NICC ND 1638 Issue 1.1.2 (2010-3)

NICC Document

VOIP - Location for Emergency Calls (Architecture)

NICC Standards Limited

Michael Faraday House,
Six Dials Way,
Stevenage
SG1 2AY

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

NOTICE OF COPYRIGHT AND LIABILITY

© 2010 NICC Standards Limited

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be that printing on NICC printers of the PDF version kept on a specific network drive within the NICC.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other NICC documents is available at:

http://www.nicc.org.uk/nicc-public/publication.htm

If you find errors in the present document, please send your comments to:

mailto:help@niccstandards.org.uk

Copyright

All right, title where and interest in this document are owned by NICC Standards Limited ("NICC") and/or the contributors to the document (unless otherwise indicated that copyright is owned or shared with a third party). Such title and interest is protected by United Kingdom copyright laws and international treaty provisions.

The contents of the document are believed to be accurate at the time of publishing, but no representation or warranty is given as to their accuracy, completeness or correctness. You may freely download, copy, store or distribute this document provided it is not modified in any way and it includes this copyright and liability statement.

You may not modify the contents of this document. You may produce a derived copyright work based on this document provided that you clearly indicate that it was created by yourself and that it was derived from this document and provided further that you ensure that any risk of confusion with this document is avoided.

Liability

Whilst every care has been taken in the preparation and publication of this document, neither NICC, nor any working group, committee, member, director, officer, agent, consultant or adviser of or to, or any person acting on behalf of NICC, nor any member of any such working group or commitee, nor the companies, entities or organisations they represent, nor any other person contributing to the contents of this document (together the "Generators") accepts liability for any loss or damage whatsoever which may arise from the use of or reliance on the information contained in this document or from any errors or omissions, typographical or otherwise in the contents.

Nothing in this document constitutes advice. Nor does the transmission, downloading or sending of this document create any contractual relationship. In particular no licence is granted under any intellectual property right (including trade and service mark rights) save for the above licence to download copy, store and distribute this document and to produce derived copyright works.

The liability and responsibility for implementations based on this document rests with the implementer, and not with any of the Generators. If you implement any of the contents of this document, you agree to indemnify and hold harmless each Generator in any jurisdiction against any claims and legal proceedings alleging that the use of the contents by you or on your behalf infringes any legal or other right of any of the Generators or any third party.

None of the Generators accepts any liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance on the contents of this document for any purpose.

The NICC Standards Web site contains the definitive information on the IPR Policy and Anti-trust Compliance Policy

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary, NICC Standards Ltd.,

Michael Faraday House,
Six Dials Way,
Stevenage
SG1 2AY

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC.

Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

1 Scope

The present document specifies a practical technical solution for identifying the physical locations of VoIP callers to UK emergency services, and for providing sufficient location information to the 999/112 Call Handling Agencies.

This NICC Document (ND) has been produced by NICC Emergency Location Working Group.

This is designed to enable the quick automatic routing of VoIP emergency calls to the correct local Emergency Authority, and for the caller's location information to be automatically delivered to the local Emergency Authority.

The present document:

- considers the basic case of a UK-based VoIP subscriber who is calling a UK emergency service (still operating in a TDM network) from a physical location within the UK.
- does not cover regulatory or legal matters, but it does provide technical information that can inform the regulatory debate.
- re-uses existing technical standards as far as possible

The contents herein represent the consensus view and recommendations of technical experts from representative organisations that are active in providing VoIP services, including those that are delivering or considering whether to deliver 999/112 service. This includes representatives from various VoIP Service Providers, Internet Service Providers, Access Network Providers, 999/112 Call Handling Agencies and the UK national regulator (to represent Government interests in this critical national service).

It identifies the interfaces needed and refers to existing interface standards with profiling to provide a clear example of how such an architecture would work in widely used access technologies for organisations operating in the UK.

2 References

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies. Where web-links are provided to reference documents, they were correct at the time of publication, but cannot be warranted to remain so.

[1] NENA i2 schema
http://www.nena.org/technical-xml-schemas

[2] NENA 08-001 (Issue 1, December 6, 2005) "NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)" http://www.nena.org/standards/technical/voip/interim-voip-architecture-i2

[3] NENA XML specifications
http://www.nena.org/technical-xml-schemas

[4] IETF RFC XXXX "HTTP Enabled Location Delivery (HELD)" Ed,MBarnes,August 2009 http://tools.ietf.org/html/rfcXXXX

(Currently Geopriv Internet Draft in RFC Editor's queue : http://tools.ietf.org/html/draft-ietf-geopriv-http-location-delivery-16)

[5] IETF RFC 5139 "Civic Location Format for PIDF-LO" , M. Thomson, J. Winterbottom, February 2008
http://tools.ietf.org/html/rfc5139

[6] ETSI SR 001 262 "ETSI Drafting Rules"
http://www.etsi.org/WebSite/Standards/DraftingRules.aspx

[7] NICC Document ND1006 Interconnect User Part (IUP)
http://www.niccstandards.org.uk/publications/public-net.cfm

[8] NICC Document ND1007 ISDN User Part (UK-ISUP)
http://www.niccstandards.org.uk/publications/public-net.cfm

[12] ETSI ES 283 035 “TISPAN; NASS; e2 interface based on DIAMETER Protocol”

2.2 Informative references

The following references are at varying degrees of development as IETF drafts, HELD Identity Extensions being most advanced as an IETF Geopriv WG draft. They have been included for background information and to show that the XML schema included in this NICC document are the same as those …….

.

[9] IETF Geopriv Internet Draft "HELD Identity Extensions"
http://tools.ietf.org/html/draft-ietf-geopriv-held-identity-extensions-09

[10] IETF Geopriv Internet Draft "Using Device-provided Location-Related Measurements in HELD"
http://tools.ietf.org/html/draft-thomson-geopriv-held-measurements-05

[11] IETF Geopriv Internet Draft " Location Information Server (LIS) Discovery From Behind Residential Gateways"
http://tools.ietf.org/html/draft-thomson-geopriv-res-gw-lis-discovery-02

[13] DSL Forum TR-101 “Migration to Ethernet-Based DSL Aggregation

http://www.broadband-forum.org/technical/download/TR-101.pdf

3 Definitions and Abbreviations

3.1 Definitions

The key words “**shall**”, “**shall not**”, “**must**”, “**must not**”, “**should**”, “**should not**”, “**may**”, “**need not**”, “**can**” and “**cannot**” in this document are to be interpreted as defined in the ETSI Drafting Rules [6], Section 23:- Verbal Forms For The Expression Of Provisions (see Section 2 "References").

For the purposes of the present document, the term CLI (Calling Line Identification) refers to Network CLI.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Accounting
ADSL	Asymmetric Digital Subscriber Line
ANP	Access Network Provider
AS	Autonomous System
BGP	Border Gateway Protocol
BRAS	Broadband Remote Access Server
C7	CCITT Signalling System No. 7
CLI	Caller Line Identification
CRM	Customer Relationship Management
DHCP	Dynamic Host Configuration Protocol

DSL	Digital Subscriber Line
EA	Emergency Authority
EHA	Emergency Handling Authority (PSAP that selects, routes to, and provides location to a responding EA)
ESCT	Emergency Services Call Termination Message
ETSI	European Telecommunications Standards Institute
HELD	HTTP Enabled Location Delivery
HTTP	HyperText Transfer Protocol
IAIC	IP Address to ISP Converter
ID	Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPR	Intellectual Property Rights
ISO	International Organisation for Standardization
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
L2TP	Layer 2 Tunnelling Protocol
LIS	Location Information Server
LLU	Local Loop Unbundling
LNS	L2TP Network Server
MGCP	Media Gateway Control Protocol
NAS	Network Access Server
NAT	Network Address Translation
ND	NICC Document
NENA	National Emergency Number Association (North America)
OBO	On-Behalf-Of
OSS	Operational Support Systems
PBX	Private Branch eXchange
PIDF-LO	Presence Information Data Format – Location Object
PIG	PSTN Internet Gateway
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
RIPE	Réseaux IP Européens
RSA	An algorithm for public key cryptography
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
SG	Study Group
SBC	Session Border Controller
SID	Service IDentifier
SIP	Session Initiation Protocol
SP	Service Provider
SRC	SouRCe
SS7	Signalling System No. 7
TDM	Time Division Multiplex
TG	Task Group
URI	Uniform Resource Identifier
UTC	Universal Coordinated Time
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Centre
VSP	VoIP Service Provider
WG	Working Group
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
XML	eXtensible Markup Language

4 Introduction

There is no straightforward mechanism for automatically and reliably locating callers using VoIP access to 999 and 112. Increasing numbers of nomadic applications make this a particularly important issue for emergency callers who cannot give /confirm their location.

This document provides a practical method for providing sufficient location information to the 999 Call Handling Agencies in all circumstances so that :-

- an emergency call (999/112) can be quickly and automatically routed to the correct local Emergency Authority (Police, Fire, Ambulance or Coastguard)
- delivery of location information to the correct local Emergency Authority can also be reliably enabled

This issue of the document focuses on the (majority) case where all parties are in the UK and ADSL access is used.

It is intended that future issues of the ND 1638 Architectural document will consider other cases where different access technologies are used, where some of the parties involved are in different countries and where corporate private networks are used.

5 Overview of VOIP 999/112 Functional Architecture to provide location

VoIP services depend on a multi-layered network architecture. At the top layer are the actual VoIP services provided by a VoIP Service Provider (VSP) that uses a protocol such as SIP. Below this are the IP services, typically supplied by an Internet Service Provider (ISP). Below this are the physical access networks, such as ADSL and WiFi, typically supplied by a wholesale Access Network Provider (ANP).

The caller's location is only directly related to their current physical network access and therefore only reliably known by the ANP. Furthermore a VoIP customer may move from one physical access point to another (or even from one ISP to another) without the VoIP provider's knowledge.

Therefore the VSP, ISP and ANP must all cooperate to determine the caller's current location and supply it to the Emergency Handling Authorities.

The UK emergency services do not currently have their own VoIP connectivity, so all calls must be delivered to an EHA via the PSTN network (TDM based) which has little capacity for additional data to be carried in the call signalling. The only in-band information available to the EHA is the caller's CLI and an identifier for the VSP. The only in-band information available to the VSP is the caller's public IP address (as used in the VoIP signalling packets). The ISP will have some form of identifier available which links its IP services to the underlying access network, but this information is not available to the VSP. Consequently, the caller's public IP address (dynamically allocated) must be used to identify their current ISP, and that ISP must then in-turn link the IP address to a particular access network point, whose address can only be verified by the Access Network Provider.

In Figure 1 below the VSP sends an out-of-band message to the EHA’s VPC (VoIP Positionning Centre) containing the caller's IP address and CLI information, which can then be associated with the emergency call CLI received through the in-band signalling received via the PSTN. The EHA is then responsible for requesting the location information from the relevant ISP. In this way the trust relationships needed are limited to being between the VSPs and EHAs, and between the EHAs and ISPs.

In those (common) cases where a VSP (VSP 1 in Figure 1) does not have its own PSTN interconnect the emergency call must be passed to another upstream VSP that does. The out-of-band signalling from the VSP to the EHA may be sent directly from the originating VSP (as shown in Figure 1), or may be proxied via the interconnecting VSP.

An overview of the organisations involved and network parameters that need to be used and exchanged is shown below. This also shows a number of boundary controllers (SBCs) which have to be taken into account.

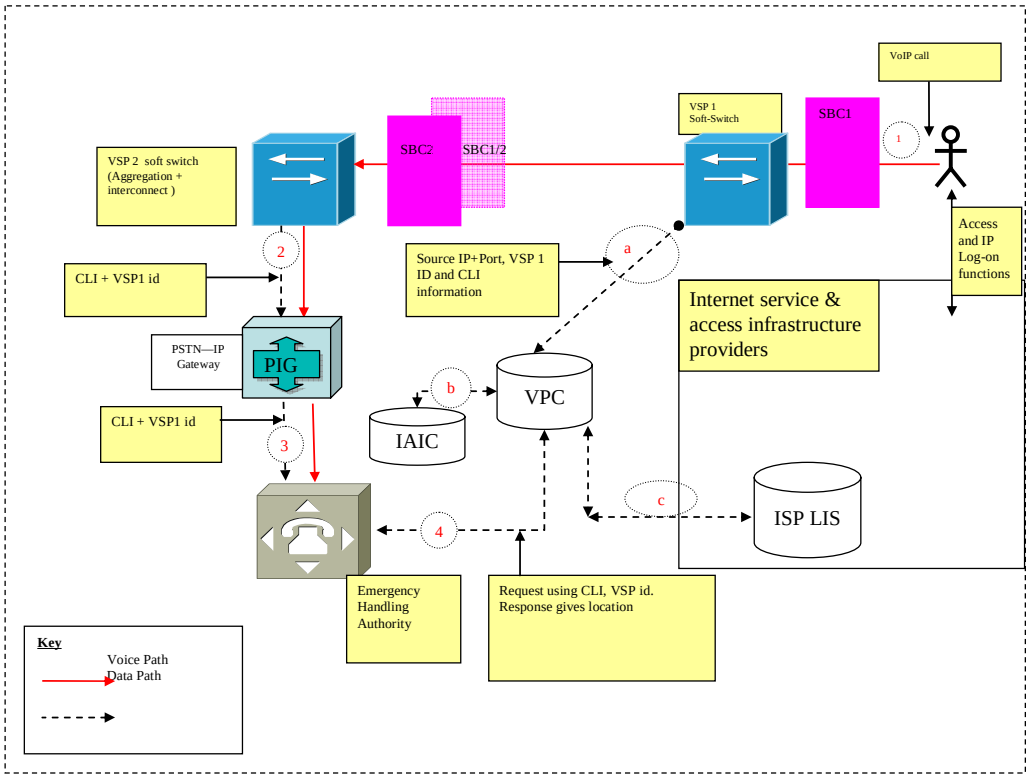


Figure 1 : Overview of the Architecture

Figure 1 is referred to in the following sections that describe in detail how the architecture allows location to be determined and provided to the emergency handling authority. Note that to simplify the diagram only the data paths needed in the location determination process described within this document are shown.

6 Functional Entity roles in the Architecture

6.1 VSP

6.1.1 General

It should be noted that to cover the majority of cases, the diagrams and explanations show two VSPs: VSP1 and VSP2.

These are logical definitions - it is possible that the functions of both VSP1 and VSP2 will be provided by a single service provider.

If only a single VSP is present then the entire call flow and connections from the originating customer (1) in Figure 1 through to the PIG (2) is under the control of that single VSP, which will need to fulfil the requirements described in sections for VSP1 and 2 below, and which will automatically control access to all the information needed.

It is also possible that there may be other intermediary VSPs between VSP1 and VSP2. If this is the case then each should pass on relevant data, to allow the function for VSPs 1 and 2 listed within the following sections.

For security requirements and recommendations for the VSP interfaces please see Annex G.

6.1.2 VSP1

The VoIP Service Provider 1 (VSP1) is the service provider that has a direct relationship with the calling party as its customer.

VSP1 has an (authenticated) signalling interface to its customers. This interface (not shown in Figure 1 for clarity) is most likely to be SIP. However a number of other protocols are possible (IAX2, Skinny, UniStim, H.323 and MGCP). This interface is used for call establishment (either from the customer, or from the VSP softswitch). Annex F shows informative telephony (and data) paths.

VSP1 operates a softswitching infrastructure and has no direct SS7 interconnect to the PSTN. VSP1 interconnects to VSP2 using a SIP interface or ISDN30 PRI interface or other VoIP signalling protocol interfaces such as IAX2 or H.323. It is also possible that VSP1 will have multiple similar telephony connections to other providers.

In order to provide access to the emergency services, VSP1 will need to be able to offer outbound PSTN calling and a CLI – an E 164 telephone number for use in the EHA and by a responding emergency authority. VSP1 may not own its own number ranges, and numbers may therefore need to be allocated from those owned by VSP2.

VSP1 shall detect when an emergency call is made, for example using dialled number digit matching. When this detection occurs VSP1 shall initiate the message exchange over interface (a) to the VPC, or a proxied interface via VSP2. The existence of a proxy has not been included in the Figure 1 in order to avoid confusion.

VSP1 shall ensure that it selects the same VPC as the one used by its upstream carrier (VSP2) with the SS7 interconnect on any particular call. If it's possible for VSP2 to vary the VPC used without reference to VSP1 then VSP2 must provide a proxy interface. The technical and commercial arrangements between VSP1 and VSP 2 need to cover this issue.

If VSP2 is providing a proxy interface then the interface (a) line that is shown will not be used – VSP1 will pass the data to VSP2 via this proxy and the interface (a) access will occur from VSP2 to the VPC.

VSP1 requires interfaces:

- To the caller (Interface 1). The longterm recommendation is that this interface is capable of conveying location information. However, as highlighted above, a variety of protocols are possible, and end user devices are not currently likely to be capable of determining and sending their location. For this reason this interface is out of scope for this issue of this document, is not shown in Figure 1and cannot be relied upon for delivery of location specific information.

- To the VPC based on the NENA i2 V2 specification (interface (a)) using http transport with XML documents. This interface can take two forms:

  - A direct interface to the VPC. This is interface (a) specified in the VSP2 section below. The main difference in the UK specification is that the interface is used to inform the VPC of the CallID, Source IP address (IP_{src}), Source Port number of the Signalling end-point ($Port_{src}$),VSP1id, Source of the Request (SRC), Date and Time of the request and the CLI of the caller initiating the emergency services call. The Source IP address and Port number is contained in the Location Information Element (LIE) location key, the format of which is defined in Annex A for UK profile of the NENA v2 Interface: Location Key Format for IP Addresses.

    VSP1 shall take measures to ensure the Source IP address is not obscured due, for example, to an SBC providing topology hiding on interface 1

  - An indirect interface to the VPC (not shown in figure 1) proxied via VSP2. This interface is provided as a convenience measure to ease adoption for smaller ITSPs and encourage participation in emergency services caller location. The indirect/proxy interface to the VPC via VSP2 will take the form of a simpler http/xml interface (agreed between VSP1 and VSP2 – see VSP2 section below) which also has to be able to pass the following key fields: CallID, Source IP address, Source Port number of the signalling end-point ($Port_{src}$), date+time, CLI and VSP1 id. The specification of this interface is out of scope for this specification and is a local design between VSP1 and VSP2 – see Annex A.5. VSP2 will then use interface (a) specified in the VSP2 section below to convey information to the VPC – see Annex A2.1.

6.1.3 VSP2

The VoIP Service Provider 2 is the service provider that has SS7 interconnect to the PSTN to reach the Emergency Handling Authority (EHA) and Emergency Authority (EA), potentially via a number of PSTN network operators.

VSP2 has the ability to route traffic to and from the PSTN, port telephone numbers and provide telephone numbers. VSP2 is probably the actual owner of the telephone number (CLI) that VSP1 has leased to provide to its customer(s) and in this case shall be the CLI presented to the EHA.

VSP2 has interfaces:

- To the caller via VSP1. The longterm recommendation is that this interface is capable of conveying location information. However, as highlighted below in the section on SBCs, this interface will be controlled and is likely be restricted. For this reason this interface is out of scope for this document, and cannot be relied upon for delivery of location specific information.

- To the VPC based on the NENA i2 V2 specification (interface a). This interface is a direct interface to the VPC (see Annex A for the UK profile for this interface). The main difference in the UK specification is that the interface is used to inform the VPC of the source IP address (IP_{src}), the source port number of the signalling end-point ($Port_{src}$) and the CLI of the caller initiating the emergency services call. This interface must pass: CallID, source IP address and port number, date and time, CLI, VSP1id and source (SRC). The Source IP address and port number is contained in the Location Information Element (LIE) location key, the format of which is defined in Annex A for UK profile of the NENA v2 interface: Location Key Format for IP Addresses.

- In some cases a proxied interface from VSP1. This interface is provided as a convenience measure to ease adoption for smaller ITSPs . Because of this, the interface can be simpler than the V2 specification. The indirect/proxy interface to VSP1 will take the form of a simpler http/xml interface and has to be able to pass the following key fields: CallID, source IP address, source port number of the signalling end-point,date and time, CLI and VSP1 id.

  The connection over the Http/XML interface from VSP1 should be initiated at the same time the call is received at VSP1 and operate in parallel with the call delivery from VSP1 to VSP2. This creates the possibility of a race condition occurring where the VSP to VPC update occurs either before or after the call has been delivered to the EHA. This cannot be avoided and the primary goal is the delivery of the emergency call, even if location information is late or not available. Further recommendations for when this interface is agreed between two VSPs is provided in informative Annex A5

- To the EHA via a PSTN-IP gateway. To interconnect to the PSTN for TDM emergency calls VSP2 must meet normal SS7 certification standards (either [7] or [8]) and provide interconnect identifier digits in the Called Party Number field (following the dialled digits 999) in addition to the VoIP caller's CLI. The EHAs have contracts for emergency call handling that cover allocation of the interconnect identifiers.

6.2 Session Border Controller (SBC)

A Session Border Controller (SBC) is an enhanced firewall specifically tailored for VoIP interconnect. Its role is to secure the perimeter of a provider's network from malicious attack and topology discovery. It usually provides signalling and media address translation and only allows media access for approved sessions. The SBC is also capable of providing session authentication & authorisation, Media Proxying and the ability for devices behind address translating firewalls to be connected without modification of the local address by the translating firewall (so-called far end NAT traversal),

The SBCs considered in this architecture may exist between the caller and their VoIP service provider (SBC1) on interface 1, and also may exist between VSP1 and VSP2 (SBC2). For each of SBC1, SBC2 shown there may be 'zero to n' SBCs present as they are entirely optional - see Figure 1. It is noted that the SBC2 may well be two separate SBCs, one owned and operated by VSP1, the other owned and operated by VSP2.

SBCs are used to provide what is referred to as Topology hiding. This process is commonly implemented in an IMS network and in other carrier networks to mask any internal infrastructure elements. The basic process in which topology hiding is implemented is through the encryption, in SIP signalling messages leaving the home network, of any URI that relates to functions within the home network. A number of SIP fields may be affected by this and these include:

- Via - used to route responses relating to a specific request.

- Route - indicating the path subsequent signalling messages should take.
- Record Route - a list of SIP agents that have proxied the specific message.
- Service Route - a list of SIP proxies that may add service to the signalling message.

Where topology hiding is implemented in an SBC, information needs to be made available to allow mapping of the voice session state to the caller's originally allocated source public IP address and port number for use later in the location process.

Another function of an SBC is the use of IP address translation which prevents downstream entities from discovering the IP address of the caller. In such a case VSPs responsible for SBCs must provide mechanisms to have access to the caller's source public IP address as this is what is required to be passed on interface (a). It's noted that end-users' routers/firewalls with their own SBC, or Application Level Gateway (ALG) function, will obscure any private (internal) IP address, and all signalling messages will be presented with the external public IP address of the router itself.

During transport of SIP signalling messages through the SBC(s) from VSP1 to VSP2, a number of fields may be used for indicating the CLI of the caller:

- From
- Contact
- P-Asserted-Identity
- Remote-Party-ID

Some or all of these fields may be present and used for communicating the CLI of the caller. The agreement between VSP1 and VSP2 should indicate which field(s) are to be used and which should not be modified by the SBC(s). It is understood that in some implementations not all fields (especially Remote-Party-ID and P-Asserted-Identity) will be present. In the case where P-Asserted-Identity is present, this shall not be modified by the SBCs as it is from a trusted entity.

6.3 VoIP Positioning Centre (VPC)

6.3.1 VPC Functional Entity Description

In the UK the VPC will be managed by the national Emergency Handling Agencies. Its core function is to provide location information suitable for:

- Routing the VoIP emergency call to the correct Emergency Authority.
- Giving the Emergency Authority sufficient CLI and location information to quickly respond to a call, especially where the caller is unable to clearly provide their location.

Once notified of an emergency call by the VSP it is the role of the VPC to recover the location data as quickly as possible in preparation for a location query from the EHA. To enable efficient call handling, location information should be returned within 2 seconds of a request being made across interface (c) for not less than 98% of requests made. Providing this performance is achieved, the emergency operator should have the automated information necessary to route the call to the appropriate emergency authority as soon as the question "Emergency, which service?" has been answered.

The VPC and its interfaces are shown in Figure 2 below. The parameters shown are not the comprehensive set.

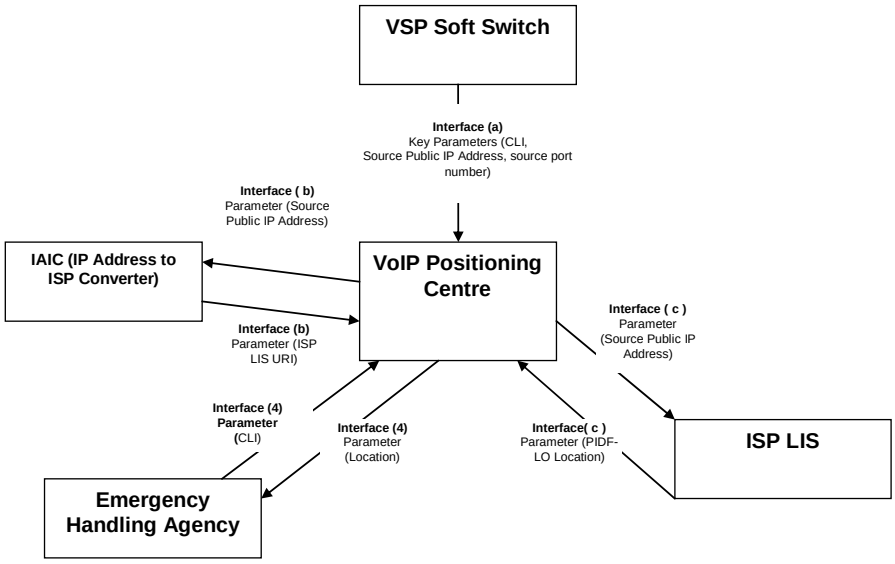


Figure 2 : VPC Interfaces

Figure 2 shows the VPC having four interfaces, these are

- Interface (a), which is described in sections 6.1 and 6.2
- Interface (b) to IAIC
- Interface (c) to the ISP LIS.
- Interface (4) to the EHA system

The VPC will be notified of an emergency call when the VSP pushes data to the VPC on interface (a). This data will contain the public source IP address, the source udp/tcp port number and the E.164 CLI of the device that initiated the emergency call.

The CLI will not play any further role in determining the location of the caller; it will only be used as matching criteria for the query from the EHA. The EHA will not have access to the source IP address as this will have been lost when the call set-up signaling crosses from the IP network to the TDM network.

Having received the data push from the VSP, the VPC will immediately initiate a location search; it will not wait for the query from the EHA. It is therefore important that the VSP only push data in the event of an emergency call rather than for every call, device registration or any other event.

6.3.2 IAIC Functional Entity Description

There will be a functional entity called the IAIC (IP Address to ISP Converter) that effectively sits within the VoIP Positioning Centre (VPC) – see Figure 3. The purpose of this entity is to establish which ISP LIS holds the location information based on the public source IP address of the caller's device.

Two alternate IAIC implementations are described. The EHA shall support both implementations in order to optimize accuracy and resilience.

6.3.2.1 IAIC implementation via Border Gateway Protocol

The IAIC will use the Border Gateway Protocol to establish the Autonomous System that contains the public source IP address of the device. The IAIC maintains a list of ISP Autonomous System (AS) numbers and their corresponding LIS URIs.

The IAIC incorporates a BGP4 Route Collector which receives routeing announcements from other parts of the internet. The last element of the "AS Path" associated with a particular IP address identifies the relevant Autonomous System.

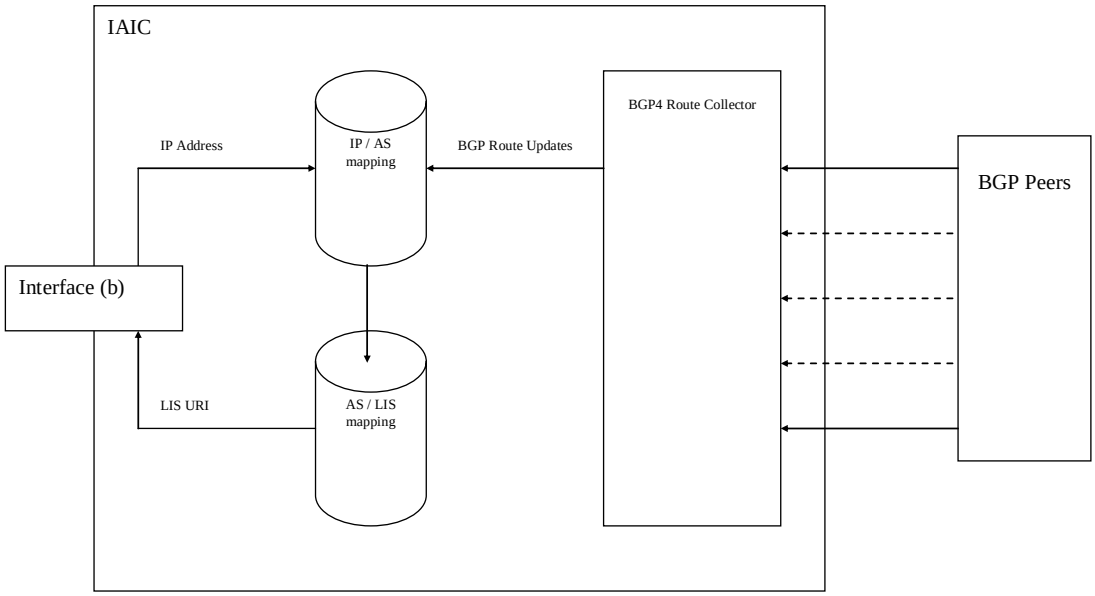


Figure 3 : BGP4 IAIC (IP Address to IP Converter)

Real-time updates sent by the BGP4 Route Collector are used to build a continuously updated table that associates IP ranges with AS numbers. The IAIC maintains a lookup table of AS number to LIS URIs - these details will be registered by the LIS provider. The method by which the LIS IP address is provided will be defined as part of the IAIC implementation, and may be a manual process. Should there be a large number of organisations with an ISP LIS in the future then a standard interface for an automated provision of the LIS URI against the ISP AS number can be considered. Construction of the IAIC lookup tables is carried out as independent configuration and does not form part of the real time call handling process.

To ensure full coverage of the global IP routeing table the Route Collector needs to receive data from multiple sources. This process is known as “peering”, although in this case the exchange of data would be unidirectional.

It is suggested that peering at the London Internet Exchange (“LINX”) would provide good access to routeing data from UK ISPs. It would also be appropriate to peer with one or more large IP transit suppliers to take a full routeing feed (essentially, set-up BGP peering and take however many prefixes it can provide). A ‘multi-hop’ configuration would allow this connection without a local presence on the provider’s network.

It is noted that the BGP4 Route Collector function can be implemented using open source software such as Quagga.

6.3.2.2 IAIC implementation via the Domain Name System

ISPs and Enterprises may store the LIS information directly in the global DNS and can therefore create and maintain their own mappings from IP address to LIS URI.

Specifically, the information may be stored within the “in-addr.arpa” and “ip6.arpa” domains that are normally used to map from IP addresses to hostnames.

In the IPv4 case, the octets forming the IP address are reversed in order and treated as (ASCII decimal) DNS labels in the “in-addr.arpa” domain. Hence the IP address 192.168.1.2 becomes 2.1.168.192.in-addr.arpa. A similar process is applied to IPv6 addresses.

The relevant portion of the IP address space when converted into this format is usually delegated to (and controlled by) the Internet Service Provider but may also be delegated further to enterprise customers who may wish to operate their own LIS.

An example DNS entry is shown below:

```
2.1.168.192.in-addr.arpa.  IN NAPTR 100 10 “u” “LIS:HELD” “!.*!https://lis.example.net/” .
```

These NAPTR records will happily coexist with the PTR records primarily found within “in-addr.arpa” and “ip6.arpa”. DNS queries specify which record type is required, so a query for NAPTR records will only return NAPTR records.

Note that the specification for NAPTR records permits the use of the final “replacement” field instead of a “regular expression”. Whilst the IAIC implementation will need to be able to follow chains of such “non-terminal NAPTR records” to find the LIS URI, it is recommended that “terminal NAPTR records” (as indicated by the “u” value in the example above) are used to ensure timely response.

This mechanism is described in more detail (including IPv6 examples) in [11], LIS Discovery from behind Residential Gateways.

6.3.2.3 IAIC Result Selection

In theory the BGP4 IAIC implementation will respond more quickly since it is just a dip into a local database, albeit one that is continuously updated. The DNS implementation, on the other hand, relies on real-time queries to the global DNS.

It is believed that the DNS implementation should provide more accurate information, but that the underlying mechanism is not quite as technically robust as the BGP implementation. Specifically, if an ISP’s DNS servers were to fail then no result would be returned.

Therefore the EHA will attempt to query via both implementations simultaneously, but will use the DNS-derived result in preference to the BGP-derived result, so long as the DNS result arrives quickly enough that any network delays do not impact on call handling. It is proposed that the cut-off point should be 200ms, after which the BGP-derived result should be used.

6.3.2.4 Caveats on the use of Public IP addresses

There is some concern that there could be cases where a call will not traverse a public IP network (so an Enterprise is acting as VSP1 and is allocating the IP address as well as providing VoIP service), and where VSP1 may try to provide to the VPC (and to VSP2) the private IP address it has allocated. However it is noted that, in a similar way to private networks in TDM PSTNs, VSP1 could be required to provide a *public* IP address to the VPC and also provide an “Enterprise LIS” function, if access is provided to the emergency service. At the very least, any VSP using private IP addresses associated with public emergency calls would be required to provide a LIS function so that if VPC cannot

derive a LIS from the IP address, it could send a HELD location request to a LIS identified from the TDM signalling parameters received on the voice call (which identify VSP 1). Future issues of this standard will consider whether other measures are needed such as additional fields in interface (a) to indicate that a private IP address is being passed, and to include an Enterprise LIS address URI.

6.3.3 External interfaces

For security requirements and recommendations for the external VPC interfaces (a) and (c) please see Annex G.

6.3.3.1 Interface (a) (VSP Soft switch to VPC)

This interface is fully documented in Sections 6.1 -6.3 and shall conform to the profile in Annex A

6.3.3.2 Interface (b) (VPC to IAIC)

The VPC will pass to the IAIC the source public IP address it has received from the VSP over interface **(a)**. The response to this request will be to return the URI for the ISP LIS that the VPC should use to collect the location information. Should the IAIC not have the ISP LIS identified for the IP address requested in its tables then it will return an error response instead of a URI.

Further details on how this interface works are an implementation choice for the VPC providers to establish and the interface is not defined by this document..

6.3.3.3 Interface (c) (VPC to ISP LIS)

It is noted that the HELD specification is targeted for 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 LIS i.e. the VPC is a 'location recipient' making a third party request from a HELD perspective.

This interface uses HELD Third Party (formerly "On Behalf Of" or "OBO") queries to obtain location information for the supplied IP address(es) and is described in more detail in section 6.4. The request is directed at the ISP identified through interface (b). Annex B describes HELD as used in the UK and interface (c) implementations shall follow Annex B. Once the appropriate ISP LIS has been determined through interface (b) then a HELD location request is used to pass the IP address received on interface (a) to the identified ISP LIS. The ISP LIS responds with a location as a PIDF-LO. Further details on the content of the PIDF-LO can be found in Annex C.

The VPC will pass a timeout parameter (using "response time" parameter) to the ISP LIS by which time it needs a location response. It may be the case that a more accurate location can be obtained by waiting longer but it is important that emergency calls are forwarded as rapidly as possible. Therefore the timeout will be selected to ensure there is a response in time for the call to be routed to the responsible emergency authority without any delay perceived by the EHA operator.

Should an error response be received from the ISP LIS then this will be notified back to the EHA operator who will then query the caller verbally to obtain approximate location details to be able to route the call to the appropriate emergency authority.

Under HELD the location Request can demand the specific address location attribute 'Civic' from the LIS, but to provide maximum flexibility a catch-all location type of 'Any' shall be used. The VPC can then decide what of the returned information is usable. Annex C describes the minimum address attributes that shall be used.

The civic address information described in Annex C is a subset of the options available under [5]. Any fields utilised that are not part of this UK specification may be ignored by the VPC and not passed forward.

Although civic address is the preferred location information where the caller's device is within a limited range, some wireless devices may use wider area technology such as WiMAX, where a civic address definition may not be feasible. Further consideration to the alternative provision of geodetic coordinates will be considered in future updates of this document.

A HELD "locationURI" response will not be considered valid by the VPC.

Interface (c) shall support the HELD transaction as described above and may also support the e2 (DIAMETER) interface described in [12],which also allows an IP address to be used to request location and for it to be returned in civic or geodetic formats

6.3.3.4 Interface 4 (VPC to Emergency Call Handling System)

The Emergency Handling Authority system will pass the CLI and VSP identity it receives via the SS7 signalling to the VPC. Once the geographic location details have been obtained from a LIS by the VPC then the information contained in the resulting PIDF-LO is returned to the EHA system. The emergency call handling system will then use the location information obtained to search the EHA database and route the call to the appropriate Emergency Services control room. Where the appropriate data connection exists the address details will also be automatically passed to the Emergency Services control room using the existing interfaces used by each EHA.

Further details on how interface (4) works are an implementation choice for the EHA implementing the VPC and the interface is not defined by this document..

6.4 Generic LIS

6.4.1 Functions of the LIS

The functions of the LIS are to:

- respond to requests from the VPC, or a higher layer LIS to provide location information for a given IP address
- provide the best location information possible within a time period specified by the VPC.
- hold information on all allocated IP addresses in order to satisfy requests for location information from the VPC or higher layer LIS in a timely fashion. If possible this information should include the actual physical location as well as the associated connection end point reference (location token) each time a user logs-in.

  The LIS must be aware of when an IP address association with a location token has been granted, re-affirmed or deallocated. The location token is specific to the access method used and for example may be an L2TP tunnel ID, DHCP option 82 information, NAS port or DSL SID/Derived Line ID/Intermediate Agent Circuit ID. Information will be received over interface iC1 (shown in figure 4) about connection status. See Annex D for the Broadband Wireline case.
- obtain information about the physical end point of the user, if necessary through interaction with the access network provider(s), either through OSS/CRM interaction at provision, or through realtime interaction with a lower layer LIS.

  The LIS must be updated at least every 24 hours from other systems (typically Operational Support Systems (OSS) or Customer Relationship (CRM) systems – over an interface iM1 illustrated in figure 4. This database population mechanism and the interface mechanism used over iM1 is access network dependent and outside the scope of this document.

  The exact data elements and period for which they are stored within the LIS will be an implementation decision, based on knowledge of the access network(s) and the nature of the user connections. For example data elements would typically be the Intermediate Agent Circuit ID as the location token and the civic location form of the PIDF-LO.

  If required, requests to the lower layer LISs for location information are made using location tokens that were passed during IP authentication and/or accounting transactions.
- retain the IP/port address translation information to assist with cases where the user connection is subject to IP (and Port) address translations. In complex connectivity cases the IP address and port number may be translated several times by border and security functions including (but not limited to) session border controllers, routers and security gateways. Interface iB1 is shown in figure 4 to illustrate the need to resolve IP address translations within the immediate domain of the organisation operating the LIS. The interface details are out of scope of this document.
- purge associated connection end point information when a user disconnects from IP access such that expired connection end point information does not give rise to false responses to the VPC. Audit trails of connections are not within scope of this specification, however it may be relevant to be able to trace the location of a call shortly after an IP disconnection, particularly if the call has dropped through network failure and the emergency services still wish to locate and assist the caller.

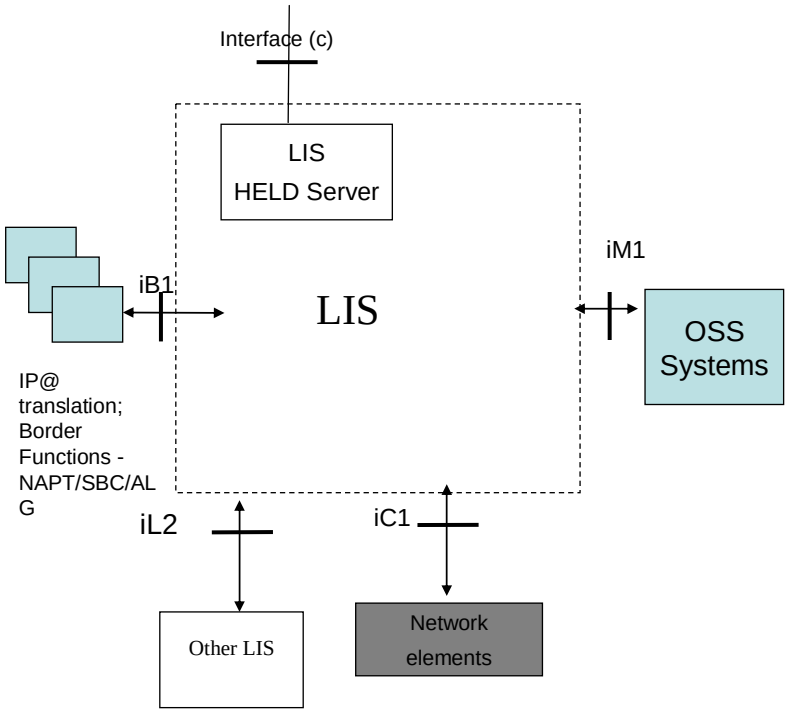


Figure 4 : Generic LIS model

6.4.2 LIS operation over interface (c)

The LIS responds to requests from the VPC over interface (c) - see figures 1 and 4 .

Location requests are received as a HELD locationRequest with the additional "device identity" reference of the target's (source's) IP address (and optionally the associated port number of the signalling end point) provided as a HELD identity extension, and the directory number of the device (or source) as a telephone URI (which will assist the LIS and VPC in tracking responses and must also be returned in the HELD response). This constitutes a HELD third party request.

The locationRequest sent by the VPC must additionally specify the location type requested as "Any"– see Annex C – and the responseTime parameter with a response required within 500 milliseconds being recommended for UK use.

The LIS HELD server will be responsible for authentication of the request : details of security requirements and recommendations are given in Annex G. Information such as date/time stamp and VPC id are derived implicitly from the message arrival time and originating IP address (of VPC).

The LIS must determine whether the device IP address is currently allocated and in use, then attempt to respond within the given time by attempting to retrieve fresh location information, yet providing what it has if attempts to obtain a fresh update time-out, or are not needed for the access networks in question. The LIS should monitor the request/response timing using its own internal timers. Time stamping of the request may be done internally by the LIS based on the time of receipt of the request, thus it will not require time stamp information within the request.

The LIS may be responsible for connections to multiple access layers - it has the task of directing the locationRequests appropriately.

Reference table for locationRequest is in section 6.4.3, Table 1 with further details in Appendix B3

The locationResponse that is sent to the VPC should contain the location object as a PIDF-LO. Civic location within a PIDF-LO would normally be expected to be returned for static access such as home or building access, whereas for access networks supporting mobility, geodetic information would usually be more suited. The option of locationURI should not be used, as this will not be supported by the VPC. Specific location type requests that limit responses to Civic or Geodetic should not be issued by the VPC as it should be access type agnostic.

Any PIDF-LO objects returned shall contain timestamp (time when PIDF-LO created), retention/expiry time and Provided-By information; the validity of a stored PIDF-LO object may be determined by the values of these parameters. The retention/expiry time parameter is set by the LIS and gives a time limit to the permitted use of a PIDF-LO. Factors influencing implementation decisions such as caching and the retention/expiry time value would include how dynamic is the nature of the connection. For example DSL users' connections would be fairly static in nature with IP address assignment typically lasting approximately 24 hours, whereas WiFi address assignment may last minutes, or less on an unreliable connection.

6.4.3 Interface (c) Primitives

Table 1: HELD Location Request

	Parameter	Mand/Optional	Description
HELD	HELD locationType	O	Type of location information requested =Any
	HELD exact	-	Specifies if LocationType must be adhered to. **Not required therefore must not be present**
	device	M	HELD Identity extension containing the target/source IP address and port details See Annex B2
	device	M	HELD identity extension as a <tel:uri> This is the E164 calling line number of the subscriber placing the emergency call. See Annex B2
	HELD responseTime	M	Time value indicating how long requestor is prepared to wait for response

Table 2 : HELD Location Response

	Parameter	Mand/Optional	Description
HELD	PIDF-LO	M	Location object containing geodetic or civic location information The presentity value in the resulting PIDF-LO MUST be sent with the tel uri provided as an identity extension in the request.

Table 3 : HELD Location Response failure

	Parameter	Mand/Optional	Description
HELD	Code	M	Failure code
	message	O	HELD Failure message

6.4.4 Other LIS interfaces

Interface iB1

This interface is needed by an LIS to resolve IP addresses where a connection path has resulted in one or more IP and port address translations, or where Topology hiding would otherwise obscure souce IP and port information. This may be implemented as either a pull or push type interface. The definition is an implementation decision and out of scope for this document

Interface iM1

OSS/CRM interface provides the LIS with a link between the physical location information and a location token. A LIS would need to be updated at least every 24 hours from other systems (typically Operational Support Systems (OSS) or Customer Relationship (CRM) systems. This database population mechanism and the interface mechanism used over iM1 is access network dependent and outside the scope of this document.

Interface iC1

This interface allows location tokens to be pushed into the LIS whenever a user attaches to the IP network.

The definition is an implementation decision and out of scope for this document. The information would typically be pushed from the AAA functions specific to the access network attachment used to log on to the ISP's service, for example iC1 could be implemented as a RADIUS authentication or accounting interface and the information passed as a location token could be assigned IP address and associated L2TP tunnel id.

Interface iL2

It is foreseen that one LIS may need to refer to another to complete a look-up request. Such cases may exist where the connection information available to higher layer LIS represents only a logical connection endpoint reference that has been assigned dynamically by a lower level access layer. Requests to lower layer access LISs can be made using HELD protocol via interface iL2 in figure 4, with the HELD Identity Extensions and HELD Measurements [see Annex section B.2 and B.3], which allow the device to be identified by its public IP address in general, or by another contextual location token understood by the access network.

Primitives for these HELD transactions are shown below.

Table 4: HELD Location Request with Measurements extension

	Parameter	Mand/Optional	Description
HELD	HELD locationType	O	Type of location information requested = Any
	HELD exact	-	Specifies if LocationType must be adhered to. **Not required therefore must not be present**
	HELD device	M	HELD identity extension as a <tel:uri:> . This is the E164 calling line number of the subscriber placing the emergency call. See Annex B2
	HELD device	M	HELD identity extension containing the device/source IP address as an identity extension. See Annex B2
	Held Measurements	M	Measurements containing 1 or more elements which uniquely define the device to the access network, ie Access network connection end point reference. See Annex B3
	HELD responseTime	M	Time value indicating how long requestor is prepared to wait for response

6.4.5 Security considerations

For security requirements and recommendations for the LIS external interfaces please see Annex G.

6.4.6 Resilience considerations

Access to the emergency service needs to be uninterrupted – the life critical nature of the service is recognised in UK regulation which says that all reasonably practicable steps must be taken to maintain, to the greatest extent possible, uninterrupted access to Emergency Organisations.

Therefore each interface and it's associated functional components shall be designed to provide a high degree of resilience – at least 99.999 % availability needs to be provided.

6.4.7 LIS Discovery

For the basic UK service, LIS discovery is described in Section 6.3.2 2.

7 International Considerations (informative)

The UK architecture for Emergency Call Location has some similarities with the NENA I2 Architecture (it tries to re-use the concept of a VPC) but also tries to use IETF standards where possible. However the UK service envisages User Agents that need not be based on the SIP protocol and it does not (at present) make an assumption that the endpoint takes an active part in the determination and conveyance of location information.

There are of course a number of cases dependant on capability and expectation of end-user device, access network capability and the country in which ISP and VoIP provider are based. These scenarios will be considered further in future updates to this document and VPCs could be expected to be enhanced to allow international access for VSPs and EHAs.

Annex A (normative): UK use of NENA i2's V2 interface for interface (a)

A.1 Purpose of UK profile of NENA i2's V2

The National Emergency Number Association Interim VoIP Architecture for enhanced 9-1-1 services (i2) [2] is the recommended architecture for the interconnection of VoIP domains with the existing emergency services infrastructure in the USA, published on December 6th 2005. This document describes a set of interfaces between various architecture elements. Where possible the names of NENA i2 interfaces have been re-used and modifed within this NICC specification with the aim of being useful when international scenarios are considered in future.

Whilst it remains a goal to interoperate with foreign systems, the current issue of this document covers situations where all entities involved are in the UK. In addition the UK scheme uses IP-based look-ups to find locations, and such location keys are not present in the NENA i2 scheme

Within the present Annex A the tables describe the information elements from V2 and their usage within the UK for interface (a). Suitable Web Service definitions and xml schema (v2.xsd) for each V2 interface message will be specified in a subsequent interface specification such that it is compatible with the NENA i2 schema [2],[3],with the expectation that this will allow straightforward adaptations to be made when future issues of this document address calls to be routed from other country's administrations using NENA i2, or NENA i2.5.

A.2 Interface (a) Primitives

There are four messages based on section 2.5.3 and section 5.3 of the NENA i2 V2 Interface specification [2] using LIE Location Key routing : two messages for updating the VPC during call establishment and two used to indicate that the call has terminated.

A.2.1 Emergency Services Routing Request (ESRRequest)

Table 7: ESRRequest

Parameter	Mandatory/ Optional/ Conditional	Description
Source	M	The identifier of the requesting VSP. i.e. the actual requester. This allows for example VSP2 to post the data in to the VPC on VSP1's behalf. In this case this field contains VSP2's id.
VSP-id	C	The identifier of the VSP originating this request. In our examples where VSP2 is often proxying the call from VSP1, this field contains VSP1's id. Where source and VSP-id are the same, only the source field is required. The large number of ITSPs expected at the VSP1 layer may mean that a VSP id is not allocated to some VSPs. So this field will be omitted or a repeat of VSP2's ID will be used. This usage is compatible with the usage described in section 5.3.1.1 of the NENA i2 specification.
Call-id	M	A unique reference generated by the VSP for this call
Datetimestamp	M	Date and time indicating UTC date and time that the message was sent
Callback	M	The E.164 number of the caller as a tel uri. This must be the same number that will be used when the VoIP call is extended into the PSTN
LIE	M	Location Information Element containing the location Key (source IP address and port number). This field in this implementation will not contain a PIDF-LO. However for compatibility with the V2 specification and future proofing of the interface, this Parameter could contain a PIDF-LO. See also Annex A3 below.
Call-orig	O	Not used in this implementation, but kept for compatibility with the V2 specification.
VPC	O	Identifier of the destination VPC. Not required for this implementation as there will only be two VPCs (corresponding to two national EHAs in the UK) and each VSP only uses one . Required for compatibility with the V2 specification

A.2.2 Emergency Services Routing Response (ESRResponse)

Table 8 : ESRResponse

Parameter	Mandatory/ Optional/ Conditional	Description
VPC	M	Identity of the responding VPC
Call-id	M	A unique reference generated by the VSP for this call
Esrn	O	The routing key. Not used in this implementation, but kept for compatibility with the V2 specification
Esqk	O	The Query Key. Not required for this implementation, but kept for compatibility with the V2 specification
Lro	O	The last routing option. Not required for this implementation, but kept for compatibility with the V2 specification
Result	M	Provides confirmation that the VPC got the request. The response codes are in table 9 of this section.
Datetimestamp	M	UTC format date and time the message was sent
Destination	O	Not required for this implementation, but kept for compatibility with the V2 specification

Table 9 : Result codes

Value	Name	Description
200	Success	Request successfully parsed and the Callback CLI and IP address have been stored in the VPC for later reference
201		Not required for this implementation, but kept for compatibility with the V2 specification
202		Not required for this implementation, but kept for compatibility with the V2 specification
203		Not required for this implementation, but kept for compatibility with the V2 specification
400	LROBadLocation	The IP address information in the LIE Location Key is badly formed
401		Not required for this implementation, but kept for compatibility with the V2 specification
402		Not required for this implementation, but kept for compatibility with the V2 specification
403	LROBadMessage	The Request message was received but the whole message was malformed
404	LRONoAuthorization	Not required for this implementation, but kept for compatibility with the V2 specification.
405		Not required for this implementation, but kept for compatibility with the V2 specification
406		Not required for this implementation, but kept for compatibility with the V2 specification
407		Not required for this implementation, but kept for compatibility with the V2 specification
408	ErrorBadMessage	Same as 403
409		Not required for this implementation, but kept for compatibility with the V2 specification, same as 404
500	LRONoResource	The VPC ran out of resources, which means the CLI and IP address will not have been stored.
501	LROGeneralError	Some internal Error occurred in the VPC, which means the CLI and IP address will not have been stored.
502		Same as 500, which means the CLI and IP address will not have been stored.
503	ErrorGeneral	Same as 501, which means the CLI and IP address will not have been stored.

A.2.3 Emergency Services Call Termination Message (ESCT)

Table 10: ESCT

Parameter	Mandatory/ Optional/ Conditional	Description
Source	M	The identity of the VSP making the call. The source as specified in ESSRRequest.
Esqk	O	Not required for this implementation, but kept for compatibility with the V2 specification
Esgw	O	Not required for this implementation, but kept for compatibility with the V2 specification
Datetimestamp	M	Date time stamp in UTC format
Call-id	M	A unique reference generated by the VSP for this call
VPC	O	Identity of the VPC

A.2.4 Emergency Services Call Termination Ack Message (ESCT)

Table 11 : ESCTAck

Parameter	Mandatory/ Optional/ Conditional	Description
Call-id	M	A unique reference generated by the VSP for this call
VPC	M	Identity of the responding VPC
Datetimestamp	M	Date time stamp in UTC format

A.3 Location Information Element - Format for IP Addresses that form location key

For the purposes of the UK V2 Interface the IP address and tcp or udp port number used as a location key is aligned with the IETF's HELD identity extensions draft [9]. As this is not yet a standard, Annex B2 includes the full schema reference - see below for examples

A.4 Web Service and XML definitions

The current NENA XML specifications can be found at [3]

A.5 Proxy inter-VSPs Interface (informative)

In some cases a proxied interface from VSP1 to VSP 2 is needed. This interface is provided as a convenience measure to ease adoption for smaller ITSPs.

It is recommendated that the Http/XML interface shall provide the following set of information:

- CLI of calling party
- Source IP address and port number of calling party's signalling end point
- ITSP ID (VSP 1 ID) – this could be a privately agreed value between VSP1 and VSP2, in which case VSP2 would be responsible for inserting its own VSP ID in the message to the VPC.
- Date and Time stamp – the format of this can be agreed between VSP1 and VSP2
- Call ID : a unique reference for this call. This is to be able to identify multiple calls against a single CLI, for example as might occur with a PBX.
- Transaction ID (to be able to notify the release of a call)
- Status of call, one of INITIATED, CLEARED.

The XML interface shall also be a transaction based on using HTTP POST and HTTP response codes, to ensure the information is correctly transferred from VSP1 to VSP2. At a minimum the application should be able to handle:

- 200 OK - XML message received and understood
- 400 Bad Request – indicating the XML message is malformed in some way, the XML message is unacceptable and should be reformatted and resubmitted
- 503 Internal Server Error - the VSP2 Server has suffered an un-recoverable error. The POST should be resubmitted.

Any further definition of this interface is outside of the scope of this document, and is a local design between VSP1 and VSP2. The above is a minimum recommendation for the content and functionality of the proxy interface.

Annex B (normative): UK Profile of HELD, HELD Identity Extensions and Measurement documents of IETF

B.1 HELD Protocol

This profile is based upon [4] HTTP Enabled Location Delivery (HELD) currently well advanced in progressing through the IETF (its in the Editor's Queue).

HELD requests sent by the VPC to the ISP LIS, or the ISP LIS to an ANP LIS, shall not initially contain a value specifying emergencyRouting or emergencyDispatch, and shall use an ANY Location Type A HELD response time attribute for both types of request is recommended to be 500 ms.

The LIS shall respond with civic location types for fixed locations and shall use either civic location or Geodetic Location data for systems such as Wi-Fi or Wimax. If a request contains the exact attribute and the Location Type Attribute does not conform with what can be supplied, the System shall respond with an error of cannotProvideLiType.

Further details are in the main text of section 6.4

B.2 HELD Identity Extensions

This profile is based upon the IETF Draft for HELD Device Identity Extensions [9]

As this is still in Draft the XML schema (which are stable) are included here for completeness and to ensure stability of this NICC document :

```
<?xml version="1.0"?>
<xs:schema
    targetNamespace="urn:ietf:params:xml:ns:geopriv:held:id"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:id="urn:ietf:params:xml:ns:geopriv:held:id"
    elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- Device Identity -->
  <xs:element name="device" type="id:deviceIdentity"/>
  <xs:complexType name="deviceIdentity">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax"
              minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="requiredIdentifiers" type="id:qnameList"/>
  <xs:simpleType name="qnameList">
    <xs:list itemType="xs:QName"/>
  </xs:simpleType>

  <xs:element name="ip" type="id:ipAddress"/>
  <xs:complexType name="ipAddress">
    <xs:simpleContent>
      <xs:extension base="xs:token">
        <xs:attribute name="v" use="optional">
          <xs:simpleType>
            <xs:restriction base="xs:token">
              <xs:pattern value="[\da-fA-F]"/>
            </xs:restriction>
```

```
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:element name="mac" type="id:macAddress"/>
<xs:simpleType name="macAddress">
  <xs:restriction base="xs:token">
    <xs:pattern value="[\da-fA-F]{2}(-[\da-fA-F]{2}){5}"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="udpport" type="id:portNumber"/>
<xs:element name="tcpport" type="id:portNumber"/>
<xs:simpleType name="portNumber">
  <xs:restriction base="xs:nonNegativeInteger">
    <xs:maxInclusive value="65535"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="nai" type="xs:token"/>

<xs:element name="uri" type="xs:anyURI"/>

<xs:element name="dn" type="id:digits"/>
<xs:simpleType name="digits">
  <xs:restriction base="xs:token">
    <xs:pattern value="[\d]+"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="hostname" type="id:domainName"/>
<xs:simpleType name="domainName">
  <xs:restriction base="xs:token">
    <!-- the following pattern does not include whitespace;
         whitespace is added only to conform to document
         formatting restrictions -->
    <xs:pattern value="([A-Za-z\d]([A-Za-z\d-]*[A-Za-z\d])*\.)*
                       [A-Za-z\d]([A-Za-z\d-]*[A-Za-z\d])*"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="duid" type="xs:hexBinary"/>

<xs:element name="msisdn" type="id:e164"/>
<xs:element name="imsi" type="id:e164"/>
<xs:element name="imei" type="id:digit15"/>
<xs:element name="min" type="id:digit10"/>
<xs:element name="mdn" type="id:e164"/>
<xs:simpleType name="e164">
  <xs:restriction base="id:digit15">
    <xs:minLength value="6"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="digit15">
  <xs:restriction base="id:digits">
    <xs:maxLength value="15"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="digit10">
  <xs:restriction base="id:digits">
    <xs:length value="10"/>
```

```
    </xs:restriction>
  </xs:simpleType>

  </xs:schema>
```

Where HELD is used between the VPC and ISP LIS and ISP LIS and an ANP LIS, the device/source IP Address, udp/tcp port number and telephone number shall be conveyed using HELD identity extensions as shown in examples below :-

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
       <ip v="4">192.168.1.1</ip>
       <udpport>51393</udpport>
</device>
```

Or for IPv6 :-

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
       <ip v="6">2001:db8:2020:2020:020f:66ff:fec9:d5db</ip>
       <udpport> 16384</udpport>
</device>
```

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <uri>tel: +442079460XXX</uri>
</device>
```

See also section 6.4 for further details.

B.3 HELD Measurements

In order that the ISP LIS can pass additional information to an ANP LIS to aid the identification of an access point, additional parameters can be specified in the associated HELD request. These are detailed in the HELD Measurements draft [10], As this is still in Draft the XML schema (which are stable) are included here for completeness and to ensure stability of this NICC document.

The HELD measurement draft is made up of three types of schemas, a containment schema, a base type schema, and a series of measurement schemas. For completeness and stability purposes the containment, base-type and DSL measurement schemas are included below.

Containment Schema

```
<?xml version="1.0"?>
<xs:schema
    xmlns:lm="urn:ietf:params:xml:ns:geopriv:lm"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="urn:ietf:params:xml:ns:geopriv:lm"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:held:lm">
    </xs:appinfo>
    <xs:documentation source="http://www.ietf.org/rfc/rfcXXXX.txt">
      <!-- [[NOTE TO RFC-EDITOR: Please replace above URL with URL of
           published RFC and remove this note.]] -->
      This schema defines a framework for location measurements.
    </xs:documentation>
  </xs:annotation>

  <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>
```

```
  <xs:element name="measurements">
    <xs:complexType>
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="time" type="xs:dateTime"/>
          <xs:attribute name="timeError" type="bt:positiveDouble"/>
          <xs:attribute name="expires" type="xs:dateTime"/>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

Base Types Schema

```
<?xml version="1.0"?>
<xs:schema
  xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:lm:basetypes">
    </xs:appinfo>
    <xs:documentation source="http://www.ietf.org/rfc/rfcXXXX.txt">
      <!-- [[NOTE TO RFC-EDITOR: Please replace above URL with URL of
           published RFC and remove this note.]] -->
      This schema defines a set of base type elements.
    </xs:documentation>
  </xs:annotation>

  <xs:simpleType name="byteType">
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="255"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="twoByteType">
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="0"/>
      <xs:maxInclusive value="65535"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="nonNegativeDouble">
    <xs:restriction base="xs:double">
      <xs:minInclusive value="0.0"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="positiveDouble">
    <xs:restriction base="bt:nonNegativeDouble">
      <xs:minExclusive value="0.0"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="doubleWithRMSError">
    <xs:simpleContent>
      <xs:extension base="xs:double">
        <xs:attribute name="rmsError" type="bt:positiveDouble"/>
        <xs:attribute name="samples" type="xs:positiveInteger"/>
```

```
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="nnDoubleWithRMSError">
  <xs:simpleContent>
    <xs:restriction base="bt:doubleWithRMSError">
      <xs:minInclusive value="0"/>
    </xs:restriction>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="ipAddressType">
  <xs:union memberTypes="bt:IPv6AddressType bt:IPv4AddressType"/>
</xs:simpleType>

<!-- IPv6 format definition -->
<xs:simpleType name="IPv6AddressType">
  <xs:annotation>
    <xs:documentation>
      An IP version 6 address, based on RFC 4291.
    </xs:documentation>
  </xs:annotation>
  <xs:restriction base="xs:token">
    <!-- Fully specified address -->
    <xs:pattern value="[0-9A-Fa-f]{1,4}(:[0-9A-Fa-f]{1,4}){7}"/>
    <!-- Double colon start -->
    <xs:pattern value=":(:[0-9A-Fa-f]{1,4}){1,7}"/>
    <!-- Double colon middle -->
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,6}
                       (:[0-9A-Fa-f]{1,4}){1}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,5}
                       (:[0-9A-Fa-f]{1,4}){1,2}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,4}
                       (:[0-9A-Fa-f]{1,4}){1,3}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,3}
                       (:[0-9A-Fa-f]{1,4}){1,4}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,2}
                       (:[0-9A-Fa-f]{1,4}){1,5}"/>
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1}
                       (:[0-9A-Fa-f]{1,4}){1,6}"/>
    <!-- Double colon end -->
    <xs:pattern value="([0-9A-Fa-f]{1,4}:){1,7}:"/>
    <!-- IPv4-Compatible and IPv4-Mapped Addresses -->
    <xs:pattern value="((:(:0{1,4}){0,3}:[fF]{4})|(0{1,4}:
                       (:0{1,4}){0,2}:[fF]{4})|((0{1,4}:){2}
                       (:0{1,4})?:[fF]{4})|((0{1,4}:){3}:[fF]{4})
                       |((0{1,4}:){4}[fF]{4})):(25[0-5]|2[0-4][0-9]|
                       [0-1]?[0-9]?[0-9])\.(25[0-5]|2[0-4][0-9]|[0-1]
                       ?[0-9]?[0-9])\.(25[0-5]|2[0-4][0-9]|[0-1]?
                       [0-9]?[0-9])\.(25[0-5]|2[0-4][0-9]|[0-1]?
                       [0-9]?[0-9])"/>
    <!-- The unspecified address -->
    <xs:pattern value="::"/>
  </xs:restriction>
</xs:simpleType>

<!-- IPv4 format definition -->
<xs:simpleType name="IPv4AddressType">
  <xs:restriction base="xs:token">
    <xs:pattern value="(25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])\.
                       (25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])\.
                       (25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])\.
                       (25[0-5]|2[0-4][0-9]|[0-1]?[0-9]?[0-9])"/>
  </xs:restriction>
</xs:simpleType>

<!-- IEEE specifies a MAC address as having a -
     between 2 hex digit pairs -->
<xs:simpleType name="macAddressType">
  <xs:restriction base="xs:token">
```

```
      <xs:pattern value="([0-9A-Fa-f]{2}-){5}([0-9A-Fa-f]{2})"/>
    </xs:restriction>
  </xs:simpleType>

</xs:schema>
```

DSL Measurement Schema

```
<?xml version="1.0"?>
<xs:schema
    xmlns:dsl="urn:ietf:params:xml:ns:geopriv:lm:dsl"
    xmlns:bt="urn:ietf:params:xml:ns:geopriv:lm:basetypes"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="urn:ietf:params:xml:ns:geopriv:lm:dsl"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:lm:dsl">
      DSL measurement definitions
    </xs:appinfo>
    <xs:documentation source="http://www.ietf.org/rfc/rfcXXXX.txt">
      <!-- [[NOTE TO RFC-EDITOR: Please replace above URL with URL of
           published RFC and remove this note.]] -->
      This schema defines a basic set of DSL location measurements.
    </xs:documentation>
  </xs:annotation>

  <xs:import namespace="urn:ietf:params:xml:ns:geopriv:lm:basetypes"/>

  <xs:element name="dsl" type="dsl:dslVlanType"/>
  <xs:complexType name="dslVlanType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:choice>
          <xs:element name="l2tp">
            <xs:complexType>
              <xs:complexContent>
                <xs:restriction base="xs:anyType">
                  <xs:sequence>
                    <xs:element name="src" type="bt:ipAddressType"/>
                    <xs:element name="dest" type="bt:ipAddressType"/>
                    <xs:element name="session"
                                type="xs:nonNegativeInteger"/>
                  </xs:sequence>
                </xs:restriction>
              </xs:complexContent>
            </xs:complexType>
          </xs:element>
          <xs:sequence>
            <xs:element name="an" type="xs:token"/>
            <xs:group ref="dsl:dslSlotPort"/>
          </xs:sequence>
          <xs:sequence>
            <xs:element name="stag" type="dsl:vlanIDType"/>
            <xs:choice>
              <xs:sequence>
                <xs:element name="ctag" type="dsl:vlanIDType"/>
                <xs:group ref="dsl:dslSlotPort" minOccurs="0"/>
              </xs:sequence>
              <xs:group ref="dsl:dslSlotPort"/>
            </xs:choice>
          </xs:sequence>
          <xs:sequence>
            <xs:element name="vpi" type="bt:byteType"/>
            <xs:element name="vci" type="bt:twoByteType"/>
          </xs:sequence>
          <xs:any namespace="##other" processContents="lax"
```

```
                  minOccurs="0" maxOccurs="unbounded"/>
        </xs:choice>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  <xs:simpleType name="vlanIDType">
    <xs:restriction base="xs:nonNegativeInteger">
      <xs:maxInclusive value="4095"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:group name="dslSlotPort">
    <xs:sequence>
      <xs:element name="slot" type="xs:token"/>
      <xs:element name="port" type="xs:token"/>
    </xs:sequence>
  </xs:group>

</xs:schema>
```

Example for a LIS only connected to an ANP using L2TP, in which case ISP LIS may only know the tunnel details (and source/Device IP address) but no ANP parameter that relates to location :

```
<measurements xmlns="urn:ietf:params:xml:ns:geopriv:lm"
  time="2008-04-29T14:33:58">
   <dsl xmlns="urn:ietf:params:xml:ns:geopriv:lm:dsl">
     <l2tp>
       <src>192.0.2.10</src>
       <dest>192.0.2.61</dest>
       <session>528</session>
     </l2tp>
   </dsl>
</measurements>
```

Annex C (normative): UK Profile of the location object PIDF-LO

C.1 RFC 5139 Revised Civic Location Format for PIDF-LO

Whilst it remains a goal to interoperate with foreign systems there are country specific geographic location features. The civic location format proposed by RFC 5139 [5] (see also RFC 4119) is intentionally global in its considerations and has many options. This section provides guidelines for the creation of civic addresses to meet UK requirements. The country element indicates the context in which the PIDF-LO was created. Future updates to this document will consider international implications.

This profile is based on the Revised Civic Location Format for PIDF-LO [5]

For successful onward routing and uniformity of location detail provided with other technologies it is important the address information is provided in the location response. Many of the address fields are marked as 'Optional' but full address information as would be meaningful to the emergency services should be populated in these fields. Relevant fields are listed below.

In the UK it is proposed to use the ADDCODE parameter to pass the Unique Property Reference Number (UPRN). This is being introduced as a more accurate location definition for use by the Emergency Services. Where this is available it should be provided as specified below. The field prefix will be the characters 'UPRN', followed by the 12 digit UPRN as defined by BS7666.

Table 12 : LocationResponse

Parameter	Mand/ Optional	Description	Example	Comment
country	M	The country is identified by the two-letter ISO 3166 code – GB for this specification	GB	
A1	O	National subdivisions	BRC	Although the default is ISO.3166-2, it may be more meaningful to use ENG/NIR/SCT/WLS
A2	O	County, Parish	Berkshire	
A3	M	City, township	Bracknell	Post town
A4	O	City division, borough, city district, ward		Village or other community
A5	O	Neighbourhood, block		
RD	O	Primary Road or Street	Longshot Lane	
HNO	O	House number, numeric part only		For a residential address this is highly desirable
HNS	O	House number suffix		
BLD	O	Building	Waterside House	
LOC	O	Additional location information		Use as a catch-all where address detail does not fit BLD or HNO/HNS
NAM	M	Name (residence, business or office occupant	Cable&Wireless	
PC	M	Postal code	RG12 1XL	
ADDCODE	O	Unique Property Reference Number - Format UPRN999999999999		

Annex D (normative): Wireline Broadband LIS

D.1 General

The ISP provides internet access to its customer via access network(s). In the general case the ISP, Backhaul and Aggregation Provider (BAP) and Local Loop Provider (LLP) are separate entities, and have been treated as separate functional entities within the model.

The customer's internet access is a logical connection of their access device to a public IP address and a virtual path through the access media and access network to the internet.

There are different connection models employed by the ISP to be considered, these affect how the LIS operates, yet the general principle is the same in each case for location determination.

Type (i) : ISP also operates the access network. The ISP has access to all information about the user's connection within its own domain.

Type (ii) : BAP is separate to the ISP. The BAP and LLP provides a virtual access path from the end user device, a handover point and may provide limited authentication, for example authentication that the line has valid broadband access. The ISP verifies end user credentials, assigns an IP address and connects the virtual access path to the internet.

In the type (ii) case there are specific identifiers conveyed at the handover : these are referred to as location tokens (connection end point references) which may be an L2TP tunnel ID, Agent Circuit ID/Derived Line ID, Service ID (SID) or an IP address. The term *Access Network Providers* (ANPs) will be used to refer to the BAP and LLP arrangement providing an access service to the ISP. Some ANPs introduce a Service ID (SID), which is based on the Agent Circuit ID or a Derived Line ID (see D2).

Annex E, Figures E1 and E2, shows an informative example of the functional entities and messaging for the type (ii) case with an ethernet backhaul so DSLAM converts from PPPoA to PPPoE through an intermediate agent that introduces an Agent Circuit ID.

D.2 ISP LIS functional description

The function of the ISP LIS is to track connections based on information received from the lower access layers. In the wireline ISP implementation of the generic LIS model , the ISP LIS relies on information from a RADIUS server collected at subscriber connection time to record the IP address and its associated connection end point reference.

The RADIUS Accounting request (received at connection time by the ISP) SHOULD contain a connection endpoint reference which uniquely identifies the physical circuit and thereby the location of the user. Such identifiers would be a Service ID (SID) based on an Agent Circuit ID created by an intermediate agent at a DSLAM for PPPoE termination [13], or a derived Line ID (based on combination of BRAS id, ATM port id, Virtual Path and Circuit information that relates to a DSLAM terminated copper access line) for PPPoA termination. An informative PPPoE example is shown in Annex E, Figures E3 and E4 where the ISP delegates IP address allocation to the BAP's BRAS, which is one widely used configuration in the UK.

The remainder of this annex will assume the physical circuit reference can be supplied by the BAP. If however the connection endpoint reference is non circuit specific such as L2TP tunnel identifier, the ISP LIS may need to forward the request on to the BAPs LIS to resolve. This is catered for in the Generic LIS model using interface iL2.

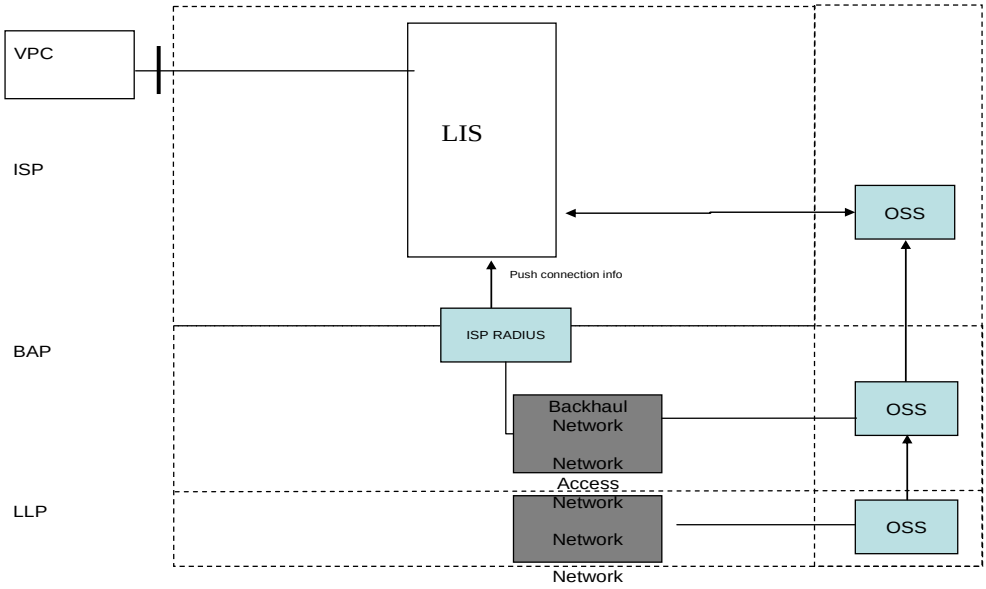


Figure D1 : Wireline ISP LIS functions, showing BAP/LLP boundaries

D.3 Implementation (normative)

D.3.1 Type (i) access

An ISP's customer will provide account information, including location of where the broadband connection is provided, to the ISP in order to be provided with service to the internet (when a customer "signs" a contract with an ISP at service provision). The association between connection end point reference and the location must be stored in the OSS system of the the ISP.

At the time of each network connection/attachment, a *public* IP address will be assigned from a pool of IP addresses owned by the ISP. Static assignment is also possible but can be handled in the same fashion. The ISP's RADIUS servers authenticate the line ID and user logon credentials (probably two radius servers involved which could include one for Access Network function and one for ISP function), assign the IP address to the line ID which is the connection end point reference (either directly or through a BRAS or LNS) and directs the PPP session to terminate on a BRAS instance or LNS switch.

Connection information (IP address and line ID) SHOULD be forwarded to a LIS when a user is authenticated or when an accounting record is received by the radius servers involved, but the decision to use connection information logged in the LIS as opposed to querying RADIUS logs for information at time of a VPC request would be an implementation decision. An ISP would also (a) decide whether to deploy separate Access Network LIS and ISP LIS entities to separate the interaction with the underlying access network (which it controls in this scenario), and (b) decide in which LIS to provide the location database of connection end point reference/location token against civic address.

D.3.2 Type (ii) access

Where the BAP is a separate organisation, the ISP LIS must manage the “real-time” requests from the VPC and if necessary to each access provider (BAP+LLP).

By separate arrangement at the OSS/CRM customer management layer, the ISP will require a regular feed of connection end point reference/physical line identifier from the BAP or LLP at provision or amendment of service to an end customer. Such information must be associated with the end customer’s known location (usually known by the ISP when the service is requested by the customer and the request for service is passed to the customer’s Access Network) and the association is fixed for the customer and does not require real-time lookup methods. An informative provisioning flow for OSS customer management systems is shown in Annex E, figure E5.

Alternatively, the ISP may require real time connection information from the BAP with a location token that can be used to reference a physical location. Those parts of HELD Device Identity Extensions and HELD Measurements included in Annex B allow the ISP LIS to make HELD requests to an Access Network LIS - these requests may contain the IP address of the end-user but may also use an appropriate connection end-point identifier such as L2TP to identify a tunnel session, using a HELD measurement parameter. In this case the ISP LIS is reliant on the Access Network to provide timely information, so it should cache location information with an associated PIDF-LO retention/expiry time and in this way it is able to provide a best effort response if nothing is received from the access network.

An Informative example of a call flow is given in Annex F.

Annex E (informative): Broadband and ADSL Access

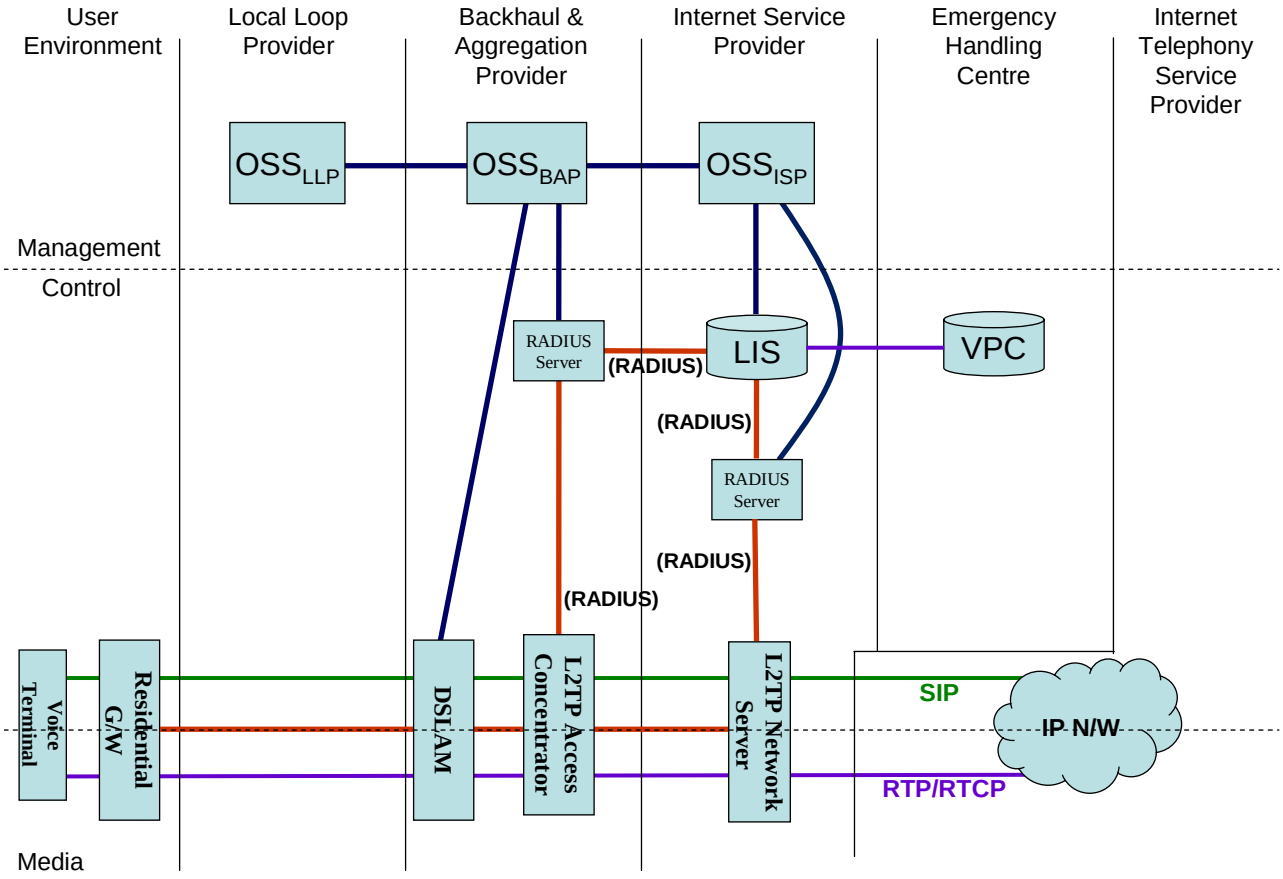


Figure E1: xDSL Architecture for PPP Tunnelled via L2TP to ISP

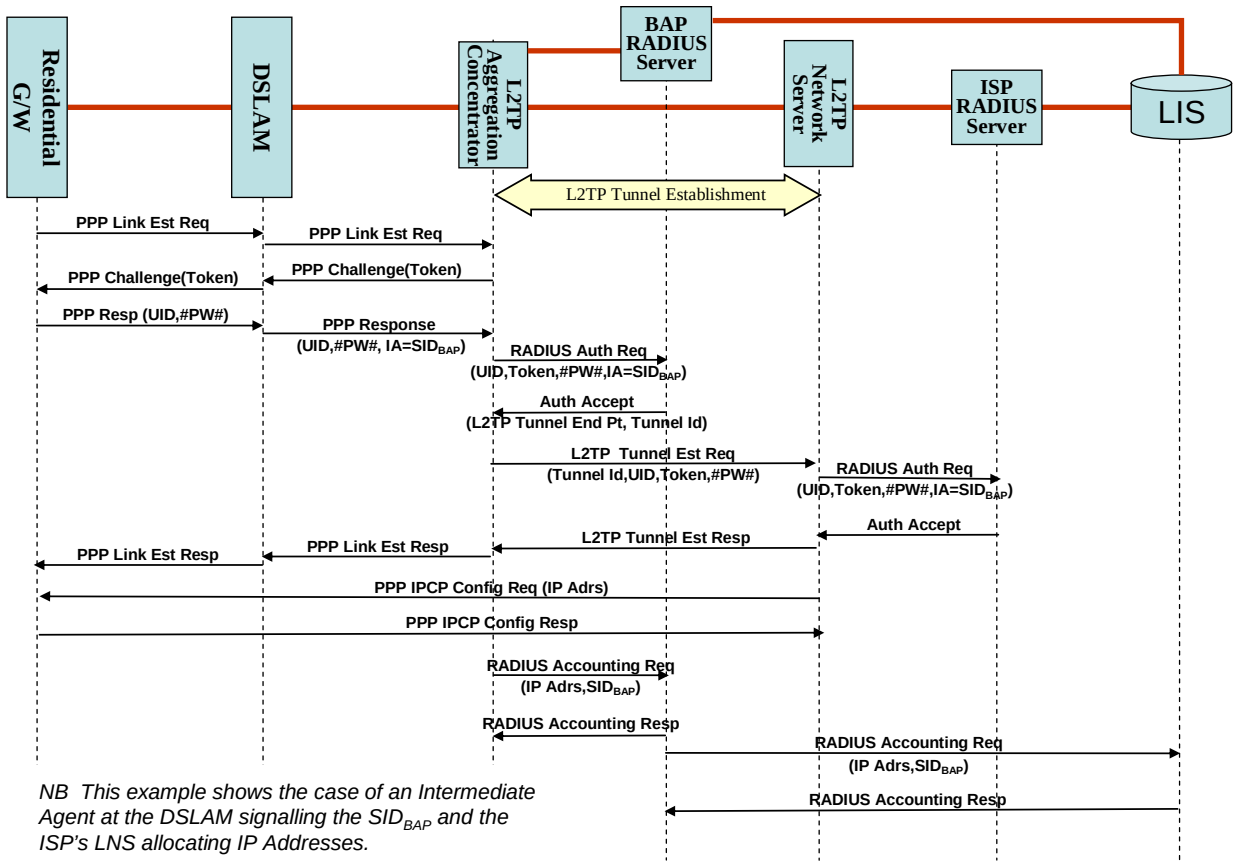


Figure E2: Network Attachment for PPP Tunnelled via L2TP to ISP

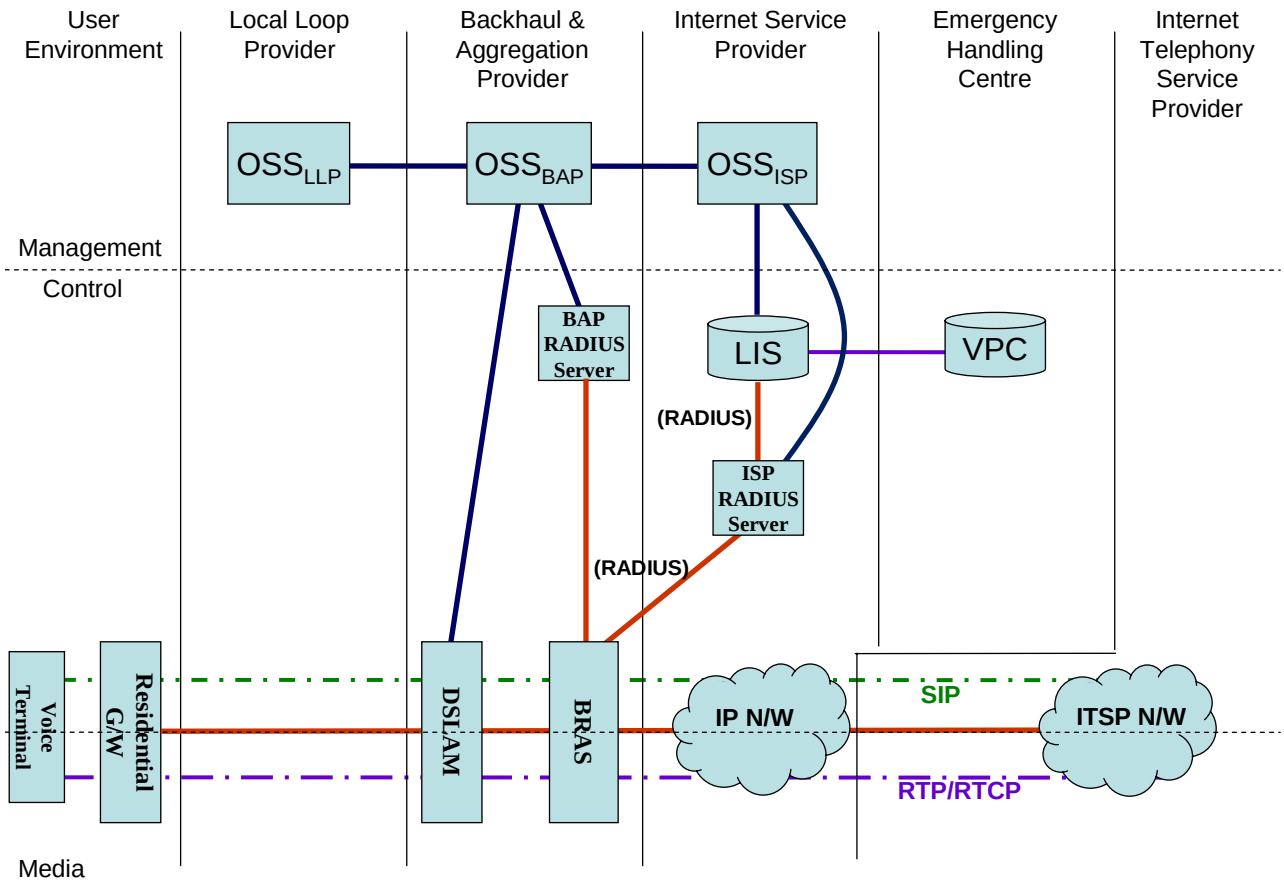


Figure E3: xDSL Architecture for PPP Terminated by Backhaul and Aggregation Provider

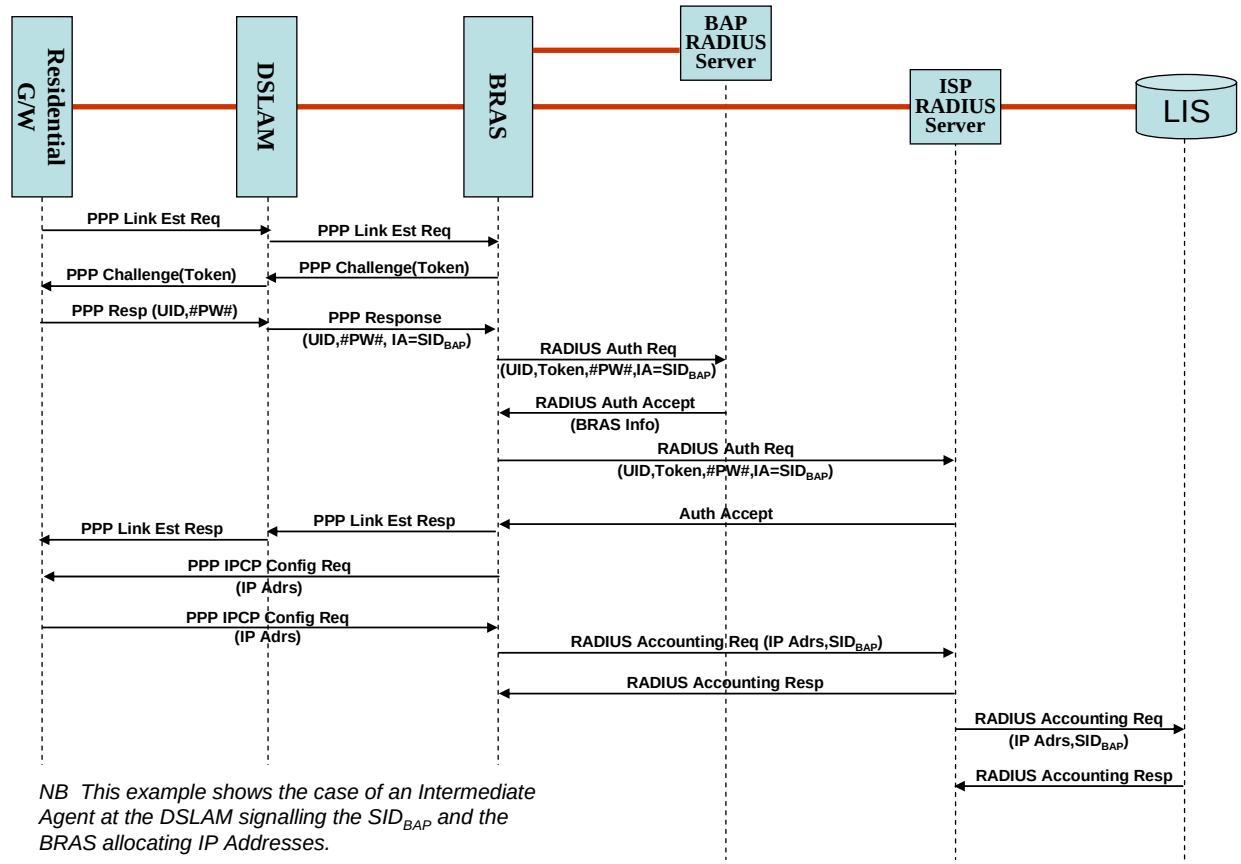


Figure E4: Network Attachment for PPP Terminated by Backhaul and Aggregation Provider

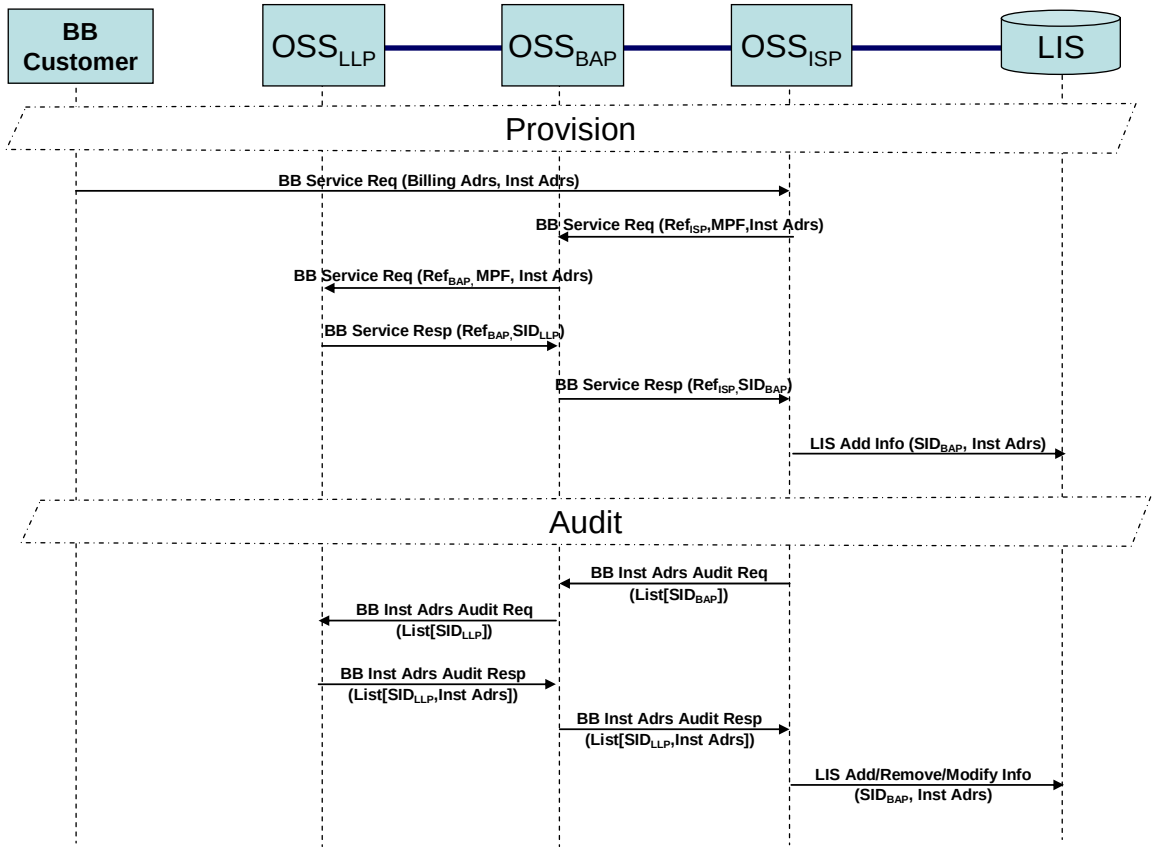
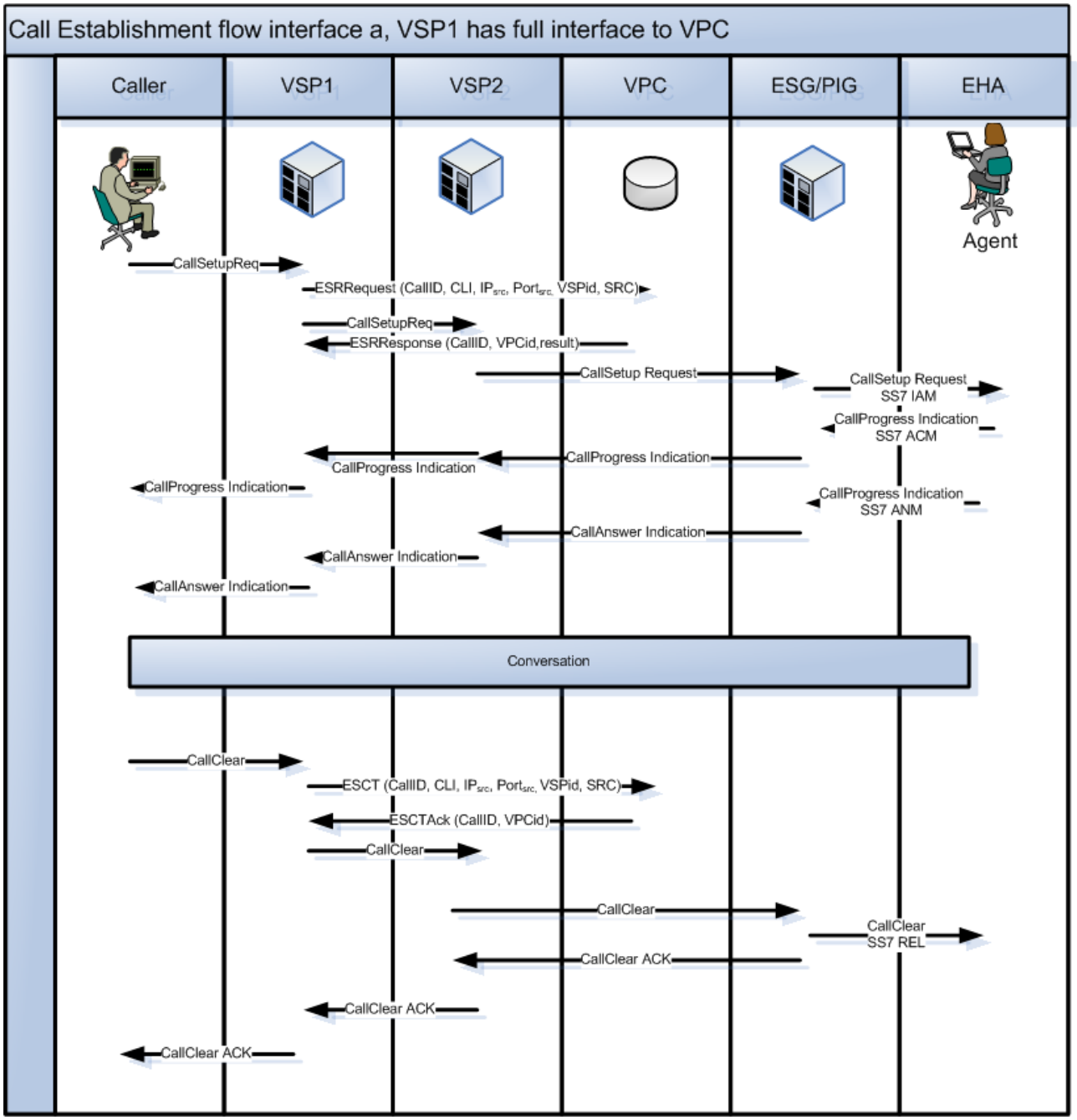
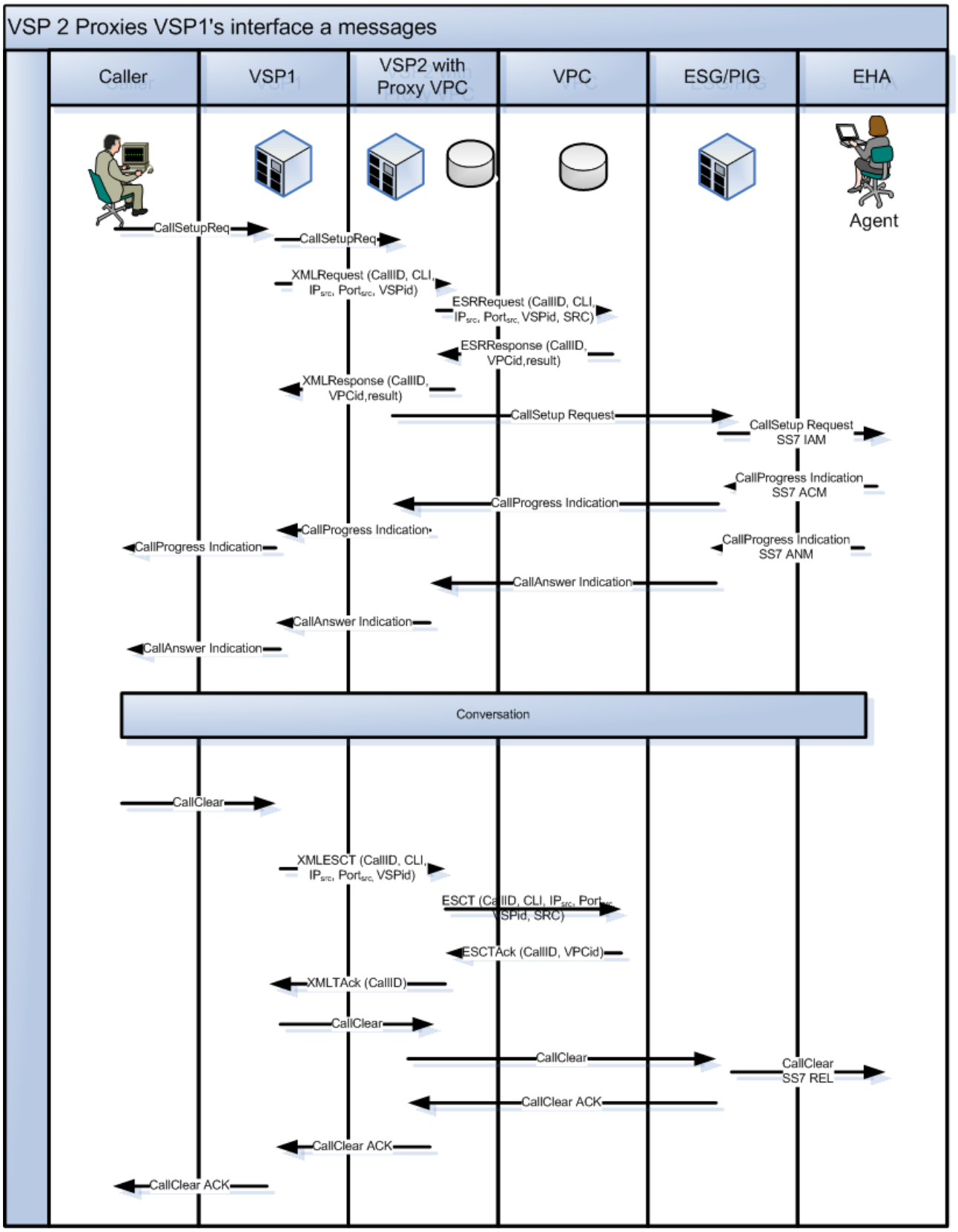


Figure E5: BB Provision and Audit on a MPF Line For Binding of Service Identifier (SID) to Installation Address (Inst Adrs)

Annex F (informative): Call Flows

This annex shows the example call flows from caller to Emergency Services Gateway. It demonstrates the telephony path and the location information flows.




VSP 2 Proxies VSP1's interface a messages
Caller
VSP1
VSP2 with Proxy VPC
VPC
ESG/PIG
EHA
Agent
CallSetupReq
CallSetupReq
XMLRequest (CallID, CLI, IPsrc, Portsrc, VSPid)
ESRRequest (CallID, CLI, IPsrc, Portsrc, VSPid, SRC)
ESRResponse (CallID, VPCid,result)
XMLResponse (CallID, VPCid,result)
CallSetup Request
CallSetup Request SS7 IAM
CallProgress Indication SS7 ACM
CallProgress Indication
CallProgress Indication
CallProgress Indication
CallProgress Indication SS7 ANM
CallAnswer Indication
CallAnswer Indication
CallAnswer Indication
Conversation
CallClear
XMLESCT (CallID, CLI, IPsrc, Portsrc, VSPid)
ESCT (CallID, CLI, IPsrc, Portsrc, VSPid, SRC)
ESCTAck (CallID, VPCid)
XMLTAck (CallID)
CallClear
CallClear
CallClear SS7 REL
CallClear ACK
CallClear ACK
CallClear ACK

Annex G (informative): Security Considerations

G.1 General

The large number of VoIP and Internet Service Providers make it impractical to use private circuits/VPCs so the external interfaces (ie between different organisations) will need to work over the internet

The selected security measures should :-

- impose minimal performance overhead as speed is critical for 999 operations
- be robust and reliable for 999 operations
- be widely known/easy to use for range of organisations (of widely varying size) involved

This information needs to be assured because it is used for purposes that relate to safety of life applications. There is also a threat that this data may be corrupted deliberately or intercepted for financial gain. In the face of these threats there is a need for authentication of the sending organisation and also authentication of the receiving organisation to prevent any attacks caused by the expected threats.

The location of individuals also needs to be protected from eavesdroppers so it is necessary to provide confidentiality of the data in transit. Additionally the location of emergency callers needs to be protected from errors, whether introduced deliberately or not, and so an integrity mechanism is recommended. Since locations are specified using XML it is recommended that digital signatures are used to assure message integrity.

In particular :-

- all communications shall be protected from interception.
- it shall be possible to authenticate that the communications are from authorised entities
- messages shall be communicated without the possibility of tampering by a 3rd party (if modified, it shall be possible to detect this)
- measures shall prevent denial of service attacks

A mutual authentication mechanism is required and all of the transport mechanisms so far envisaged use http, hence the use of TLS would seem appropriate. It is recognised that TLS adds a slight delay for authentication each time a session is established and that it is unlikely that long lived sessions will be maintained. The range of sizes of organisations co-operating in VoIP location means that whilst TLS represents a low cost option it may be unsuitable for larger operators.

As an alternative, the authentication and confidentiality requirements can also be met using IPSEC and current NICC recommendations should be used to aid the setting of options.

G.2 Authentication Mechanism

The management of identity remains to be resolved and there needs to be a clear process for the issuing and signing of certificates to be used for mutual authentication.

The details of this scheme are outside the scope of the present document.

The certificates when used for TLS shall produce a session key of 128 bits which will allow the data transferred to meet the confidentiality requirement for a period in excess of that needed, which is perhaps of the order of weeks. In common with all security requirements of this type the key length should be kept under review, a review every five years is recommended at the outset.

The keys used for digital identity should be chosen to meet the security objective. The objective should be that the keys remain valid for non-repudiation for not less than five years after five years use of the system, i.e. a design life of ten years. This probably indicates that a 2048 bit key should be recommended if RSA is used.

Annex H (informative): History

Document History		
V1.1.2	March 2010	NICC Approved (minor editorial change as figures did not print)