data
Internet
VoIP PROVIDER
VPC
Carrier's VoIP Positioning Center
Automatic Location Information (ALI)
SELECTIVE ROUTER
PSAP

Figure 6.4: E911 emergency call handling (US) [Source: 911.gov]

The supply of E911 capabilities to VoIP customers has so far largely been driven by FCC Ruling FCC 05-116, under which interconnected VoIP service providers are required to collect certain information and take other actions to comply with FCC rules requiring interconnected VoIP service providers to supply E911 capabilities to their customers. The Order requires collection of information in four instances:

1. Interconnected VoIP providers must obtain from each customer, prior to the initiation of service, the physical location at which the service will first be utilised, and must provide customers a way to update this information (i.e., the “Registered Location”).

2. Interconnected VoIP providers must place the Registered Location information for their customers into, or make that information available through, ALI databases maintained by local exchange carriers (and, in at least one case, a state government) across the country.

3. The Order requires all providers of interconnected VoIP service specifically to advise new and existing subscribers of the circumstances under which E911 service may not be available through the interconnected VoIP service or may be in some way limited by comparison to traditional E911 service, and to obtain and keep a record of affirmative acknowledgement by every subscriber of having received and understood this advisory.

4. The Order requires all interconnected VoIP providers to submit a letter to the Commission detailing their compliance with the rules set forth in the Order.

Under the FCC Ruling, Part 9.5 of Title 47 of the Code of Federal Regulations (CFR) was added to read as follows:

> 9.5 E911 Service.
>
> (a) Scope of Section. The following requirements are only applicable to providers of interconnected VoIP services. Further, the following requirements apply only to 911 calls placed by users whose Registered Location is in a geographic area served by a Wireline E911 Network (which, as defined in §9.3, includes a selective router).
>
> (b) E911 Service. As of November 28, 2005:
>
> (1) Interconnected VoIP service providers must, as a condition of providing service to a consumer, provide that consumer with E911 service as described in this section;
>
> (2) Interconnected VoIP service providers must transmit all 911 calls, as well as ANI[20] and the caller's Registered Location for each call, to the PSAP, designated statewide default answering point, or appropriate local emergency authority that serves the caller's Registered Location and that has been designated for telecommunications carriers pursuant to §64.3001 of this chapter, provided that "all 911 calls" is defined as "any voice communication initiated by an interconnected VoIP user dialling 911;"
>
> (3) All 911 calls must be routed through the use of ANI and, if necessary, pseudo-ANI, via the dedicated Wireline E911 Network; and
>
> (4) The Registered Location must be available to the appropriate PSAP, designated statewide default answering point, or appropriate local emergency authority from or through the appropriate automatic location information (ALI) database.
>
> (c) Service Level Obligation. Notwithstanding the provisions in paragraph (b) of this section, if a PSAP, designated statewide default answering point, or appropriate local emergency authority is not capable of receiving and processing either ANI or location information, an interconnected VoIP service provider need not provide such ANI or location information; however, nothing in this paragraph affects the obligation under paragraph (b) of this section of an interconnected VoIP service provider to transmit via the Wireline E911 Network all 911 calls to the PSAP, designated statewide default answering point, or appropriate local emergency authority that serves the caller's Registered Location and that has been designated for telecommunications carriers pursuant to §64.3001 of this chapter.
>
> (d) Registered Location Requirement. As of November 28, 2005, interconnected VoIP service providers must:

[20] Automatic Number Identification.

(1) Obtain from each customer, prior to the initiation of service, the physical location at which the service will first be utilized; and

(2) Provide their end users one or more methods of updating their Registered Location, including at least one option that requires use only of the CPE necessary to access the interconnected VoIP service. Any method utilized must allow an end user to update the Registered Location at will and in a timely manner.

(e) Customer Notification. Each interconnected VoIP service provider shall:

(1) Specifically advise every subscriber, both new and existing, prominently and in plain language, of the circumstances under which E911 service may not be available through the interconnected VoIP service or may be in some way limited by comparison to traditional E911 service. Such circumstances include, but are not limited to, relocation of the end user's IP-compatible CPE, use by the end user of a non-native telephone number, broadband connection failure, loss of electrical power, and delays that may occur in making a Registered Location available in or through the ALI database;

(2) Obtain and keep a record of affirmative acknowledgement by every subscriber, both new and existing, of having received and understood the advisory described in paragraph (e)(1) of this section; and

(3) Distribute to its existing subscribers warning stickers or other appropriate labels warning subscribers if E911 service may be limited or not available and instructing the subscriber to place them on or near the equipment used in conjunction with the interconnected VoIP service. Each interconnected VoIP provider shall distribute such warning stickers or other appropriate labels to each new subscriber prior to the initiation of that subscriber's service.

(f) Compliance Letter. All interconnected VoIP providers must submit a letter to the Commission detailing their compliance with this section no later than November 28, 2005.

The FCC Ruling was an important step towards addressing the complex issues affecting the deployment of VoIP E911 services, and emphasised the importance of all entities involved in the delivery of VoIP E911 operating from common principles and understanding. However, both the FCC and NENA see this is an evolving issue that will continue to require diligence and cooperation to ensure the quality of VoIP E911 service matches that of the traditional wireline E911. The FCC Notice of Inquiry FCC 10-200, released in December 2010 and considered later in this document, seeks comments on how to further the transition to IP-based communications capabilities for emergency communications and NG911.

NENA i3 specification

In its i3 specification[21], NENA has applied standards from IETF and 3GPP (3rd Generation Partnership Project) and other SDOs to specific NG9-1-1 requirements. The i3 specification describes a complete redesign of the entire 911 system towards NG911. It deals with the long-term architecture, where both the access network and the emergency service provider network are based on IP.

NENA i3 introduces the concept of an emergency services IP network (ESInet), which is designed as an IP-based inter-network (network of networks) shared by all agencies which may be involved in any emergency. The i3 PSAP is capable of receiving IP-based signalling and media for delivery of emergency calls conforming to the i3 standard.

The i3 standard specifies that all calls enter the ESInet using SIP signalling. The PSAP is selected using the ECRF server[22], and calls are delivered to the PSAP with location and call-back information. It further specifies that a Location Verification Function (LVF) must be applied by the origination network to validate location prior to the origination of 911 calls.

The i3 document references several types of originating networks that could be used to deliver calls to an ESInet, including legacy circuit-switched networks (wireline or wireless). Those must undergo mediation via a gateway to convert the incoming signalling to SIP. In addition, functionality must be applied to legacy emergency calls to acquire location and use the information obtained in call setup signalling to route a call to the PSAP. A generic SIP and an IMS-based ESInet are described in this version.

The i3 location architecture is based on the following IETF standards:

- GEOPRIV requirements [RFC 3693]
- A Presence-based GEOPRIV Location Object Format [RFC 4119 and updates]
- Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information [RFC 3825 and updates]
- Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information [RFC 4776 and updates]
- HTTP Enabled Location Delivery (HELD)
- SIP Location Conveyance
- Location-to-Service Translation Protocol (LoST) (RFC 5222) allows routing to the suitable PSAP providing the PSAP URI from the location and the emergency service name.

The general approach supported in i3 is to determine location at the point of origin (the phone) in the access network. This is a radical difference with the present-day approach, where location is generally obtained via a phone number–postal address database or, in the case of cellular

[21] http://www.nena.org/sites/default/files/08-002%20V1%2020071218.pdf

[22] In NENA terminology, the ECRF (Emergency Call Routing Function) server refers to the IETF LoST server.

networks, a dedicated network node (the Gateway Mobile Location Centre or GMLC). In i3, it is assumed the location is known by the access network through the use of an LIS.

Figure 6.5 shows a simplified illustration of the i3 architecture and its key functional elements.

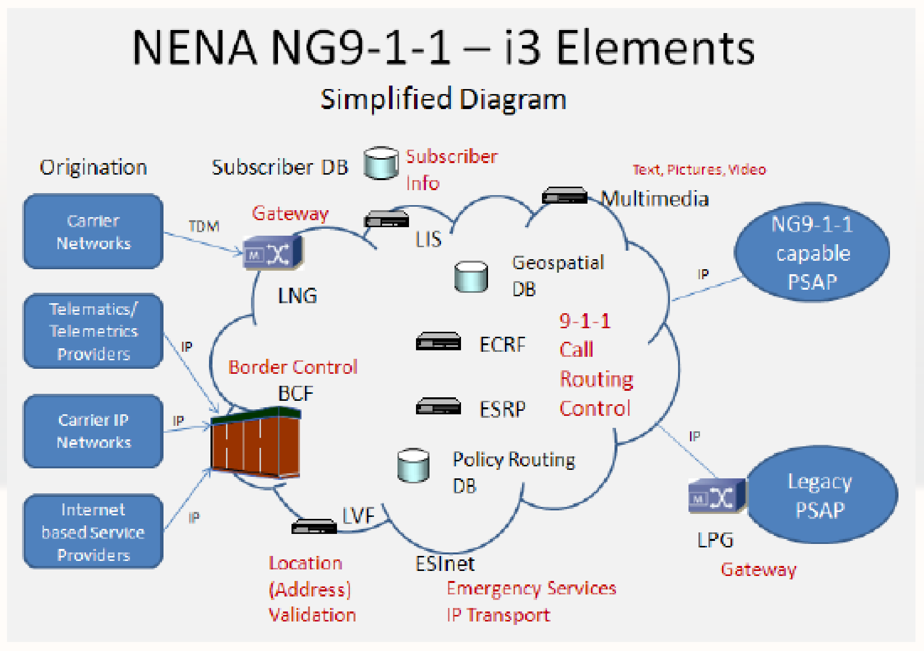


Diagram from the FCC CSRIC Working Group 4B Report (Transition to NG911)
Available at: www.fcc.gov/pshs/docs/csric/CSRIC-WG4B-Final-Report.pdf

Figure 6.5: i3 simplified diagram [Source: FCC]

The key features of i3 may be summarised as:

- Multimedia communication with the PSAP (voice, video and text).
- Calls arrive over IP, routed by LoST, carrying the caller’s location and call-back number. In the case of calls from legacy equipment, the gateways will be outside the i3 network and will use Emergency Services Routing Proxies (ESRPs) at the edge of ESInet and the ECRF server to route the call to the PSAP.
- The Policy Routing Function can be used to route calls to appropriate call takers (e.g. use language preference information to route calls and automatically engage interpreters).
- i3 further specifies that a Location Verification Function (LVF) must be applied by the origination network to validate location prior to the origination of 911 calls.

NENA i3 status

The NENA i3 specification is pending approval by the NENA Board, and a vote to approve is expected soon. Whilst the specification represents a significant step towards meeting the next-generation vision, some in the industry have misgivings. For example, Intrado, a 911 technology solutions provider, has raised concerns about i3. Whilst Intrado generally supports i3, the company has indicated there are problems within the current draft document that need to be remedied before it is adopted by NENA. Intrado is a major proponent of the ATIS RFAI standard that includes using ANI/ALI for location resolution, a service currently provided by Intrado. i3, on the other hand, uses the IETF PIDF-LO standard for location identification.

However, in support of the i3 document, several other vendors in the 911 sector are eagerly anticipating the adoption in order to kick-start the technology deployment in the market. Recently a group of seven other vendors including TCS and Cassidian joined Avaya in issuing a press release urging immediate approval of the i3 document.[23]

Also of relevance to this report is the FCC Notice of Inquiry FCC 10-200, released in December 2010, which, as recommended in the US National Broadband Plan, initiates a comprehensive proceeding to address how NG911 can enable the public to obtain emergency assistance by means of advanced communications technologies beyond traditional voice-centric devices. In the NOI, the FCC acknowledge the NENA Handbook, released in March 2010, which states that "it is critical that state regulatory bodies and the FCC take timely and carefully scrutinised action to analyse and update existing 911, PSTN, and IP rules and regulations to ensure they optimize 911 governing authority choices for E911 and NG911 and foster competition by establishing a competitively neutral marketplace."

A steady stream of filings has been made, and amongst those received to date (under FCC Proceeding Number 10-255) Intrado has repeated its concerns about the current version of i3, explaining some of the many reasons why in its view i3 in its present iteration does not satisfy appropriate principles related to NG911, and that i3 is not ready for investment by the public at this time.

AT&T has also expressed some concern. For example, it claims that "the FCC should not require providers of portable Interconnected VoIP Service to automatically provide Location Information to PSAPs – there are currently no feasible solutions that allow a provider of portable VoIP service to determine the location of a caller absent the user affirmatively providing their location (address). The services included in the definition of Interconnected VoIP service include a myriad of portable devices that preclude any single standard or solution for determining location".

There is no denying that NG911 and i3 is a radical departure from current mechanisms – it is therefore entirely understandable why the FCC is seeking to gain a better understanding of how the gap between the capabilities of next generation networks and devices and today's 911 system can be bridged. The due diligence around the legitimacy of the i3 guidelines that NENA is doing before approval is also justified given the step changes involved.

[23] http://www.geo-comm.com/press_NENAi3Support.html

6.2.2 NENA Industry Collaboration Events

NENA views a range of testing programmes as a critical component to accomplishing standards-based NG911. NENA understands that it is the vendors of NG911 elements that will ultimately deliver the interoperability that NG911 promises. Therefore NENA organises Industry Collaboration Events (ICEs) to bring together vendors in an open, supportive, and collaborative environment that fosters a spirit of technical cooperation. However, taking part in or success in testing at an ICE does not confer any formal NENA certification for a vendor’s products.

While NENA has played a central role in the creation of the ICE programme, its wish is to include all stakeholder groups and it is open to partnering with other industry organisations in the creation and implementation of the programme. This is evidenced by the makeup of the NG911 ICE Steering Committee, which has seats for vendors, government users and buyers, other industry associations, government organisations, NENA Technical and Operations Committee leadership, and NENA senior staff. Three events have been held so far, all in the United States:

- ICE 1 (November 2009): i3 end-to-end testing
- ICE 2 (May 2010): NG911 transitional elements
- ICE 3 (November 2010): location information.

These events have been considered successful vis-à-vis NENA’s goals for ICE. There has been significant vendor participation and cooperation, and details-related issues as well as the need for clarity in relevant interface specifications have been identified as part of the testing process. According to a senior NENA representative, the focus of the ICE trials to date has been more on call routing functionality rather than the management of location-related data.

ICE 4 is tentatively planned for October 2011, with its focus likely to be on LoST hierarchy-based call routing.

6.3 EENA

The European Emergency Number Association (EENA) is a Brussels-based NGO set up in 1999 which serves as a discussion platform for emergency services, public authorities, decision makers, associations and solution providers, with the aim of improving emergency response in accordance with citizens' requirements. EENA membership includes 430 emergency services representatives from 39 European countries, 25 solution providers, 9 international associations/organisations as well as 26 Members of the European Parliament.

EENA recognises the European situation is somewhat different from that in the United States as the emergency infrastructure in the different member countries does not show such a harmonised structure. A technical group within EENA, the Next Generation 112 Technical Committee (NG112TC), has therefore been formed to synchronise various activities by considering the country-specific circumstances regarding their current emergency infrastructure. Technically, available standards are still applicable to these environments, but require different profiling.

The Technical Committee plans to survey organisations across Europe to understand their particular requirements for next-generation emergency services. EENA hope to complete this survey by July 2011, and this is expected to form the basis of a requirements document. EENA's current thinking is then to cluster countries based on their existing emergency services network architecture, and construct its first architecture document around those countries operating single Stage 1 PSAPs – for example the UK, Cyprus, Ireland, the Netherlands and Portugal. In this regard, EENA intend to leverage the experience gained by the NICC (ND1638) in the UK. According to EENA representatives, it is hoped the initial draft of the architecture document will be available by October 2011 but, with the large number of stakeholders involved, EENA acknowledge it may be delayed. The intention is then to develop the architecture to incorporate the requirements of countries operating multiple PSAPs, such as Bulgaria, Denmark and Sweden.

6.4 3GPP – IMS

The 3rd Generation Partnership Project (3GPP) was initially formed to make a globally applicable specification for 3G based on evolved GSM specifications. It later was responsible for the development of the IP Multimedia Subsystem (IMS), which was originally designed to evolve UMTS networks to deliver IP-based multimedia to mobile users. IMS has become the core component within 3G, cable TV and next-generation fixed telecoms networks.

The IMS specification began in 3GPP Release 5 as part of the core network evolution from circuit-switching to packet-switching, and was refined by subsequent Releases 6 and 7. 3GPP is continuing to develop the necessary elements to enhance IMS support of emergency services. The IMS emergency call architecture is shown in Figure 6.6.

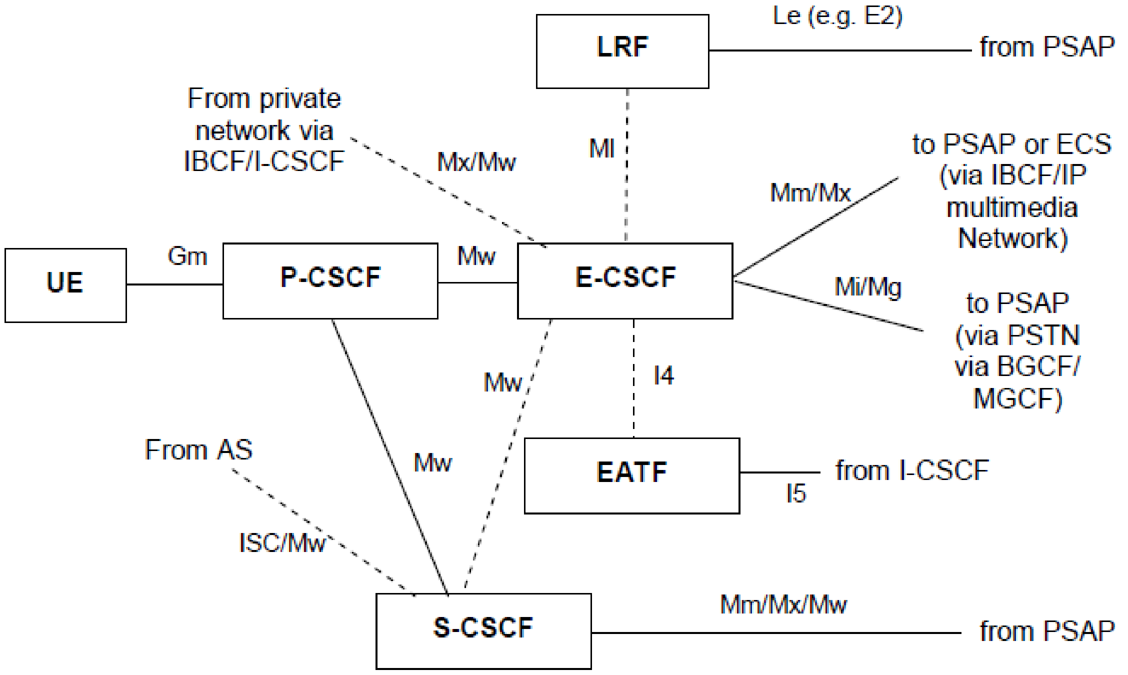


Figure 6.6: IMS emergency call architecture [Source: 3GPP (TS 23.167 11.0.1 2011-01-04)]

A full description of the functional elements and interfaces used in the 3GPP IMS emergency call architecture is beyond the scope of this study, but a brief description of the functional elements responsible for routing emergency requests, and retrieving location information, is presented below:

- The Emergency Call Section Control Function (E-CSCF) is the entity in charge of routing the emergency requests to the appropriate PSAPs, even if these requests are anonymous. Upon receiving an emergency request from a Proxy-Call Session Control Function (P-CSCF), the first contact point for the users of the IMS, if the location information is not included in this request or additional location information is required, then the E-CSCF may make a request to the Location Retrieval Function (LRF) to retrieve location information. It might also be possible that the E-CSCF requests the LRF to validate the location information if this is included by the user's terminal. If the E-CSCF is not able, itself, to determine the proper routing information or the PSAP destination, it may query the LRF for this purpose.

- The LRF is in charge of retrieving the location information of the user's terminal that has initiated an IMS emergency session. The information provided by the LRF to the E-CSCF includes the routing information and other parameters necessary for emergency services and which are subject to local regulation, for instance, PSAP SIP URI.

A summary of the 3GPP IMS emergency call status is provided below:

- Release 9: Supports IP-based emergency calls for voice, and can support Real Time Text (RTT).
- Release 10: Enhancements added to support emergency calls using private numbering in an enterprise network.
- Release 11 and later:
  - — non-voice emergency services (NOVES)[24]
  - — improved support for location by reference is expected
  - — network-provided cell ID for more reliable PSAP routing is expected.

6.5 OMA

The OMA Location Working Group was created in 2002 by the Open Mobile Alliance (OMA) to develop specifications to ensure interoperability of mobile location services on an end-to-end basis, as well as to provide technical expertise and consultancy on mobile location services for other groups belonging to OMA.

The working group covers the primary aspects of mobile location services, including an end-to-end architectural framework with relevant application and contents interfaces, privacy and

[24] NOVES could support the following examples of non-voice communications to an emergency services network: Text messages from citizen to emergency services; session-based and sessionless instant messaging type sessions with emergency services; transfer of multimedia (e.g., pictures, video clips) to emergency services either during or after other communications with emergency services; real-time video session with emergency services.

security, charging and billing, and roaming. The group works with industry organisations and other OMA groups to ensure interoperability of specifications and to address new opportunities for collaboration.

The working group's efforts, in relation to emergency caller location information, are focused on the following technologies and protocols:

- Secure User Plane Location (SUPL)
- LTE Positioning Protocol (LPP) extensions (LPPe)
- Location in SIP/IP core (LOCSIP).

6.6 ESW

The Emergency Services Workshop (ESW) series is an ongoing effort in the emergency services community to coordinate global standards and technologies for emergency calling and emergency notification. The primary focus of the workshop series is to foster coordination among the many SDOs involved in emergency services as they all work toward a global solution for emergency communications using Internet technologies. In addition, the workshops try to bring in operational and regulatory perspectives on emergency services, so that these experiences and requirements can be incorporated into ongoing technical development processes. Participation is open all stakeholders in the emergency communications system, including industry (e.g. equipment vendors and telecommunications service providers) as well as government (e.g. regulatory bodies or emergency response organisations).

The first workshop was held in New York in 2005, and the second in Washington early in 2007. Since then a further six workshops have been held alternately in locations in the United States and Europe; the most recent (ESW8) was held in April 2011 in Budapest and hosted by EENA. Just like earlier ESWs, ESW8 was an international forum for discussing issues related to IP-based emergency calling, with a focus on coordination between different specific efforts, especially standards efforts.

6.7 Summary

In the United States, the FCC and NENA are strongly influencing how IP-based emergency services are to be provided, and the obligations that the various parties have. However, even there regulation is still at a relatively early stage: current requirements demand only manual update of location information by the VoIP user. The ability to obtain location information automatically is, however, crucial for reliable emergency service operation, and it is essential for nomadic and mobile devices.

The number of new IP-enabled communication mechanisms is also steadily increasing. Many emergency service organisations have recognised this trend and advocated the use of new communication mechanisms including video, real-time text and instant messaging, to offer improved emergency calling support for citizens. The NENA i3 architecture deals with this longerterm outlook, and there is a growing momentum behind its approval and implementation. However, the transition will not be straightforward and the timing of implementation will largely be driven by the FCC.

In Europe, it appears likely that different countries will deploy IP-based emergency services over different time horizons. The work being guided by the EENA NG112 TC is likely to influence the direction countries will take, and the ND1638 architecture is expected to influence EENA’s first architecture document, built around those countries that are operating single Stage 1 PSAPs.

7 Conclusions

The ND1638 architecture has been developed to meet a specific requirement to provide real-time emergency service location capability for VoIP users contacting UK emergency services via the existing stage one PSAP TDM architecture from DSL access points. The architecture achieves this specific requirement and remains, where possible, compatible with international interface standards, namely those developed by NENA in the United States and the IETF. In a European context, ND1638 is the most detailed work that has been done to address a specific national requirement. ND1638 is, as a result, well placed to influence the EENA European-wide initiative that is due to progress towards specifying VoIP emergency location standards during 2011 (although a common pan-European approach is unlikely due to variances in emergency service architectures between countries).

However, ND1638 is just the first stage in the development of the emergency services location architecture to meet the developing needs of users. The use of different means of VoIP access (e.g. cable, Wi-Fi hotspots, private networks) as well as other next-generation services (e.g. text, images and video) are not currently covered. Work is continuing on addressing these issues in the NICC working group, and it needs to be ensured that its initial implementation is compatible with its on-going development. Our investigations suggest that this is likely to be the case, as for example the ND1638 architecture does not exclude an evolution from a network-centric to an end-device-centric physical location request model which may be more appropriate to all-IP networks in the future.

To date, there has been very little (if any) progress towards implementation of ND1638 in the UK, and there remain considerable challenges in achieving this. During the study we spoke with a number of UK-based VSPs, ISPs and EHAs, which raised several concerns about the current architecture, relating to:

- range of access types supported
- alignment with other standards
- need for additional implementation guidance
- costs of implementation (significant investment is likely to be required)
- challenge of managing the implementation across so many VSPs and ISPs
- ensuring the participation of the ISP and ANP community.

The engagement of ISP and ANP organisations is particularly important to the success of the project as their participation is required to implement the LIS, which is required to determine the physical geographic address of the VoIP 999 caller. As ISPs and ANPs are not currently involved in emergency calling, and as VoIP callers will in many cases not be their taking a voice service directly from them, this may prove difficult (as economic incentives are misaligned). It is of note that in the United States, where an LIS has been included in the NENA i2 architecture for some time, actual LIS implementation is very sparse: non-real-time registered location by the end-user is still the usual method for determining their location, as in the current UK situation (pre-ND1638). The large number of VSPs, ISPs and ANPs in the UK will also provide a challenge in terms of implementation programme management.

The lack of progress towards implementation has also made it difficult to establish definitive costs for implementation across different entities (EHA, VSP, ISP, and ASP). Cost estimates provided by the industry varied widely: estimates of capital costs ranged from £200 000 to £1 million plus, while for operating costs, estimates varied from £2000 to £200 000 per annum. The wide discrepancies in the cost estimates provided by the study participants reflect both a certain lack of focus on this area to date, as well as their different starting positions. However, it is apparent that significant investment will be required by a large number of parties.

While it appears that ND1638 provides a viable way forward for VoIP emergency location, the progress of EENA standardisation and the on-going FCC consultation on the NENA i3 "next generation 911" architecture should be closely monitored. Both are due to report during 2011. EENA should provide a clear indication of the position of the ND1638 architecture in the context of European compatibility, while the level of NENA architecture implementation that the FCC mandates in the United States may provide some guidance on what can reasonably be expected to be implemented in the UK.

Annex A Abbreviations used

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorisation and Accounting
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ANP	Access Network Provider
API	Application Protocol Interface
ASP	Application Service Provider
BT	British Telecommunications plc
C&W	Cable & Wireless
CLI	Calling Line Identity
CSV	Comma Separated Values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSL	Digital Subscriber Line
ECRF	Emergency Call Routing Function
ECRIT	Emergency Context Resolution with Internet Technologies
E-CSCF	Emergency Call Section Control Function
EENA	European Emergency Number Association
EHA	Emergency Handling Authority
ESGW	Emergency Service Gateway
ESInet	Emergency Services IP network
ESW	Emergency Services Workshop
FCC	Federal Communications Commission
FCC NOI	FCC Notice of Inquiry
GEOPRIV	Geographic location/Privacy
GPS	Global Positioning System
HELD	HTTP Enabled Location Delivery
HTTP	HyperText Transfer Protocol
IAIC	IP Address to ISP Converter
ICE	Industry Collaboration Event
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISP	Internet Service Provider
ITSPA	Internet Telephony Service Provider Association
IUP	Interconnect User Part (UK)
LIE	Location Information Element
LIS	Location Information Server
LLU	Local Loop Unbundling
LoST	Location to Service Translation
LRF	Location Retrieval Function
LTE	Long Term Evolution
LVF	Location Verification Function
NAT	Network Address Translation
NENA	National Emergency Number Association
NICC	Network Interoperability Consultative Committee
OMA	Open Mobile Alliance
OTT	Over The Top
PIDF-LO	Presence Information Data Format - Location Object
POTS	Plain Old Telephony Service
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RFC	Request for Comment

SBC	Session Border Controller
SDO	Standards Development Organisation
SIP	Session Initiation Protocol
SMS	Short Message Service
TDM	Time Division Multiplex
TLS	Transport Layer Security
UK-ISUP	UK - Integrated Services User Part
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Centre
VSP	VoIP Service Provider
VSP ID	VoIP Service Provider Identification