ND1519 V1.1.1 (2022-01)

NICC Document

Implications and Consequences of the UK implementing ETSI ES 203 178

NICC Standards Limited

c/o TWP ACCOUNTING LLP,
The Old Rectory,

Church Street,

Weybridge,

Surrey KT13 8DE

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

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.

Foreword

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

Executive Summary

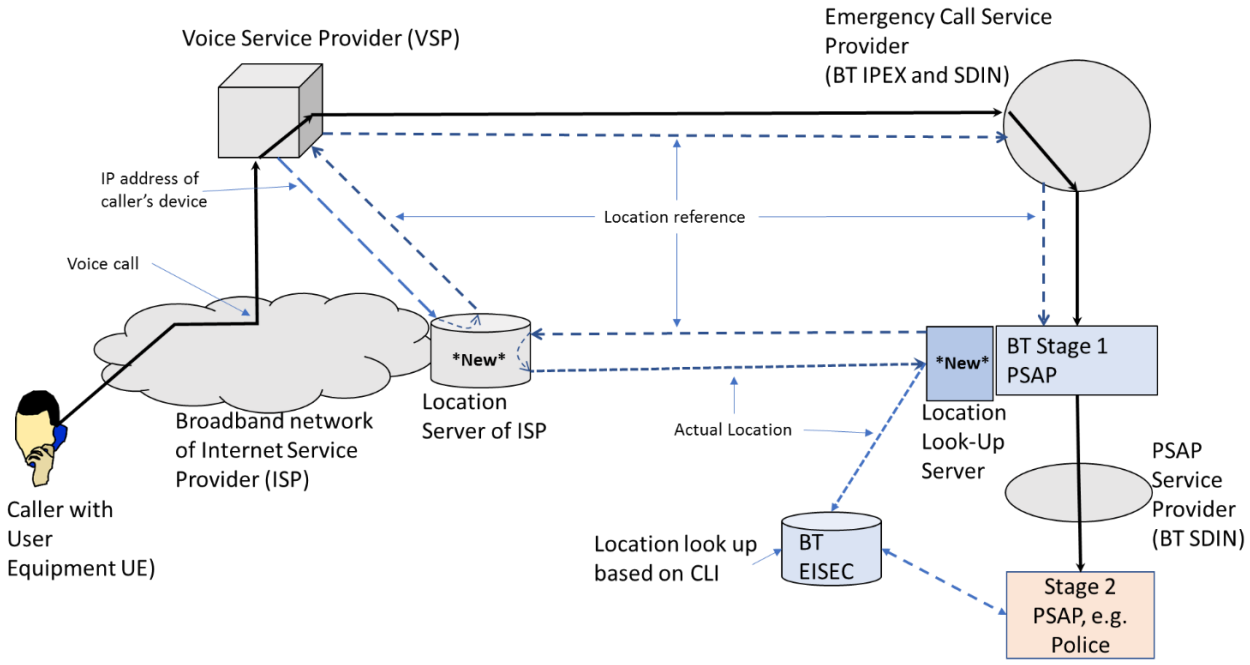
For the avoidance of doubt, this document concludes that at the present time, the full implementation of ETSI M493 is not appropriate for the UK. However, a more focused analysis of UK Use Cases will be carried out with a view to publishing a new ND detailing solutions.

The European Telecommunications Standards Institute (ETSI) has published standards ES 203 178[1] and ES 203 283[2] to try to ensure that an emergency call made using a VoIP service can be routed to the appropriate Emergency Authority (EA) and that the EA has accurate caller location available at the same time that the call is answered. This covers fixed, mobile and nomadic VoIP users.

This report considers the scope and applicability of the ETSI approach for implementation in the UK. For example, it is not expected to be needed in cases where fully satisfactory emergency calling solutions already exist, such as where the VSP is only supporting a service delivered at one location over a fixed line, or when the VSP and Interconnect Service Provider (ISP) are both the same mobile network for which existing 3GPP solutions and/or use of Advanced Mobile Location (AML), can provide good locations. However, it can be expected to cover many cases where a VSP can readily identify the access ISP, such as an “over the top” VSP (e.g. Skype, Vonage) supporting a nomadic device using a public Wi-Fi access point, or a residential broadband line for a voice call.

The approach is unable to cover all end user cases in an increasingly complex communications environment, such as cases where it is not practical to identify the access ISP due to various security measures, e.g. within virtual private networks used by Corporate Enterprises for nomadic workers, or cases where a mobile handset has to fall back to Wi-Fi, provided by another access provider, when there is no available mobile RAN.

The figure below shows in outline how the ETSI approach could be implemented in the UK, should the approach be adopted.



Under the architecture of the ETSI standard, the procedure for ensuring the correct processing of an emergency call would be as follows:

1. **The caller's User Equipment (UE) makes an emergency call request** to its VSP and may, in some cases, include location information from the UE (such as handset derived location information in form of GPS coordinates). The ETSI approach covers both the case where VSP is in the UK and where its call server may be in another European country.
2. **The VSP is then required to find the UE's network location from the ISP** and to identify the correct PSAP which the call should be routed to. Once the location is confirmed as the UK, things are straightforward as there is a single Stage 1 PSAP for the UK. The VSP uses a new process to determine the identity of the ISP and the associated network information needed to contact the ISP's Location Server (LS) – known as the 'LS discovery' process. This process requires all Access Network Providers (ANPs) to provide physical address information to the ISPs, who need to establish and maintain a Location Server and ensure that it can be discovered through readily available protocols. Such protocols have been described, but it is not known whether they satisfy the reliability, security and accuracy requirements that would need to be established for widespread use.
3. **The VSP interrogates the ISP's Location Server (LS) to determine the Location Reference**. Using the IP address (and other information associated with the call) the VSP receives from the Location Server (LS) a unique Location Reference, which, in and of itself, is insufficient for the VSP to identify the location of the caller. The use of a Location Reference maintains appropriate privacy for the UE as it avoids the VSP being given a network provided UE location by the ISP. The Location Server also provides the identity of the PSAP to which emergency calls should be routed - this is the way by which the VSP can determine whether the call needs to be routed abroad. For ISP LSs in the UK this will simply be the Stage 1 PSAP. The identity of the PSAP will be in the form of a URL (Uniform Resource Locator) of the PSAP's Emergency Call Service Provider (ECSP).
4. **The VSP routes the emergency call towards the Emergency Call Service Provider**. With knowledge of the appropriate ECSP and with the associated Location Reference, the VSP routes calls to the ECSP, potentially via an intermediary voice aggregation provider (VAP), with whom a trusted relationship has been previously established. The VSP (or VAP) must establish a trusted relationship with the ECSP before providing service to prevent the ECSP from having to handle calls from unrecognised entities, which would elevate the risk of attacks on the ECSP. However, while the technical methods/protocols to achieve this exist, to create these relationships VSPs will first need to identify the appropriate ECSP(s) in each relevant country. It is not clear which organisation, even simply for the UK, would determine and maintain ECSP and VAP contact details to be provided to any VSP so that they could then learn what was needed for that ECSP (or ECSPs in some countries) to accept their emergency calls.
5. **The VSP also sends the Location Reference of the UE to the ECSP**. Once a solution is established and adopted, the VSP would be required to send network provided location information for the UE (which for the UK is expected to be a Location Reference), and any location information that may be provided by the UE itself, to the ECSP within the SIP signalling.
6. **The ECSP then routes the call onward towards the Stage 1 PSAP**, via the PSAP Service Provider (PSP, which is also a function of ECSP in the UK).
7. **The Stage 1 PSAP uses the Location Reference to interrogate the Location Server to retrieve the location of the caller.** In addition to a reference, the SIP signalling also contains the identity of the ISP Location Server that issued the reference. With this information the stage 1 PSAP can interrogate the Location Server to retrieve the physical location of the UE. This communication would be via a secure connection given the sensitivity of the information being transferred.
8. **The Stage 1 PSAP is then able to route the call to the most appropriate Stage 2 PSAP** (e.g. London Ambulance) again using the PSAP Service Provider and to provide the EA's Stage 2 PSAP with the network location of the UE and any location provided by the UE itself. The Stage 1 PSAP is initially expected to convey location through the existing "out of band" EISEC interface to Stage 2 PSAPs. It is expected that location conveyance via SIP signalling would also be gradually deployed as the Stage 1 and Stage 2 PSAPs become more fully SIP enabled.

The way in which components operate and interact is defined in ES 203 283; how well they are expected to perform is not. Non-functional requirements and expected performance standards will need to be developed by NICC covering aspects such as:

- Location establishment timeout values;
- Enquiry throughput (peak, burst and average);
- Response time between enquiry and response.

To ensure the successful conveyance of emergency calls to the appropriate emergency service and to provide accurate location information, new protocols, procedures, relationships and components (hardware) are required. These requirements are summarised below:

1. **All ISPs would need to operate and maintain a Location Server (LS).** This includes those ISPs that offer only broadband and/or Wi-Fi connectivity. Such servers track, in real time, the physical access points to which an IP address is currently allocated.

2. **All ISPs need to keep up to date details of the IP addresses for which it is responsible**, as well as the address (URI) of its Location Server, and provide this information to the organisation managing the Location Discovery facility.

3. **One or more organisations need to create and maintain a Location Discovery facility**. If one organisation establishes this, then it needs to advertise to all European ISPs of its existence and the process for uploading information. If each country creates its own database/facility, then all VSPs across Europe will need to know the address of each, and have processes by which to interrogate them all in a prompt manner when a call from an unknown IP address is received.

4. **An ISP's Location Server must provide location reference details to any requestor.** As it is not possible to differentiate requests from valid VSPs and general requests, the LS must be robust enough to withstand erroneous/malicious attacks on these open (public) interfaces. It also needs sufficient resources to respond to requests for information promptly, as without the correct routeing information the VSP is unable to forward the call to the correct PSAP, leading to delays in call set-up and answer.

5. **All ISPs must establish a trust relationship with the PSAP**, so as to allow secure communications between them to convey accurate location information from the Location Server.

6. **All VSPs must incorporate the following protocols** into their emergency call handling procedures:

    a. To interrogate the Location Discovery database(s) to quickly identify the correct Location Server from which to request location information;

    b. To route calls to the correct PSAP and include the necessary location(s);

    c. Provide a VSP identifier (VSP ID); and

    d. To have robust exception handling processes in place for when lookups and queries are unsuccessful, provide erroneous information, and/or take too long to achieve.

7. **All VSPs must establish a trusted relationship with the ECSP**. This can be achieved either:

a to directly route emergency calls or

b form a contractual relationship with an aggregating VSP to do so on its behalf.

8. **The PSAP needs to create a Location Look-Up capability** (shown as Location Look-Up Server in the architecture figures) which will enable it to interrogate, in real time, the relevant ISP Location Server identified by the Location reference in order to retrieve a valid location.

9. **All parties will need to ensure that network components allow the conveyance of key SIP fields.** VSPs, ISPs, ECSP, Stage 1 PSAP need to ensure that SIP fields used to convey location and VSP identity can be transmitted. Additionally ISPs and VSPs must allow emergency call IP flows (IP address, port number and IP version) to be tracked across network components (such as Firewalls).

10. **There needs to be an organisation to allocate and manage VSP IDs**.

For emergency calls to successfully use the approach set out here, all organisations identified need to take on new roles and responsibilities. For example, a new entrant VSP will need to:

- Identify any and all Location Server discovery databases in all countries in which it advertises service provision
- Identify and establish the routeing details and mechanisms to all PSAPs in all countries in which it advertises service provision (and potentially in countries in which its customers may roam and make emergency call), so as to ensure that calls by its subscribers arising in any country can be successfully routed. The VSPs will also need to register and form a trusted relationship with all ECSPs to ensure that calls can be identified as legitimate for onward routeing to the PSAP. If such direct mechanisms/registrations are not possible then the VSP must establish relationships with one or more (usually larger) VSPs that act as a VAP and will route calls to any and all PSAPs in Europe.

Similarly, a new ISP or broadband provider that has not previously had a direct role in providing an emergency service, will need to:

- Identify any and all location discovery databases across Europe, make contact and upload relevant IP address ranges and network address details for their Location Server (to assist VSPs offering service to subscribers in the UK);
- Contact the relevant PSAP to agree and establish the secure communication channel needed for the PSAP to recover location information from a location reference issued by that ISP.

Even with strictly defined technical standards and regulations, effective coordination and dialogue is likely to be needed.

Introduction

In traditional telephone networks, both fixed and mobile, the identification of calls through a telephone number of a line or a SIM card is directly linked to the physical infrastructure being accessed. When the network recognises that an emergency call is being attempted, amongst other things, the network has a generally clear understanding of the caller's location. Knowing the caller's location is important for two reasons: firstly, it allows the call to be passed to the nearest, or most appropriate, Public Safety Answering Point (PSAP), and secondly it allows the emergency services to more quickly dispatch assistance, particularly when callers are unable to provide sufficient information.

In 2020 only about 4% of emergency calls came from IP originated devices where the location of the caller was uncertain. However, this is still around 0.7 million calls each year and is expected to increase substantially over the coming years. Moreover, for IP-based calls, there is no direct association of call identification (normally the telephone number) and the physical location of the caller; further, the voice Service Provider (VSP) may not be able to know the location of the caller based on the IP-address or other signalling information available. Indeed, the VSP may not know even the country from which the call is being made, making the correct routeing of the call to the appropriate PSAP extremely difficult.

In May 2011, the European Commission set out a mandate M/493: "Standardisation Mandate to the European Standards Organisations (ESO) in support of the location enhanced emergency call service" for the following requirement: "*The process for the determination of the location of fixed and more importantly nomadic VoIP users in case of an emergency is required. This is particularly needed when the originating VoIP Service Provider is an enterprise separate from lower layer Service Providers as well as one or several contributing infrastructure operators.*"

In response the relevant European Standardisation body (ETSI) set up a working group to construct a suitable standard [DES/E2NA-00001-M493-stage2].

ETSI has subsequently published standards ES 203 178 and ES 203 283 to try to ensure that (if implemented) an emergency call made using a VoIP service any country where these standards are implemented can be routed to the appropriate emergency authority (EA) in the correct country, and that the EA has accurate caller location available at the same time that the call is answered. This covers fixed, mobile and nomadic VoIP users.

In 2010 NICC published ND1638, a standard that set out a method by which caller location from VoIP emergency calls could be reliably and automatically derived ND1638 focused on the case where all parties are in the UK and Asymmetric Digital Subscriber Line (ADSL) access is used, which was considered to be the predominant use case.

The most recent regulation (EECC Recital 256) says that: "Member States should ensure that standards ensuring accurate and reliable routeing and connection to the emergency services are implemented as soon as possible in order to allow network-independent providers of number-based interpersonal communications services to fulfil the obligations related to access to emergency services and caller location information provision at a level comparable to that required of other providers of such communications services. Where such standards and the related PSAP systems have not yet been implemented, network-independent number-based interpersonal communications services should not be required to provide access to emergency services except in a manner that is technically feasible or economically viable."

1 Scope

This document reviews the ETSI architecture and protocols (ETSI ES 203 178 and ETSI ES 203 283) to describe how these could be implemented in the UK, and what would be required from Internet Service Providers (ISPs), as well as VoIP SPs (VSPs), transit networks and the PSAPs.

The ETSI approach is not expected to be needed in cases where fully satisfactory emergency calling solutions already exist – for example where the VSP is only supporting a service delivered at one location over a fixed line, or when the VSP and ISP are both the same mobile network for which existing 3GPP solutions and/or use of AML, can provide good locations.

It can be expected to cover many cases where a VSP can readily identify the access ISP, such as an “over the top” VSP (e.g. Skype, Vonage) supporting a nomadic device using a public Wi-Fi access point, or a residential broadband line for a voice call.

However, it is unable to cover all end user cases in an increasingly complex communications environment, such as cases where it is not practical to identify the access ISP due to various security measures, e.g. within virtual private networks used by Corporate Enterprises for nomadic workers, or cases where a mobile handset makes a call controlled by the mobile network as VSP, but has to use a Wi-Fi Access Point of another provider.

This report sets out known use cases where the ETSI approach would help and the risks of not providing a solution, as well as seeking to include some estimated volumes of the various use cases.

In the UK there is a single Stage 1 PSAP and this report assumes that this architecture will continue for the foreseeable future. In view of the significant changes that will be needed to support the ETSI approach, this report also assumes that the Stage 1 PSAP is IP-based, as the project to make that change from TDM to SIP is at the time of writing, in implementation.

2 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:

[1] ETSI ES 203 178: "Functional architecture to support European requirements on emergency caller location determination and transport".

[2] ETSI ES 203 283: "Protocol specifications for Emergency Service Caller Location determination and transport"

[3] IETF RFC 1918: ” Address Allocation for Private Internets”

[4] IETF RFC 3261: “SIP: Session Initiation Protocol”

[5] IETF RFC 3264: “An Offer/Answer Model with the Session Description Protocol SDP)”

[6] IETF RFC 3325: “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”

[7] IETF RFC 4320: “Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction”

[8] IETF RFC 5222: “A Location-to-Service Translation Protocol”

[9] IETF RFC 5393: “Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies”

[10] IETF RFC 5954: “Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261”

[11] IETF RFC 5985: “HTTP-Enabled Location Delivery (HELD)”

[12] IETF RFC 5986: “Discovering the Local Location Information Server (LIS)”

[13] IETF RFC 6422: “Relay-Supplied DHCP Options”

[14] IETF RFC 6442: “Location Conveyance for the Session Initiation Protocol”

[15] IETF RFC 4566: “SDP: Session Description Protocol”

[16] IETF RFC 6967: “Analysis of Potential Solutions for Revealing a Host Identifier (HOST_ID) in Shared Address Deployments”

[17] IETF RFC 7216: “Location Information Server (LIS) Discovery Using IP Addresses and Reverse DNS”

[18] IETF RFC 7852: “Additional Data Related to an Emergency Call”

[19] ND 1035 – “SIP Network to Network Interface Signalling”

[20] ND 1016 –“Requirements on Communications Providers in relation to Customer Line Identification display services and other related services”

[21] ND 1439-“ Guidance for Implementing ND1016 in SIP networks”

3 Definitions, symbols and abbreviations

3.1 Definitions

Access Network Provider (ANP): Service Provider that provides physical and IP connectivity to a User Equipment (UE) via a fixed or mobile access.

NOTE 1: The access network may be provided by a single organisation or it may be provided by a number of different organisations, BUT the interfaces between these organisations are not relevant to the scope of the present document as it is a matter of contractual relations between the parties.

Emergency Call Service Provider (ECSP): Service Provider that acts as a mediator between the Voice Service Providers and the Public Safety Answering Point Service Providers

Publicly Available Telephone Service (PATS): A service made available to the public for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan.

https://www.ofcomorg.uk/__data/assets/pdf_file/0023/106394/Annex-14-Revised-clean-conditions.pdf

Note - Refer to the General Conditions at www.ofcom.org.uk for the definition of PATS.

Secure: The term 'Secure' means that the information can be passed without fear of interception or malicious manipulation.

NOTE 2: Secure may include the use of encryption.

Private Network: A network that specifically determines the addressing plan and address assignments within that network. (As Defined in IETF RFC 1918 [1])

VSP Aggregation Provider (VAP): provider that a VSP or group of VSPs can use to support call routeing to remote ECSPs and for the generation of related call data records

Voice Service Provider (VSP): For the purposes of this document VSP is defined as an entity that provides PATS

PSAP Service Provider: Service Provider that provides connectivity to Public Safety Answering Points (PSAPs) and directs emergency calls from the ECSP to the PSAP

3.2 Abbreviations

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

3GPP	3rd Generation Partnership Project
4G	4th Generation Mobile
AAA	Authentication, Authorization and Accounting
ADSL	Asymmetric Digital Subscriber Line
AML	Advanced Mobile Location
ANP	Access Network Point
ASN	Autonomous System Number
ATM	Asynchronous Transfer Mode

BAP	Backhaul Aggregation Provider
BRAS	Broadband Remote Access Server
CID	Cell ID
CLI	Calling Line Identity
CP	Communications Provider
CRM	Customer Relationship Management
CSCF	Call Session Control Function
DNS	Domain Name System
DSLAM	Digital Subscriber Line Access Multiplexer
EA	Emergency Authority
ECSP	Emergency Call Service Provider
EECC	EU Electronic Communications Code
EISEC	Enhanced Information Service for Emergency Calls
ESCP	Emergency Call Service Provider
ESO	European Standards Organisations
ESRP	Emergency Service Routeing Proxy
ETSI	European Telecommunications Standards Institute
EU	European Union
GC	General Conditions
GMLC	Gateway Mobile Location Centre
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Interconnect Service Provider
ISUP	ISDN User Part
L2TP	Layer 2 Transport Protocol
LAN	Local Area Network
LLP	Local Loop Provider
LRF	Location Retrieval Function
LS	Location Server (ETSI Definition of LIS)
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extensions
PAID	P-Asserted-Identity
PATS	Publicly Available Telephone Service
PIDF-LO	Presence Information Data Format Location Object
POTS	Plain Ordinary Telephone Service
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PPPoA	Point to Point Protocol over ATM
PSAP	Public Safety Answering Point
PSP	PSAP Service Provider
PSTN	Public Switched Telephone Network

RADIUS	Remote Authentication Dial-In User Service
RDF	Routeing Determination Function
RFC	Request For Comment
SBC	Session Border Controller
SID	System Identification Code
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SOS URN	Emergency URN
TDM	Time Division Multiplexing
TG	NICC EmLoc Task Group
UE	User Equipment
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VAE	VSP Aggregating Entity
VAP	VSP Aggregation Provider
VSP	Voice Service Provider

4 Overview of the ETSI ES 203 178 architecture in a UK context

4.1 High level functional architecture

The high-level functional architecture is taken from Annex C of ES 203 178, as this is the most likely, practical deployment for the UK.

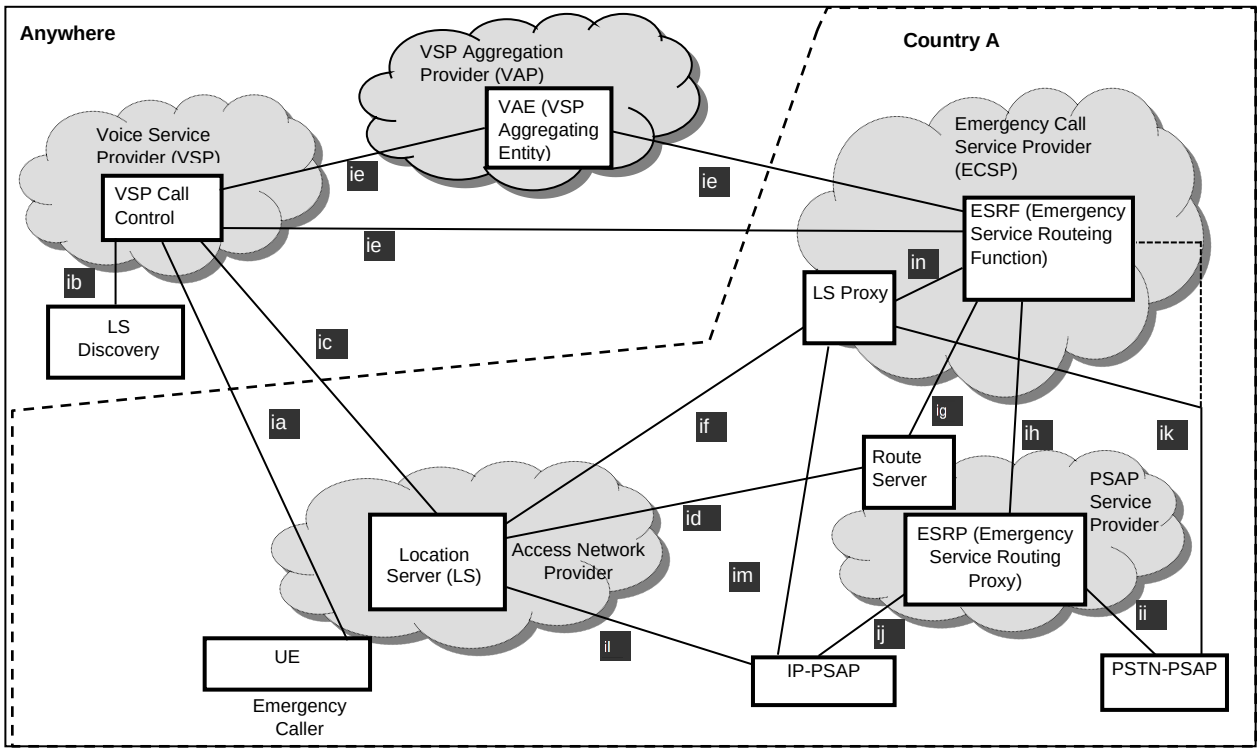


Figure 1: ETSI ES 203 178 generalised architecture with all interfaces and entities shown

The functional architecture to support emergency calling requirements on emergency caller location determination and transport, identifies a number of key Communication Provider (CP) roles that would need to function at a high level in the UK as follows:

- Access network provider (ANP);
  ANP in the UK : following the definition from ETSI, the ANP is the “Service Provider that provides physical and Internet Protocol (IP) connectivity to a User Equipment (UE) via a fixed or mobile access.” For the UK this applies to Internet Service Providers (ISPs) that provide the IP access to UE at a specific location, some of which will also provide underlying physical access through copper, cable and fibre access networks, or through wireless access using Wi-Fi or 3GPP standards, while other ISPs will require use of separate organisations' physical access networks(the interfaces between these organisations outside the scope of the ETSI approach). In the UK profile of the architecture we identify the ANP as an Internet Service Provider (ISP).

- Voice Service Provider (VSP);
  VSPs in the UK, in line with the ETSI definition, are a “specific type of application Service Provider that provides voice related services and optionally text and video-related services, on IP”. In the UK, Voice Service Provider (VSP) may also refer to cloud based Service Providers. The Voice Service Provider (in this context could also be referred to as the VoIP

Service Provider) has a direct relationship with the calling party/end user as its customer and has an (authenticated) signalling interface to its customers. This interface is most likely to be Session Initiation Protocol (SIP). However a number of other protocols are possible (IAX2, Skinny, UniStim, H.323 and Media Gateway Control Protocol [MGCP]). This interface is used for call establishment (either from the customer, or from the VSP softswitch).

SIP allows a number of different types of identities to be used in both calling other users, and in identifying the sending entity. Primarily these are sip Uniform Resource Identifiers (URIs) and tel URIs, but others also exist. Thus ETSI ES 203 178 architecture places no constraint on any of these.

In accordance with ETSI ES 203 178 , the VSP will use the emergency URI in the Request URI to place the emergency call.

In emergency calls made by Plain Ordinary Telephone Service (POTS) in the UK, the calling line identity, as provided by the local network provider, has two separate functions:

I. to enable a location to be determined based on the location registered for that calling line identity.

II. to provide an identity to enable the emergency service to return the call.

The ETSI ES 203 178 architecture does not specify any requirements in regard to the type of URIs used by the VSP, except in regard to the Request-URI.

Because in the ETSI ES 203 178 architecture, location is provided by separate means in the architecture, any calling line identity provided by the VSP in the From: or P-Asserted-Identity header fields is not essential to the support of (I) above. It is possible that emergency Service Providers might use it for additional validity checking of the emergency call itself.

While (II) above may be useful to emergency Service Providers, there is no mandatory requirement in the UK for response calls to be so enabled, or therefore for VSPs to provide such an identity.

NOTE 3: Not all VSPs have interconnect arrangements with other VSPs or with the Public Switched Telephone Network (PSTN), so that there may be an aggregation VSP that collects calls, including the emergency calls, from various VSPs – see the VSP bullet above. A VSP Aggregation Provider(VAP) has the necessary interconnects to reach the Emergency Call Service Provider (ECSP) and PSAP.

NOTE 4: In addition to providing an interface to the ECSP and PSAP, the VAP may also assist with the conveyance of emergency calling through the suballocation of E.164 numbers or other capabilities that facilitate call back or caller identification.

- Emergency Call Service Provider (ECSP);
  ECSP is the Service Provider that acts as a mediator between the Voice Service Providers and the Public Safety Answering Point Service Providers.

- PSAP Service Provider (PSP)
  PSP is the Service Provider that provides connectivity to Public Safety Answering Points (PSAPs) and directs emergency calls from the ECSP to the PSAP. In the UK, the Public Safety Answering Point (PSAP) SP is also the ECSP network which will directly host the new Stage 1 PSAP platform.

NOTE 5: The ANP, ECSP and PSP are in the same regulatory domain. The VSP can be inside or outside this domain.

NOTE 6: On the basis of the European Regulatory Framework the emergency services provision inside a country is in charge of its administration; so the term "regulatory domain" typically coincides with a single country. In some cases a specific agreement can be defined between neighbouring countries to correctly manage the provision of the emergency services, for example in areas close to the common border.

- VSP Aggregation Provider (VAP)
  A VAP is a provider that a VSP, or group of VSPs, can use to support call routeing to remote ECSPs and for the generation of related call data records. There are many UK VSPs that do not connect directly to ECSP, but through another VSP (which will then, by definition, assume the VAP role).
  For the full scope of the ETSI approach, supporting non-UK VSPs, we expect there to be VAPs in most countries that can route calls between them, allowing cross-border European routeing of calls for VSPs.

- User Equipment (UE)
  The M493 architecture defined in ES 203 178 and further specified in ES 203 283 makes no assumptions about the UE. It does not require User Equipment (UE) to be able to initiate emergency calls. However, it does require UEs to be able to recognise emergency calls and indicate such calls as emergency calls to its associated VSP.

4.2 Architecture interfaces

Interface Definitions

Interface	'a' end	'b' end	Description
ia	User Equipment	VSP call control	Communication provides sufficient information to the VSP, to indicate that the User Equipment is making an emergency call, and conveys sufficient information to enable the VSP call control to invoke location server discovery.
ib	VSP call control	Location Server Discovery Functional Entity	The VSP call control provides sufficient information to allow the Location Server discovery functional element to provide either the ANP domain name or the URI of the Location Server serving this domain.
ic	VSP call control	Location Server	The VSP call control includes sufficient information to allow the Location Server to identify the User Equipment in the access network. The Location Server returns location information and may return the address of the ESRF assigned to service the call. The ESRF

			address shall be returned by the Location Server when the VSP requests routeing information.
id	Location Server	Route Server	The Location Server provides a location value to the route server and the route server responds with the address of the ESRF associated with the proffered location. The Location Server's primary function is to determine the location of devices attached to the access network and make appropriate information available to functional entities involved in the emergency call. To determine the ECSP and ESRF responsible for serving an emergency call made at a certain location is the responsibility of the route server. In order for the Location Server (LS) to provide ECSP address information the LS acquires it from the route server. This can be done at provisioning time or in real-time depending on implementations. The Location Server may be provisioned with the address of the route server or it may discover the address of the route server using mechanisms such as those described in IETF RFC 5222 [8]. NOTE 7: This interface is used when an ESRF URI is requested by VSP and no such URI is configured on LS.
ie	VSP call control	Serving ESRF in the ECSP network	The VSP call control adds the location information and directs the call to the ESRF address.
if	LS Proxy	Location Server	The ESRF or PSAP uses the location information to acquire the User Equipment location value from the Location Server via the LS Proxy.
ig	Serving ESRF	Route Server	The ESRF provides a location value to the route server. The route server responds with the address of the Emergency Service Routeing Proxy (ESRP) in the PSP network or the destination PSAP address.

ih	Serving ESRF in the ECSP network	ESRP in the PSP network	The serving ESRF in the ECSP network includes with the call, location information (reference identifier and/or a location value) in the signalling to the ESRF in the PSP network.
ii	ESRP in the PSP network	PSTN-based PSAP	The ESRP provides sufficient information with the call to allow the PSTN-based PSAP to identify the serving ESRF and the call in progress through that ESRF in the ECSP network. Information transported across this interface is limited by the capabilities of the legacy PSTN protocol. If the protocols do not support transport of location information, the location information can be retrieved through ik.
ij	ESRP in the PSP network	IP-based PSAP	The ESRP provides with the call, location information (reference and/or location value).
ik	PSTN-based PSAP	LS Proxy or the ESRF	
il	IP-based PSAP	Location Server	The IP-based PSAP uses the location reference to request information from the Location Server. The Location Server responds with the current location of the caller in the form of a location value.
im	IP-based PSAP	LS Proxy	The IP-based PSAP uses the location reference to request information from the Location Server.
in	ESRF	LS Proxy in the ECSP	The ESRF sends a location request to acquire the caller's location. The ESRF receives one or more location values from the LS proxy. In addition the in interface can be used to exchange call context data.

4.2.1 Protocols for the interfaces

The following defines where possible protocols to be used across each of the interfaces highlighted in section 4.1 or where decisions will need to be made as part of the ETSI ES 203 178 UK specification.

4.2.1.1 Interface - ia

The protocol used on the interface ia is determined by the VSP only

4.2.1.2 Interface - ib

The ib interface permits the interactions between the VSP call control and the LS discovery functional entity. The VSP call control uses the public IP address of the UE to interrogate the LS discovery functional entity in order to obtain the address of the LS serving the access network to which the UE is attached. Since this function is expected to be accessible to any VSP anywhere, this is an open interface. If a pre-established relationship exists between the ANP and the VSP then Domain Name System (DNS) may be used for the LS discovery function.

The first part of this discovery process in IETF RFC 7216 [17] yields the domain name of the serving access network. If the VSP knows the address of the LS for the serving ANP, then no further discovery is required, otherwise an additional DNS query may be used. If no pre-established relationship exists between the VSP and the ANP then the LS Discovery function shall use the Domain Name Service (DNS).

The VSP requires the Uniform Resource Locator (URL) of the LS serving the access network to which the UE is attached. The URL shall be a HELD URI (IETF RFC 5985[11]). The URL discovery shall perform the U-NAPTR procedures defined in sections 2 and 4 of IETF RFC 5986[12] with the following variations:

- the domain shall be known as a result of having performed the steps in IETF RFC 7216 [17]; and
- the device-based interfaces are irrelevant as discovery is performed by a third-party, i.e. the VSP; and
- the process stops once the URL for the LS has been resolved based on the steps in section 4 of IETF RFC 5986[12].

4.2.1.3 Interface - ic

Depending on the pre-established relationship the VSP call control can use interface ic to request location and routeing information from the Location Server. The protocol of choice will need to be established with further work and standardised accordingly. The use of HELD or Diameter are potential candidates for this interface.

4.2.1.4 Interface - id

Interface id can be used by the Location Server to acquire routeing information from the route server. Interface id can be an intra-operator or an inter-operator interface. Often, the routeing information can be determined at the time that location information is provisioned into the LS. Other implementations may allow the LS to be provisioned with location information, and then require the LS to "validate" the provisioned location information against the route server, to ensure that the location information is in the correct format.

This interface has not been standardised and will require standardisation within the UK. It is worth noting that this interface is not standardised within the ETSI documentation, being marked as a matter for regional standardisation.

4.2.1.5 Interface - ie

The interface ie connects the VSP call control and the ESRF in the ECSP network. In the case where a VSP is connected via a VAP, the interface ie defines the interactions between the VSP

call control and the VSP Aggregating Entity (VAE) and between the VAE and the ESRF. This is an open interface, all VSPs, VAPs and ECSPs shall provide this interface. Entities at each end of the interface shall support the following specifications as appropriate for either proxy or UA usage:

- IETF RFC 3261 [4]
- IETF RFC 4320 [7]
- IETF RFC 5393 [9]
- IETF RFC 5954 [10]
- IETF RFC 6442 [14]
- IETF RFC 4566 [15]
- IETF RFC 3264 [5]

The VSP call control and the VAE shall use the Session Initiation Protocol (SIP) towards the ESRF.

Where interworking between SIP and ISDN User Part (ISUP) occurs, there is a possibility that some location information will not be passed.

4.2.1.6 Interface - if

The if interface supports the interactions between the LS and the LS Proxy. If no LS proxy acts between the ESRF and the LS, the if interface coincides with the in interface.

The ETSI specification provide two options - the first being the use of HELD; the second being the use of Open Mobile Alliance (OMA) Mobile Location Protocol (MLP) Version 3.5. This interface will need to be defined in UK specific Specifications for the Operation of ETSI ES 203 178 in the UK.

4.2.1.7 Interface - ig

Interface ig can be used by the ESRF to acquire routeing information from the route server. Interface ig can be an intra-operator or an inter-operator interface. Often, the routeing information can be determined at the time that location information is provisioned into the ESRF.

Note that this interface has not been standardised and would require standardisation within the UK. It is worth noting that this interface is not standardised within the ETSI documentation being marked as a matter for regional standardisation.

4.2.1.8 Interface - ih

The interface ih is located between the ESRF and the ESRP. According to ETSI ES 203 178 , this is an internal interface and country Specific. If the interface ih is IP-based and SIP is used across this interface. Note that the definition of the protocol of use across this interface will be subject to standardisation within the UK.

4.2.1.9 Interface - ii

The interface ii is located between the ESRP and the PSTN-PSAP. According to ETSI ES 203 178, this is an internal interface and country specific. Note that the definition of the protocol of use across this interface will be subject to standardisation within the UK.

4.2.1.10 Interface - ij

The interface ij is located between the ESRP and the IP-PSAP. According to ETSI ES 203 178, this is an internal interface and country specific. If the interface ij is IP-based and SIP is used across this interface. Note that the definition of the protocol of use across this interface will be subject to standardisation within the UK.

4.2.1.11 Interface - ik

The interface ik is located between the PSTN-PSAP and the ESRF or between the PSTN-PSAP and the LS-Proxy. According to ETSI ES 203 178, this is an internal interface and country specific. Note that the definition of the protocol of use across this interface will be subject to standardisation within the UK.

4.2.1.12 Interface - il

The interface il is located between the IP-PSAP and the LS. According to ETSI ES 203 178, this is an internal interface and country specific. Note that the definition of the protocol of use across this interface will be subject to standardisation within the UK.

4.2.1.13 Interface - im

The interface im is located between the IP-PSAP and the LS-Proxy. According to ETSI ES 203 178, this is an internal interface and country specific. Note that the definition of the protocol of use across this interface will be subject to standardisation within the UK.

4.2.1.14 Interface - in

The in interface is used between the ESRF and the LS-Proxy within the ECSP domain to support the implementation option where these two functional entities are not co-located. The ESRF shall provide either a location reference or a location identifier to receive a location value from the LS-Proxy. Furthermore, for example under the following conditions, the ESRF may send a create context message to the LS-Proxy:

- no mechanism to deliver a location information to a PSTN-PSAP via interface ii;
- PSTN-PSAP uses pull mode via interface ik for retrieval of the location value;
- PSTN-PSAP does not have a location reference or a location identifier, and therefore uses the network-based caller identity as look-up key when using pull mode;
- VSP delivers network-based caller identity in a form that is not compatible to PSTN (e.g.: sip:bob@example.com).

In this case, the ESRF can require a binding of the network-based caller identity and a location reference (created by the LS-Proxy) via interface in. The LS-Proxy sends a response to the ESRF including a location reference that can be delivered to the PSTN-PSAP. Upon the receipt of the location reference the PSTN-PSAP may require location dereferencing via interface ik. For this procedure the LS-Proxy is using the network-based caller id as look-up key for dereferencing via interface if towards the LS. On completion of the emergency call, the ESRF requires the deletion of the call context. If no LS-Proxy is implemented the interface in coincides with interface if.

4.3 VSP Aggregation Entity

The function of the VAE is to aggregate the emergency calls for a number of VSPs and deliver these calls to the ESRF (Emergency Service Routeing Function) in the relevant country.

The requirement in the UK, is for the ESRF to only have connections from a small number of VAEs so limiting the number of inter-connections for the Emergency Call Service Provider (ESCP). This enables there to be a trust relationship between the VAP (VSP Aggregation Provider) and the

ESCP (Emergency Call Service Provider). This trust relationship also facilitates cost recovery for the UK PSAP.

NOTE 8 : To minimise the complexity of the LS discovery process for a UK VSP the UK is considering that a VSP Aggregation Provider could also extend its role, as defined in ETSI ES 203 178 [1], to conduct the LS discovery process (including interface ib) as well as to provide the interface ic access to the LS as a proxy for UK VSPs. If adopted, UK VSPs would not need to communicate directly with LSs and LSs will need only to communicate with a limited number of VAE proxies (on behalf of UK VSPs). This would require additional UK specific development and standardisation.

4.4 Architecture functional elements

4.4.1 ISP functional entities

4.4.1.1 Location Server (LS)

The LS provides functions which are used to retrieve location information and optionally IP routeing information. It may provide a location value, location identifier or location reference, with only location reference being used in the UK.

An LS will need to be managed by, or on behalf of, the ISP, which associates IP addresses that are in use and/or allocated by the ISP to its customers/end-users to physical addresses or locations. The Location Server must return a location reference identifier to any external source on receipt of an IP address currently allocated to, and being used by a customer of, the ISP. The Location Server must also, when interrogated by the ECSP using the location reference, return the actual address associated with the IP address. The connection between the ECSP and the Location Server will be via a trusted and secure communication channels.

4.4.1.2 Location Server discovery function

The LS discovery function provides functions to derive the address of the correct Location Server within the ANP domain. It also provides the URI of the LS or the ANP domain name to the VSP.

LS Discovery is a function or capability whereby an IP address is resolved to the owning ISP that has been allocated the IP address and provides the URI (or internet address) of the ISP's Location Server so that a request for a location reference can be made. The ETSI standard does not identify which organisation(s) would be responsible for hosting and managing such a facility and for ensuring that the data held remains current.

NOTE 9: (to be further explored by EmLoc Task Group) the process in ES 203 283 requires the VSP to use the DNS service to discover LS URI, and the Autonomous System Number (ASN)/Domain Name should be enough to determine LS for large UK ISPs. That being so do we actually need any organisation to host an LS Discovery Server – is it more a question of ISPs' normally used DNS servers being correctly populated by the ISP?

4.4.2 User Equipment (UE)

The UE is connected directly to a public network access point or within a private network connected to a public network access point. In the context of emergency service the UE allows a user to access the emergency call service delivered by the VSP.

4.4.3 VSP functional entities

4.4.3.1 VSP Call Control

The VSP provides a call control function that is the first point of contact for call signalling coming from the UE.

On identifying a call as an emergency call the VSP determines the public IP address of the UE and acquires from the LS Discovery function the LS URI, and then retrieves the ESRF IP routeing information and UE's network-provided location information from the LS.

The VSP call control directs the call to the ESRF. The UE’s location information is included in the call setup message towards the ESRF.

4.4.4 VAP functional entities

4.4.4.1 VSP Aggregating Entity (VAE)

A VSP aggregating entity provides a call control transit function that resides inside the VSP aggregation provider network and may be used by a VSP or group of VSPs to manage trust relationships with, and routeing to, ECSPs or other VAEs that may reside in other areas or countries. The VAE may also generate call data records for calls using its services.

It is recommended in the UK that there is an option for the VSP Aggregation Provider(s) to extend its role to provide the interface ic access to the LS as a proxy for UK VSPs. This requires the VSP to send the UE's IP address and Port information to the VAE over the ie interface (which is one of the elements allowed on ie). Then UK LSs will only communicate with VAE proxies, and VSPs do not have to communicate directly with LSs. Overseas VSPs could also benefit from this; to do so they would have to be aware that the caller was in the UK, and that the VAE would be available.

Conversely, UK VSPs with overseas users may not have the option of a VAE in the remote country so may have to implement interface ic for these overseas cases.

4.4.5 ECSP functional entities

The ECSP receives calls from a VSP or VAP and directs them to the PSAP, taking into account location information.

There will be at least one ECSP per country. There could be more than one ECSP in the UK, e.g. each mobile network could operate as its own ECSP . Each ECSP will have to provide a Location Server Proxy unless a shared, or national level, LS proxy is introduced.

In the UK we can identify the ECSP with the ECSP network as UK VSPs will use this interconnect capability to route calls to the IP-PSAP.

4.4.5.1 Emergency Service Routeing Function (ESRF)

The ESRF is a routeing proxy hosting emergency-specific logic that resides within the ECSP domain. It is expected to interact with the LS Proxy or LS to obtain location information from the ANP, unless that was provided with the call, and uses it to determine the correct PSAP address to which to direct the emergency call. In the UK there is currently only one stage 1 PSAP, so the ESRP will always forward calls to this PSAP, and will need to be part of the ECSP provision by the ECSP network.

The ESRF can set the network-provided caller identity to a locally generated value that maps to the received value:-

- If no meaningful value was received from the VSP or VAP.
- If the call is to be routed to the PSTN and the received value cannot be conveyed using legacy PSTN signalling protocols.

Legacy PSTN Signalling protocols are expected to be used in the UK alongside SIP signalling for the next 5 years.

The ESRF may request the LS Proxy to create a call context and delete this call context once the call is completed. However, this functionality is not expected to be needed since, for calls originated by a UK VSP, or which are interconnected to the UK ECSP, the originating VSP must ensure that emergency calls be accompanied by a caller identity. This caller identity must be;

(a) carried in a P-Asserted-Identity header field (as specified by RFC 3325 [6]) inserted by the originating VSP (as mandated in ND 1035[19]);

(b) a valid network number (see ND 1016[20]) - it is recognised that this number may not be answerable if called.

The From header field must also be supported as normal (its value may be inserted by the end-user's equipment) and will be treated as a presentation number (see ND 1016 [20]).

NOTE 10: The From header field received by the VSP from the UE may not always carry a valid value. In this case the VSP may anonymise the From header field, or replace it with a known valid value.

4.4.5.2 LS Proxy

The LS Proxy acts as a proxy between the Location Server and an ESRF or a PSAP. The LS proxy shall be able to create and delete call context data upon request from the ESRF. Upon receipt of a location request from the ESRF or a PSAP, the LS Proxy responds to the request with one or more location values which it may have locally stored or may obtain from the LS.

The functionality of the LS Proxy in the UK is not expected to be needed as it should not need to create and delete call context data upon receipt of a request from the ESRF (as calls are expected to arrive with a valid P-Asserted-Identity [PAID] and From number). In the UK the location request can be made direct from the Stage 1 PSAP to the LS.

4.4.6 PSAP Service Provider functional entities

4.4.6.1 Emergency Service Routeing Proxy (ESRP)

The ESRP is a routeing proxy, that resides in the PSAP Service Provider, which forwards emergency calls towards their final destination. The ESRP can be (for example) a PSTN transit or local exchange, a SIP proxy or a SIP back-to-back user agent.

Upon the receipt of an emergency call from an ECSP, the ESRP acquires all information necessary for the selection of the correct Stage 2 PSAP to route the emergency call to, and forwards the emergency call towards this selected PSAP.

In the UK context the PSAP Service Provider is the Service Provider that provides connectivity to Public Safety Answering Points (PSAPs) and directs emergency calls from the ECSP to the PSAP. In the UK, the PSAP SP is also the UK ECSP network which will directly host the new IP based Stage 1 PSAP platform.

4.4.6.2 Route Server

A route server is a functional element which maps a location value into an address URI to route an emergency call toward the correct PSAP.

The Route Server is not needed in the UK as there is currently only one PSAP.

4.4.6.3 IP-PSAP

The IP-PSAP is a Public Service Answering Point connected to the ESRP using IP technologies. In the context of emergency calls made in the UK, the Stage 1 IP-PSAP would be expected to receive location information via interface il, with no need to use an LS Proxy, and to also allow for receiving location information through interface ij as VSPs and ECSP gradually allow an end-to-end path for location to be conveyed with SIP.

4.4.6.4 PSTN-PSAP

The PSTN-PSAP is a Public Service Answering Point connected to the ESRP using PSTN technologies (e.g. Integrated Services Digital Network [ISDN] or POTS). We are expecting the Stage 1 PSAP to have moved to being an IP PSAP so this is not considered further.

5 Potential implementation options of the ETSI ES 203 178 architecture in the UK

5.1 Access Network Providers and Internet Service Providers

5.1.1 General

To enable emergency call location identification solution described in this document to work, all ANPs would need to be mandated to provide a mapping between physical location and IP address.

The ANP in ETSI ES 203 178 and ETSI 203 283 represents an ISP providing IP access (after authentication) and includes the role of the Physical Access Provider (local loop provider using copper, cable or fibre, Wi-Fi, femto/pico/macro cells)

The ANP is expected to populate its own records on the LS Discovery Server.

The ANP needs to provide a Location Server (LS) that identifies the physical access point where the IP address is currently allocated plus real time interfaces to the LS for ECSP/PSAP.

The ANP needs to ensure confidentiality of records stored in the LS

It is anticipated that the ANP's Location Server will always return a Location Reference (not Location or Location identifier).

A number of access configuration and user authentication mechanisms exist in the UK as described below and these are used to allow the mapping of user location to IP Address to be recorded in the LS.

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

Type (ii) : A separate Backhaul Aggregation Provider (BAP) and Local Loop Provider (LLP) associated with the ISP provide a virtual access path from the end user device and a handover point and may provide limited authentication, for example authentication that the line has valid broadband access. In this case the ISP is not operating the access network.

In the type (ii) case there are specific identifiers conveyed at the handover : these are referred to as location tokens (connection endpoint references) which may be a Layer 2 Transport Protocol (L2TP) tunnel ID, Agent Circuit ID/Derived Line ID, Service ID (SID) or an IP address.

The term Access Network Providers (ANPs) is used in NICC to refer to the BAP and LLP arrangement providing an access service to the ISP, that owns the IP address being used.

Some ANPs introduce a Service ID (SID), based on an Agent Circuit ID created by an intermediate agent at a Digital Subscriber Line Access Multiplexer (DSLAM) for Point to Point Protocol over Ethernet (PPPoE) termination, or a derived Line ID (based on combination of Broadband Remote Access Server (BRAS) id, ATM port id, Virtual Path and Circuit information that relates to a DSLAM terminated copper access line) for Point to Point Protocol over ATM (PPPoA) termination.

As stated above, all CPs that provide IP access to end users (i.e. all ISPs) will have to manage an LS, relating IP address to underlying physical access point. In some cases the BAP will also have to provide an LS, for example see Section 5.1.2.

The ISP is expected to populate its Location Server URI within the Discovery Server. The implementation design of both Location Server and Discovery Server will require further UK specific design and standardisation in order to meet the requirements clause 5.4.5.1 of ES 203 178.

NOTE 11: The management of location information requests to an ISP's LS by VSPs presents challenges to an ISP as there are many VSPs (not simply those in the UK) that may make such requests and the ISP needs to protect itself, for example against malicious attacks.

5.1.2 ISP using ADSL

For Wireline, ISP LS relies on information from a Remote Authentication Dial-In User Service (RADIUS) server collected at the connection time of the session, to record the IP address and its associated connection endpoint reference. The RADIUS Accounting request (received at connection time by the ISP) should contain a connection endpoint reference (e.g. SID) which uniquely identifies the physical circuit and thereby the location of the user.

An informative PPPoE example is shown below in Figure 2 where the ISP delegates IP address allocation to the BAP's BRAS, which is one widely used configuration in the UK.

If the connection endpoint reference is non-circuit specific, such as L2TP tunnel identifier, the ISP LS may need to forward the request on to the BAPs LS to resolve.

Where the BAP is a separate organisation, the ISP LS must manage the "real-time" requests and if necessary to each access provider (BAP+LLP).

By separate arrangement at the OSS/ Customer Relationship Management (CRM) customer management layer, the ISP will require a regular feed of connection endpoint 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. Upon the receipt of a location information request via interface ic the LS:

1) may require authentication and authorisation of the requesting entity before returning a location reference;

NOTE 12: Authentication of the requesting entity may be explicit or implicit depending on network configuration and operator agreements.

2) should only transfer data using a secure (free from tampering) communications channel;

3) if not locally available, shall retrieve from other entities in the ANP's domain the location information of the physical access belonging to the calling user; and

4) shall provide the appropriate location information to the requesting entity depending on the level of trust between the requesting entity and the ISP.

If the location information request comes from a VSP call control and includes a routeing request, the LS shall:

5) if an ESRF URI is not locally configured for the concerned location (ESRF should be known for the UK), retrieve routeing information from a route server; and

6) provide the relevant ESRF URI to the VSP call control.

5.1.3 Example of an ISP using Cable

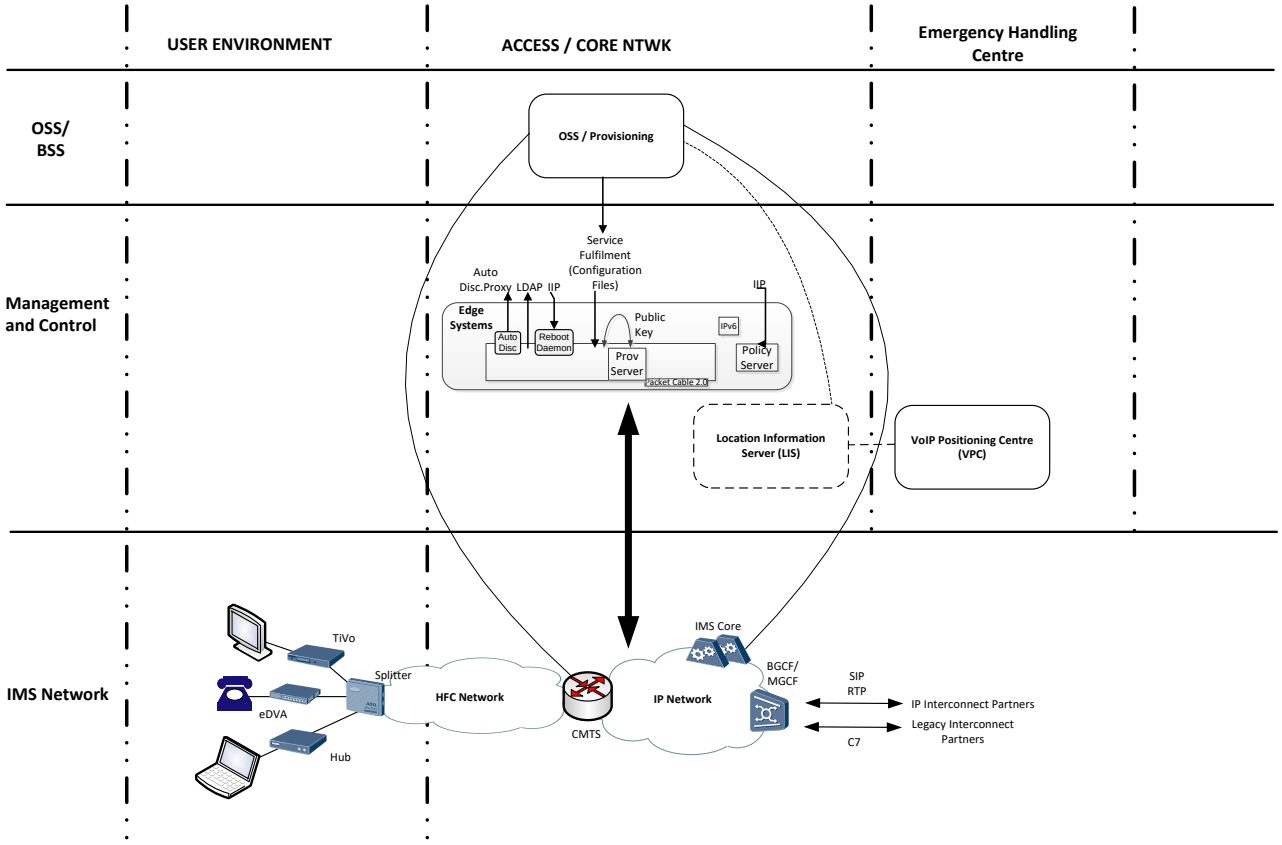


Figure 2 - Example of an ISP using Cable

Figure 2 describes the example of an ISP using Cable, either based on Hybrid Fibre Coax or Fibre To The Premise, that provides telephony service by means of an IP Multimedia Subsystem (IMS) using the CableLabs PacketCable 2.0 standards; which are deltas to the 3GPP standards.

For this example, under normal operating conditions the A-SBC provides the P-CSCF (CSCF) plus E-CSCF, which, for emergency calls to 999/112, routes these directly to the MGCF. The MGCF then onward routes these calls with the B Number suffixed with 'ii' digits to the PSAP1 along with valid unique callable A Number to allow the ESDB to correlate to the civic address of the A Number; which can be trusted as the Embedded Digital Voice Adaptor (eDVA) in the end user premise is a static non-nomadic device.

Whilst it should be possible to extend this to align to the ETSI 203 178 architecture, this is considered to be challenging because -

- the need for the ISP to populate its entries directly on the LS Discovery Server,
- potential objection of the ISP Data Protection Office to this,
- no obvious function to track IPv6 address of endpoints in the PC2.0 architecture as implemented.

5.1.4 ISP using mobile IMS (3GPP) with 3GPP VSP

Figure 3 shows how UK 3GPP mobile networks, using IMS, should be connected to the ETSI ES 203 178 architecture for the handling of emergency calls.

This example covers inbound roamers to the UK with the user attached to the visited IMS network (3GPP) using a 3GPP terminal (UE) that provides voice and data access authorised by its home network (also 3GPP) so that visited network can manage both.

These callers will use the P-CSCF and E-CSCF in UK visited mobile network.

Note 13: The outbound roamers are out of scope. These callers will use the P-CSCF and E-CSCF in the mobile network they are visiting.

The Mobile Access Network Provider may need a Location Server to give additional locational information to the PSAP. Location is not required for routeing of emergency calls in the UK as the UK has only one PSAP.

The new interfaces required for a mobile access provider are:

- Location Server (LS) to LS Proxy (if)
- Location Server (LS) to IP-PSAP (il)

The IMS Architecture, as defined by 3GPP TS 23.167, V11.11.0, Section 5 is:

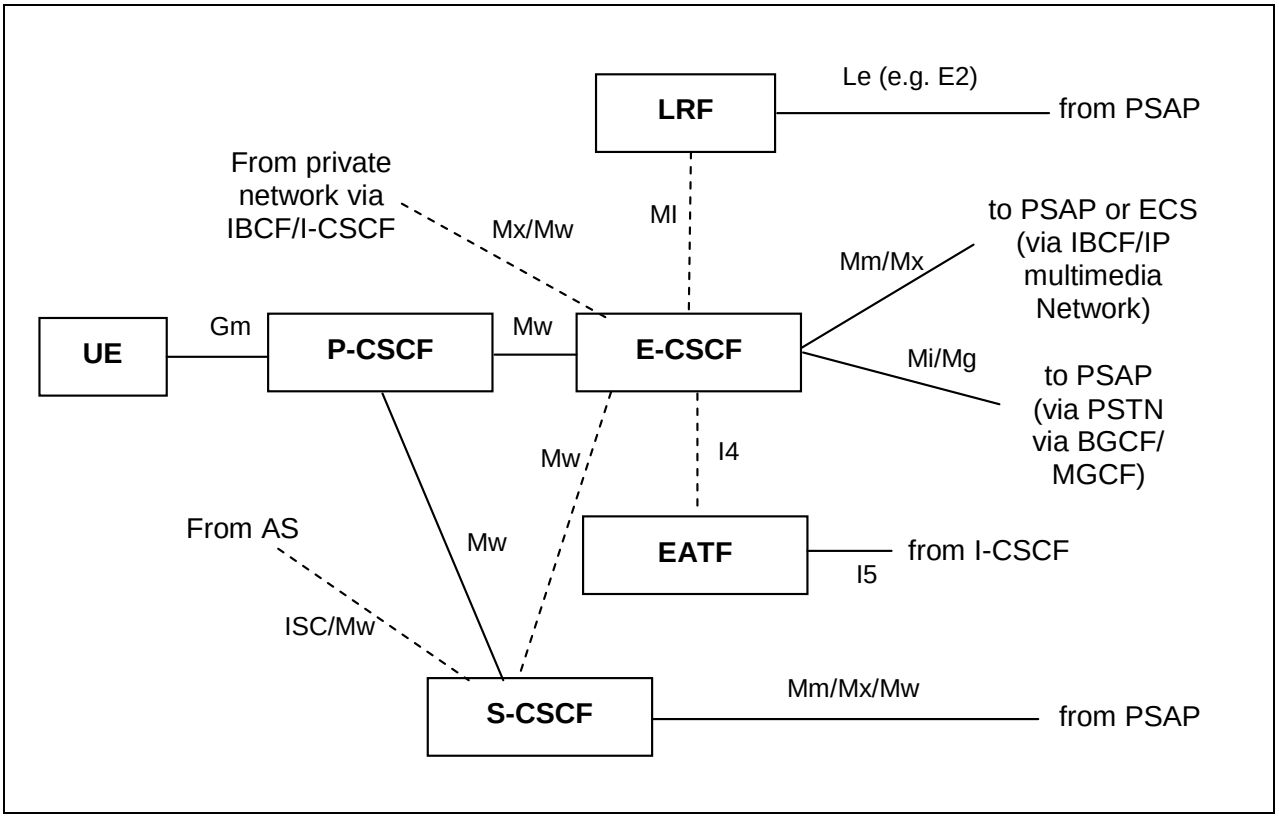


Figure 3: 3GPP Architecture

The resulting merged architecture for the UK is:

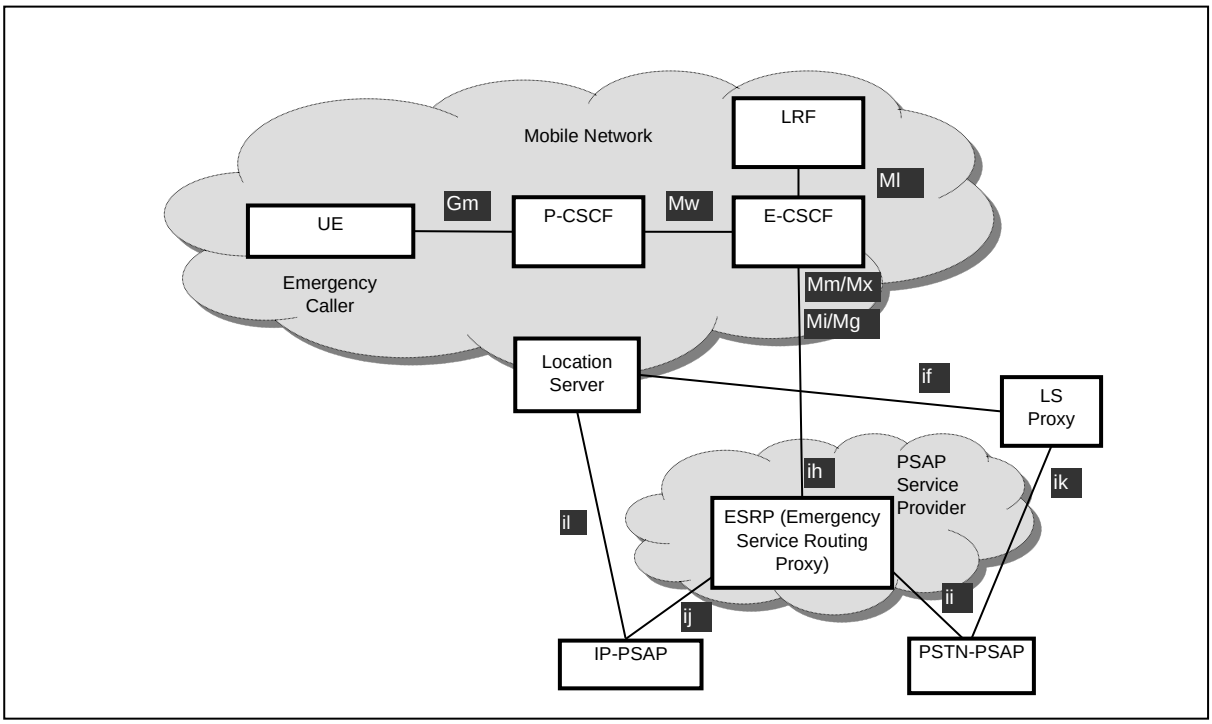


Figure 4: ISP using mobile IMS (3GPP) with 3GPP VSP
NOTE 13: The non-used elements have been removed for the diagram for clarity.

For this example, the emergency call flow is:

1 The caller uses the User Equipment (UE) to make an emergency call. The SIP INVITE request may contain Global Positioning System (GPS) location information recorded by the UE.

2 The Proxy CSCF (P-CSCF) recognises the call as an emergency call and routes the call to the Emergency CSCF (E-CSCF).

3 The E-CSCF routes the call to the Location Retrieval Function (LRF). The LRF also contains the Routeing Determination Function (RDF). The RDF sends a redirect to the E-CSCF with the new number that routes to the PSAP.

4 The E-CSCF routes the call onto the Emergency Service Routeing Proxy (ESRP).

Question for further study: Should the E- CSCF route to ESCP rather than straight to the ESRP??

5 The ESRP routes the call onto the PSAP; either an IP-PSAP or PSTN-PSAP.

6 Additional location information can be retrieved by the PSAP from the Location Server (LS) directly or via the LS Proxy

Question for further study: Which entity should operate the LS Proxy??

Question for further study: Will the LS have location information for roamers as does not normally do so now ??

5.1.4 Mobile Data Access Network Provider with non 3GPP VSP

This case is when the mobile network (3GPP) is providing a mobile data service to a customer. This customer is using the data service to provide a localised Wi-Fi service (Wi-Fi Hot Spot). Then another customer is using that same Wi-Fi service to make a voice emergency call.

The requirement is to provide the location of the caller.

It is the mobile network that has a location for the Wi-Fi device. The VSP needs to ask for location from the mobile network.

This requires an interface between the VSP (ETSI specified) and the mobile network (3GPP specified). This interface has not been defined.

See section 5.2.2 of ETSI ES 203 283 for the ib interface. See section 5.3.1.4 of ETSI ES 203 283 for the ic interface.

Further development will be required by ETSI and 3GPP to support provision of location for this call case.

5.1.5 Mobile customer (3GPP VSP) roaming on Wi-Fi

This case is where a mobile IMS customer (3GPP) has roamed onto a ETSI defined Wi-Fi network. The roamed customer then makes an emergency call. The requirement is for the mobile network to provide a location for the calling customer.

As the customer roams around the Wi-Fi networks the Authentication, Authorization and Accounting (AAA) in the mobile network is updated with the current location. It is this location that is provided at the time of the emergency call.

This area will require further design consideration and UK specific standardisation.

5.2 VoIP Service Providers

5.2.1 Call routeing

VoIP Service Providers (VSP) will need to find caller location information to enable routeing of calls and to provide location to emergency services (network derived location and, where, provided device locations). The VSP will also need to: -

– determine the call is an emergency call. This is already done by VSPs and so this requirement should need no further effort.

- determine the ECSP identity. This will (in most general case) require the VSP to make a query using interface ib to an LS Discovery service.

It should be noted that the current method of delivering 999 calls in the UK effectively ‘shortcuts’ the usage of both interfaces ib and ic for this purpose, since the destination of the ie interface is the emergency call handling centres (via the ECSP). This assumption is correct for all UK calls, so the requirement to utilise the discovery and query processes defined by interfaces ib and ic for ALL calls will add an avoidable delay into the delivery of ALL 999 calls from a UK subscriber who is making the call within the UK. However, if VSP is not UK based, then these processes will be needed to at least determine the UE is in the UK.

There is a need to accept all the possible Uniform Resource Names (URNs) even if you do not use or need them; hence calls to 112, 999 and urn:service:sos and its extensions should be processed as an emergency call, where this usage/processing does not clash with numbering present in the UK dial plan.

5.2.2 Call originator identity

ES 203 178 states it is mandatory for originating VSP to provide a verified, screened P-Asserted-Identity header field which can uniquely be assigned to a certain subscriber. For call originated in the UK this is enforced by Ofcom's General Conditions, and UK signalling standards will also apply (see ND1035[19]), ND1016[20] and ND1439[21]).

The originating VSP must ensure that emergency calls are accompanied by a valid Network Number Calling Line Identity which assists the PSAP. This must be carried in a P-Asserted-Identity header field (as specified by RFC 3325[6]) inserted by the originating VSP (as mandated in ND1035 [19])

5.2.3 Session Border Controller (SBC) requirements

Emergency call geolocation information can be passed through using IETF RFC 6422 [13] SIP Geolocation header and the use of a location URI reference, or a Presence Information Data Format Location Object (PIDF-LO) carrying actual civic or geodetic location in the body of the SIP message.

Where VSP SBCs currently remove this information, functionality should be added to identify the call type being made and, for recognised emergency calls, exceptions should be added to SBC configuration to ensure that such required headers are not removed.

To avoid the removal of useful information, SBCs should not remove any header fields from emergency call signalling.

5.2.4 VSP Identity

It is recommended that every VSP uses a valid x.509 Certificate in the Request as discussed in Annex D of ES 203 178. This should apply to any VSP in Europe.

Further information on identity can be found in section 4.1 of RFC 7852 [18], This, as the name suggests, contains information about the data provider which, in the case of ETSI ES 203 178, would be the VSP.

This element shall be supplied by the VSP and is either a Multipurpose Internet Mail Extensions (MIME) component in the body of the SIP INVITE or a data field stored on an external repository. The VSP shall include in the SIP Call-Info header field of the SIP INVITE a URI pointing to the ProviderInfo. In the first case, the URI in the Call-Info-header is a Cell ID (CID) URI, in the second case it is a pointer (e.g. a Hypertext Transfer Protocol Secure [HTTPS] URI) which can be dereferenced by authorized third parties (e.g. a PSAP); these cases are both specified in IETF RFC 7852 [18].

The ProviderInfo includes the following data elements, and the VSP shall include all these elements with appropriate information, in accordance with IETF RFC 7852 [18]:

- DataProviderReference.
- DataProviderString.
- ProviderID.
- ProviderIDSeries.
- TypeOfProvider: Value "Telecom Provider".
- Language.
- DataProviderContact.

Any VAP shall pass the VSP identity without modification.

The practical implementation of a registry of VSPs is an area that will require further investigation within the UK.

5.3 Emergency Call Service Providers

The ECSP is expected to be the ECSP national network as this will host the UK's national Stage 1 PSAP when the PSAP transitions to IP in 2022. The ECSP (through ESRF role) needs to route a call on to the PSP (also within ECSP in UK set-up) and provide location(s) – the locations (network location reference and UE provided location when available) will be conveyed in SIP using RFC 6422[13] SIP Geolocation header and use of a location URI reference, or a PIDF-LO carrying actual civic or geodetic location in the body of the SIP message. Wherever possible, user provided location shall be conveyed.

There could be more than one ECSP in the UK, e.g. each mobile network could operate as its own ECSP. Within such a scenario, every ECSP may have to provide a Location Server Proxy (and Route Server). However, there is currently no need for more than one Stage 1 PSAP address and this is expected to continue so there is no need for more than one ECSP.

The VSP may need to generate a local network provided caller identity, especially for cases where user provided identity for the caller is non-numeric and calls are still being routed to a circuit switched PSAP.

With regards to PAID within IMS, there will always be a SIP URI in the SIP request. There may also be a Tel URI if the subscriber has been allocated one.

An option is for the Stage 1 PSAP's call takers to insert a numeric number (CLI) based on verbal questioning of the caller, which may help the Stage 2 PSAP if call back is needed. If network provided location exists this option need not be required.

The LS Proxy would need connection to all Access Network Providers that VSPs using a given ECSP could use.

5.4 PSAP Service Providers

The PSAP Service Provider requires the ability to convey location information over SIP signalling.

The Route Server is not required in the UK as there is only one PSAP

The PSAP SP (PSP) is expected to be ECSP service which hosts the UK Stage 1 PSAP

5.5 Aggregation VSP

This is required for the architecture to be practical with large numbers of VSPs (100s in the UK) and ANPs.

A VSP aggregating entity resides inside the VSP aggregation provider network and may be used by a VSP or group of VSPs to manage trust relationships with, and routeing to, ECSPs or other VAEs that may reside in other areas or countries, as well as the UK. The VAE may also generate call data records for calls using its services. The ESRF in (ECSP) would then only have a limited number connections from VAEs. This enables there to be a trust relationship between the VAP (VSP Aggregation Provider) and the ESCP (Emergency Call Service Provider). This trust relationship facilitates cost recovery for the UK PSAP.

Upon receipt of an emergency call request from a VSP or VAE with which the VAE has a trust relationship, the VAE:

1) shall address the call to the trusted emergency handler (e.g. VAP or ECSP);
2) shall forward the emergency call to the trusted emergency handler (e.g. VAP or ECSP).

In the UK, the VSP Aggregation Provider(s) could/should extend its role to be able to provide the interface ic access to the LS as a proxy for UK VSPs.

In this case, the VSP sends the information received on the interface ia to the VAE unchanged. It is the VAE that performs the Location Discovery (interface ib) and communication with the Location Server (interface ic) in all networks. Then UK LSs will only talk to VAE proxies and VSPs do not have to talk to LSs. This would be explored further as it allowed a VAE to do most of the 'hard work' for the VSPs.

The interfaces in the ES 203 178 are: _
-VSP Call Control to VAE (ie)
- VAE to ESRF (ie)

With an extended VAE functionality as being considered by EmLoC TG , the interfaces are:
- VSP Call Control to VAE (ie)
- VAE to ESRF (ie)
- VAE to LS Discovery (ib)
- VAE to Location Server (ic)

NOTE 14: For overseas VSPs they would still have to know that the caller was in the UK before they could similarly benefit and send calls to UK VAE. UK VSPs with overseas users may not have the same option of a VAE in another country so may have to implement interface ic for overseas cases.

5.6 PSAP

The Stage 1 PSAP forwards calls and location to Stage 2 PSAPs.

The M493 architecture covers two methods for transmission of location values to the PSAPs, the push and the pull method:-

In the push method, the location values are transmitted via the ii or ij interface as part of the call setup signalling information or via the ik or im interface directly to the PSAP as soon as the emergency call request is sent to the PSAP.

In the pull method the PSAP receives via the ii or ij interface the information required to acquire a location value from the LS or the LS Proxy via the ik, il or im interface. The request is triggered manually by the PSAP operator on a case-by-case basis or automatically in the PSAP entity with every emergency call request received. The 'pull' method is currently used in the UK by stage 1 and stage 2 PSAPs to obtain mobile location information from Gateway Mobile Location Centre (GMLCs), and it would be expected for interfaces im and il to also be pull interfaces when IP-PSAPs ready for the information. The Stage 1 PSAP uses the location reference received in SIP signalling to look-up the network location from the ISP LS and can use this to route the call to correct Stage 2 PSAP and provide the Stage 2 PSAP with the network location and any UE location provided.

The Stage 1 PSAP is initially expected to continue to convey location through the "out of band" Enhanced Information Service for Emergency Calls (EISEC) interface to Stage 2 PSAP.

5.7 Private Telecoms Network Environments

This section refers to VoIP services originating from an enterprise network separate from lower layer Service Provider as well as one or several contributing infrastructure operators.

One solution to the private network problem is to not support emergency calls at all, and simply to post a notice on the device or display screen indicating that emergency calls are not supported, and possibly indicating what alternatives are available.

A more limited form of this scenario would be to support emergency calls only when the users are known to be in a defined location in relation to the enterprise, for “on site” and using the enterprise IP network, rather than “off-site” and accessing the enterprise services using some other IP network.

In many cases, the alternative might be available on the same device. For example the enterprise application might be accessed using IP provided on a mobile phone, which is inherently capable of making emergency calls in its own right, using the mobile phone network rather than the enterprise network.

Conversely, it may be important that the caller ID does identify the enterprise, rather than some miscellaneous end user. For example, a PSAP might initiate a larger response if the call is identified as coming from a phone controlled by a chemical plant, as opposed to one from an outside user, even where the accompanying locations are one and the same. Whether this option is available will depend on the regulator, and their perception of whether the public need is met by such alternatives, rather than any technical considerations.

Another option would be where it is not technically possible to identify the location of a caller the device should ask the user to confirm their location prior to voice service activation.

In general, the opinion of the ETSI technical body addressing the ETSI ES 203 178 specifications was that any enterprise network would not be an originating telephony or electronic communications Service Provider. However, the decision as to which bodies qualify as the providers is up to the local regulator. Even if the UK decision is generally that they cannot, then there might be certain categories of enterprise network providers in the UK, or certain designated enterprise network providers in the UK, that could meet the relevant requirements set by the regulator for such providers.

Is the location of the voice server in the enterprise sufficient? Without any modification, the architecture in the main body of ES 203 178 will deliver the location of the ANP supporting the voice server of the enterprise, rather than that of the end user devices. For a number of enterprise deployments, where the physical separation of all end user devices and the voice server are located within a tightly constrained geographical area, this may be sufficient to meet the needs of the emergency Service Providers.

Are the additional mechanisms specified in ES 203 178 Annex B sufficient? Annex B defines a new term “flow changer” that incorporates elements of an enterprise network. It goes on to define two mechanisms to cover such “flow changers”.

Annex B.2 covers an LS chaining solution, which requires support from ANPs (which would consequently need to be required to support that mechanism). Some work would also be required to define the interface protocols for the additional interfaces, said interface protocols would then need to be supported by the enterprise equipment and the ANP. It would need to be decided whether this additional specification work could be carried out on a national basis or whether it would need to be performed by ETSI.

Annex B.3 references a HOST_ID solution. The referenced IETF RFC 6967 [16] is not a fully defined solution for this proposal and further specification work would be required to define this solution. Again, it would need to be decided whether this additional specification work could be carried out on a national basis or whether it would need to be performed by ETSI.

If the enterprise uses a private IP network, the potentially the ANP of the end user falls outside the regulation, and is no longer a trusted source of location, even if they are capable of providing a location and operating according to the same standards. Further, this scenario has not been explicitly covered by the mandate as it falls outside the statement “an enterprise separate from lower layer Service Providers”, and has not been considered further by the architecture of ES 203 178.

Many private IP networks will be a single wireless Local Area Network (LAN) and therefore the locality will be limited, along with the voice handling handled by a voice server within the same location. As such, as already discussed, the location provided by the ANP of the enterprise voice server will be sufficient.

Outside of this, no technical solution currently exists, and what is adequate in the absence of that will depend on the regulator.

The general conclusion is that, due to the wide variety of enterprises, there is no one solution that fits all. Thus rather, the regulation may need to come down on the enterprise operator, rather than the enterprise equipment, to provide a solution where the individual enterprise employees have a means of emergency calling that fits within the needs of an enterprise. This could range from providing all enterprise users with a mobile phone with emergency calling capabilities (that might also parallel other enterprise needs) to specialised emergency equipment environments that might be required by, say, a chemical works. The toolkit of solutions in the ETSI ES 203 178 documentation, and other technical solutions, may help to support this need, but are not the only answer to it.

The manner in which emergency calls are handled may have to differ from normal calls in an enterprise environment, and some aspects of this may be a matter of configuration rather than technical solution, e.g. turning off “least cost” routeing and ensuring that the emergency call enters the “public network” at a point closest to the caller.

The solution to caller location & identification from private telecommunication network requires further design consideration and standardisation.

5.8 Requirements for the new UK non-functional aspects additional to ETSI ES 203 178

The way in which components operate and interact is defined in ES 203 283: how well they are expected to perform is not. Non-functional requirements and expected standards will need to be developed by NICC covering aspects such as:

- Latency in some of location establishment processes, which should not hold-up call set-up leaving caller unsure of whether to re-dial. So key timeouts will be needed and if breached then, for example, default call routeing and reliance on verbal questioning for location may need to be used.
- Enquiry throughput (peak, burst and average) affecting performance of components
- Response time between enquiry and response

VSPs must have robust exception handling processes in place for when lookups and queries are unsuccessful, provide erroneous information, and/or take too long to achieve.

6 Use Cases

Use cases for emergency calling are included as a table in Annex A.

Further Study will be required in the areas of :-
- the rate of growth of the cases where ETSI ES 203 178 would help
- use of any known alternative methods to ETSI ES 203 178 approach of any of the use cases
- consideration of partial implementation of ETSI ES 203 178 to help with some use cases

7 Alignment of UK with ETSI Architecture

Figure 5 shows in outline how the ETSI approach could be implemented in the UK.

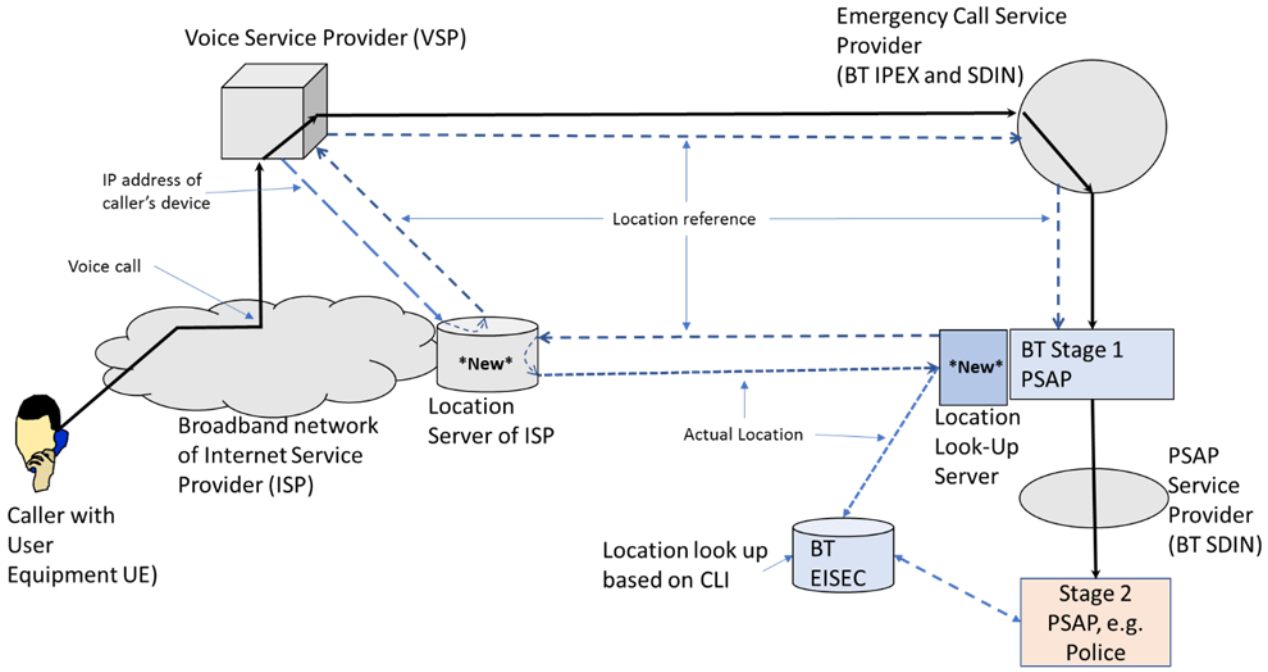


Figure 5: Outline architecture and transactions for ETSI standard as envisaged for the UK

7.2 Emergency call processing

Under the architecture of the ETSI standard, the procedure for ensuring the correct processing of an emergency call would be as follows:

1. The caller's User Equipment (UE) makes an emergency call request to its VSP and may, in some cases, include location information from the UE (such as handset derived location information in form of GPS coordinates). The ETSI approach covers both the case where VSP is in the UK (as in Figure 1) and where its call server may be in another European country.

2. The VSP is then required to find the UE's network location from the ISP and to identify the correct PSAP to which to route the call (only a single Stage 1 PSAP for UK so this is straightforward once location is confirmed as UK). The VSP uses a new process to determine the identity of the ISP and the associated network information needed to contact the ISP's Location Server (LS) – known as the 'LS discovery' process. This process requires all Access Network Providers (ANPs) to establish and maintain a Location Server and ensure that it can be discovered through readily available protocols. Such protocols have been described , but it is not known whether they satisfy the reliability, security and accuracy requirements that would need to be established for widespread use.

3. The VSP interrogates the ISP's Location Server (LS) using the IP address (and other information associated with the call) and receives from the LS a unique Location Reference, which, in and of itself, is insufficient for the VSP to identify the location of the caller. The use of a Location Reference avoids the VSP being given a network provided UE location by the ISP, so allowing the ISP to maintain appropriate privacy for the UE. The Location Server also provides the identity of the PSAP to which emergency calls should be routed - this is the way by which the VSP can

determine whether the call needs to be routed abroad, though for ISP LSs in the UK this will simply be the Stage 1 PSAP. The identity of the PSAP will be in the form of a URL (Uniform Resource Locator) of the PSAP's Emergency Call Service Provider.

4. With knowledge of the appropriate ECSP and with the associated Location Reference, the VSP routes the emergency call towards the Emergency Call Service Provider , potentially via an intermediary voice aggregation provider (VAP) with whom a trusted relationship has been previously established. The VSP (or VAP) must establish a trusted relationship with the ECSP before providing service to prevent the ECSP from having to handle calls from unrecognised entities, which would elevate the risk of attacks on the ECSP. However, while the technical methods/protocols to achieve this exist, to create these relationships VSPs will first need to identify the appropriate ECSP(s) in each relevant country. It is not clear which organisation, even simply for the UK, would determine and maintain ECSP and VAP contact details to be provided to any VSP so that they could then learn what was needed for that ECSP (or ECSPs in some countries) to accept their emergency calls.

5. Once a solution is established and adopted, the VSP would be required to send network provided location information for the UE (which for the UK is expected to be a Location Reference), and any location information that may be provided by the UE itself, to the ECSP within the SIP signalling.

6. The ECSP then routes the call onward towards the Stage 1 PSAP, via the PSAP Service Provider (PSP, which is also a function of the ECSP in the UK).

7. The Stage 1 PSAP then uses the Location Reference received in SIP signalling (which also contains the identity of the ISP Location Server that issued the reference) to interrogate the Location Server in order to retrieve the network provided location of the UE. This communication would be via a secure connection given the sensitivity of the information being transferred.

8. The Stage 1 PSAP is then able to route the call to the most appropriate Stage 2 PSAP (e.g. London Ambulance) again using the PSAP Service Provider and to provide the EA's Stage 2 PSAP with the network location of the UE and any location provided by the UE itself. The Stage 1 PSAP is initially expected to convey location through the existing "out of band" EISEC interface to Stage 2 PSAPs. It is expected that location conveyance via SIP signalling would also be gradually deployed as the Stage 1 and Stage 2 PSAPs become more fully SIP enabled. (See Annex B for fuller discussion)

7.3 Implementation and operational oversight

For emergency calls to successfully use the approach set out here in section 8, all organisations identified need to take on new roles and responsibilities. To highlight many of these this section considers the impact on new entrants to the market.

In addition to the call handling requirements discussed above, a new VSP will need to:

- Identify any and all Location Server discovery databases in all countries in which it advertises service provision
- Identify and establish the routeing details and mechanisms to all PSAPs in all countries in which it advertises service provision (and potentially in countries in which its customers may roam and make emergency call), so as to ensure that calls by its subscribers arising in any country can be successfully routed. The VSPs will also need to register and form a trusted relationship with all ECSPs to ensure that calls can be identified as legitimate for onward routeing to the PSAP. If such direct mechanisms/registrations are not possible then the VSP must establish relationships with one or more (usually larger) VSPs that act as a VAP and will route calls to any and all PSAPs in Europe.

A new ISP or broadband provider that has not previously had a direct role in providing an emergency service, will need to:

- Identify any and all location discovery databases across Europe, make contact and upload relevant IP address ranges and network address details for their Location Server (to assist VSPs offering service to subscribers in the UK);
- Contact the relevant PSAP to agree and establish the secure communication channel needed for the PSAP to recover location information from a location reference issued by that ISP.

Given the different types of business and organisations that need to be involved in the successful routeing of emergency calls, operational complexities and issues are likely to arise in the implementation of this approach.

Even with strictly defined technical standards and regulations, effective coordination and dialogue is likely to be needed.

There is a brief discussion in Annex C but further consideration of how such oversight is achieved and by whom is outside the scope of this report.

8 Implications & Recommendations for UK providers

To ensure the successful conveyance of emergency calls to the appropriate emergency service and to provide accurate location information, new protocols, procedures, relationships and components (hardware) are required. These requirements are summarised below:

1. UK ISPs, including those that offer only broadband and/or Wi-Fi connectivity, would need to operate and maintain a Location Server (LS), tracking in real time the physical access points to which an IP address is currently allocated.

2. UK ISPs need to keep up to date details of the IP addresses for which it is responsible, the address (URI) of its Location Server and provide this information to the organisation managing the Location Discovery facility.

3. One or more organisations need to create and maintain a Location Discovery facility. If one organisation establishes this, then it needs to advertise to all European ISPs of its existence and the process for uploading information. If each country creates its own database/facility, then all VSPs across Europe will need to know the address of each, and have processes by which to interrogate them all in a prompt manner when a call from an unknown IP address is received.

4. An ISP's Location Server must provide location reference details to any VSP that may require this information. As it is not possible to establish that an entity making a request is a valid VSP, the LS must be robust enough to withstand erroneous/malicious attacks on these open (public) interfaces. It also needs sufficient resources to respond to requests for information promptly, as without the correct routeing information the VSP is unable to forward the call to the correct PSAP, leading to delays in call set-up and answer.

5. All ISPs must establish a trust relationship with the PSAP, so as to allow secure communications between them to convey accurate location information from the Location Server.

6. All VSPs must incorporate the following protocols into their emergency call handling procedures:

a. To interrogate the Location Discovery database(s) to quickly identify the correct Location Server from which to request location information;

b. To route calls to the correct PSAP and include the necessary location(s);

c. Provide a VSP identifier; and

d. To have robust exception handling processes in place for when lookups and queries are unsuccessful, provide erroneous information, and/or take too long to achieve.

7. All VSPs must also either -

(a) establish a trusted relationship with the ECSP to directly route emergency calls or

(b) form a contractual relationship with an aggregating VSP to do so on its behalf.

8. The PSAP needs to create a capability (shown as Location Look-Up Server in Figure 1) to interrogate, in real time, all the ISP Location Servers to retrieve a valid location using the location reference provided by the VSP.

9. All parties – VSPs, ISPs, ECSP, Stage 1 PSAP – will need to ensure that network components allow key SIP fields used to convey location and VSP identity to be transmitted, and ISPs and VSPs must allow IP flows (IP address, port number and IP version) used for emergency calls to be tracked across network components (such as Firewalls).

10. There needs to be an organisation to allocate and manage VSP IDs

In conclusion, there are a large number of outstanding practical implementation issues highlighted in this report, requiring detailed UK design agreement and specification. It is the considered opinion of the EmLoc Task Group that to pursue the full implementation of ETSI ES 203 178 would be protracted. Therefore, a more targeted, UK use case centric approach based on ETSI ES 203 178 would lead to earlier resolution of location issues being seen in the UK today. However there are some use cases which would require a full implementation of ETSI ES 203 178 to be resolved.

The recommendation of this report is that full implementation of ETSI ES 203 178 is currently not adopted within the UK. Furthermore it is recommended that the UK NICC EmLoc Task Group be focused on prioritisation of the identified use cases found in ANNEX A , with the view to identifying and publishing solutions to these specific use cases including detailed specifications as required.

Although work on ETSI ES 203 178 is in abeyance in the UK this does not preclude it from being reviewed in the future for potential implementation. It is also acknowledged that other European partners may implement ETSI ES 203 178 in which case interworking will have to be addressed.

ANNEX A : Summary of potential use cases

Introduction

Call volume figures are approximate monthly totals provided by the PSAP.
There is a current underlying increase in demand of ~3% per year in 999 calls from all sources over the last couple of years due to various societal factors and the impact of emergency authority performance for emergency and non-emergency numbers. That level of increase may well continue though this will not be taken into account for this initial view where overall volumes are kept constant, until such a time as we can better understand the way end users may move between device types.
Location sources include:-
- accurate Voice Service Provider (VSP) records for
(i) installation addresses of lines to which specific telephone number is physically associated and also
(ii) the concept of a "default address" (or normal registered address) for a telephone number where the service could possibly be used at a different address to that indicated by the VSP's record of where it was provided. Such default addresses have to be verbally confirmed by PSAPs and typically applies to VOIP services, and to services that form part of a private network over several sites with limited access to a public network.
- cell identifier (or zone corresponding to a group of cells) from 3GPP mobile networks and cell coverage location from network's GMLC (General Mobile Location Centre)
- device locations: ETSI ES 203 178 and ES 203 283 allows for locations established by the device to be conveyed to the PSAP alongside a VSP provided location. The device's SIP client may be able to learn its location in various ways including use of its built-in location sensors (such as use of GNSS)
Note16 : Location information established by smartphones using built-in GNSS and Wi-Fi connectivity is already transported (e.g. use of SMS or HTTPS) to PSAPs using AML – see ETSI TS 103 625 – which is considered as supplementary information to the location provided by CPs as part of regulation.
- ISP LIS: in ETS ES 203 178 and ES 203 283 sVSPs are expected to use an ISP's Location Server (LS) to provide the location of the device
- Verbal provision to a 999 PSAP call operator is fallback if none of the above sources are available.

NOTE 15: Some VSPs and Enterprises may make provision for end users to manually update their own location information for nomadic callers with their VSP, but this is not included in the table at present as a reliable method as it is not clear how this would reach PSAP in a timely manner. It is possible that it could be considered in future as a form of "Device Provided" location through SIP Location Conveyance if it can be marked as manually provided to distinguish from CP or device provided using GNSS, or other automated methods.

"Phone" is used in the table to represent a conventional, analogue, line powered telephone (or base unit which may include a wireless handset) that that can be connected into either a wall socket for a PSTN line or into a powered Analogue Telephone Adapator to use a VoIP service.

Glossary and Abbreviations

Voice Service Provider (VSP) - the Communication Provider (CP) that provides voice access to the emergency service, which will be either a VoIP CP or a Time Division Multiplexing (TDM) CP
Global Navigation Satellite System (GNSS) – various systems like GPS, GLONASS and GALILEO are now widely used by devices to establish location
Location Server (LS) – Location Server provided by an Internet Service Provider (ISP) that allows location information to be provided to a VSP and to a PSAP
999 – 999 and 112 are both used as emergency numbers, but only 999 is included in the table to save space
PSAP - Public Safety Answering Point

ECSP - Service Provider that acts as a mediator between VSPs and the PSAP Service Provider. This is currently the PSTN for TDM CPs and normally ECSP for VoIP CPs.
Fixed end user – use case where the voice service is expected to be used at one normal location
Mobile end user – use case where voice service can be used at multiple locations and while moving between locations (usually on the same access network)
Nomadic end user – use case where voice service can be used at multiple locations after device re-registration at each endpoint (often using different access networks)
IMS - IP Multimedia Core Network Subsystem (3GPP standard)

Table of potential use cases - for further study

End user	**Device Type**	**VSP1**	**VSP2 (option needed for interconnect to ECSP)**	**ISP (provides IP access for end user)**	**Notes**	**Location Sources for 999**	**999/112 calls now (PSTN or VoIP) – estimated from June 2019**	**Estimated 999s in June 2022 (PSTN or VoIP) – with/without ES 203 283 implemented ***
Residential fixed	Phone	TDM CP	N/A – direct connection to ECSP	N/A – not needed for TDM voice.	PSTN or Cable Provider	**VSP records**	430k	300k/300k
Residential fixed	VoIP Phone (built in SIP) Phone + ATA	VoIP CP	VoIP CP	Broadband Provider (could be different to VoIP CP and physical Access Provider**)	Some current VoIP Includes fixed line replacement services (some may be tied to location where Broadband service provided)	**VSP records (default address)** ISP LS and/or Device location may be possible if ES 203 283 implemented	28k	50k/50k
Residential fixed	Phone +ATA (eDVA – enhanced Digital Voice Adaptor)	VoIP CP	VoIP CP	Cable Provider	Some current VoIP	**VSP Records (default address)** ISP LS and/or Device location may be possible if ES 203 283 implemented	Included in line 2	Included in line 2
Personal Mobile	Smartphone	Mobile CP	Mobile CP	Mobile Network (inc. IMS)	2G, 3G, 4G, 5G	CP cells/GMLC DeviceGNSS/ Wi-Fi (currently AML)	1940k 1455k with AML	2100k/2100k

Personal Mobile	Smartphone	Mobile CP's VoWiFi –Wi-Fi access to VSP IMS (Mobile CP=VSP)	Mobile CP	Wi-Fi Provider provides data path for Wi-Fi Access Pt.	-Fallback if no Mobile Access through 2 - 5G -Could include >1 Wi-Fi AP provider - IMS (3GPP) does not have interfaces associated with use of ES 203 283 LS	Device may be able to provide (e.g. AML) Can IEEE Wi-Fi standards help?	3k (no location at present)	10k/10k
Personal Mobile	Smartphone	VoIP CP - Wi-Fi access to VSP's Call Server	VoIP CP	Mobile Network provides data path for Wi-Fi Access Pt.	"Over the top" (OTT) voice service Mobile network IMS (3GPP) does not provide ETSI ES 203 283 LS or associated LS interfaces	Device?	<1k	>1k/<1k ??
Personal Mobile	Vehicle Telematics	Mobile CP	Mobile CP	Mobile Network	Includes eCall	Device Cell ID + GMLC	4k	100k?/100k?
Personal Nomadic	Digital Assistant	VoIP CP	VoIP CP (Aggregation)	-Broadband Provider - Wi-Fi Provider	E.g. Smart speaker NB Currently linked to another UK partner VSP's CLI, that may provide a default address	VSP records (default address) ISP LS if ES 203 283 implemented Device capability may allow location to be established.	<0.1k	c10k/c10k?
Personal Nomadic	Tablet, laptop	VoIP CP	VoIP CP (Aggregation)	- Broadband Provider	Laptop with OTT VSP	ISP LS if ISP provides one? Device capability may	<1k	c1k/c1k?

				- Wi-Fi Provider		allow location to be established?		
Personal Nomadic	Tablet, Laptop	VoIP CP	VoIP CP (aggregation)	Mobile Network provides data path for Wi-Fi Access Pt.	E.g. Laptop tethered to mobile CP's dongle or router, with OTT VSP Mobile network IMS (3GPP) does not provide an ES 203 283 LS or associated LS interfaces	Device capability allows location to be established?	<1k	c1k/c1k?
Personal Nomadic	Phone + ATA	VoIP CP	VoIP CP (aggregation)	-Broadband Provider - Wi-Fi Provider		VSP Records (default address) ISP LS may be possible if ES 203 283 implemented	<1k	<1k/<1k?
Non-personal	IoT sensor	VoIP CP	VoIP CP	-Mobile Network -Wi-Fi Provider	Not an interpersonal, conversational 999. As such, should we assume 999 message arrives at PSAP via a Service Provider's Monitoring Centre? [As for Burglar/Fire alarms]	Device? Monitoring Centre address records?	0	??
Business fixed (SME)	Phone	TDM CP	N/A – direct connection to ECSP	N/A	Single Sites	**VSP records**	200k	100k?/100k?
Business fixed (SME)	VoIP Phone (built in SIP) Phone + ATA	VoIP CP	VoIP CP	Broadband Provider	Single Sites Includes fixed line replacement services (some may	**VSP records (Default Address)** ISP LS and/or device location may be	60k	160k?/160k?

					be tied to BB service location)	possible if ES 203 283 implemented		
Enterprise PBX	Phone on PBX extension	TDM	N/A – direct connection to ECSP	N/A	Multiple Sites	**VSP records – default address**	45k PSTN	15k?
Enterprise iPBX	VoIP Phone on PBX extension	VoIP CP	VoIP CP	SIP- Trunk provider (could be different to VoIP CP)	Service intelligence in on site iPBX. Multiple Sites	**VSP records – default address** LS/Enterprise LS considered impractical due to private network complexity Device locations may be possible ?	Included Above (not able to separate)	15k?
Enterprise Cloud	VoIP Phone (built in SIP) Phone + ATA	VoIP CP	VoIP CP	SIP-Trunk provider (could be different to VoIP CP)	Service iPBX-like intelligence in remote data centres. Multiple Sites	**VSP records – default address** LS/Enterprise LS considered impractical due to private network complexity. Device locations may be possible	Included in other 2 lines above(not able to separate)	15k?
Nomadic user for Enterprise	Laptop/Tablet	VoIP CP	VoIP CP	Broadband Provider Wi-Fi Provider	More complex than personal nomadic (as may be routed via iPBX)	VSP records – default address LS/Enterprise LS considered impractical due to private network complexity. Device locations may be possible	<1k	<1k/??
Streetphone	Public payphone	TDM	N/A – direct connection to ECSP	Not applicable	Some VoIP sites now active	**CP records**	40k	<<40k

Text Relay end user at fixed location* **	Textphone	TDM CP	TDM CP	Not applicable	Textphone uses TDM voice channel	Textphone uses VSP records	1.3k (c.80% of which start as SMS)	1.5k
Text Relay end user at fixed location* **	Laptop/tablet or Textphone	VoIP CP	VoIP CP	Broadband Provider (could be different to VoIP CP and physical Access Provider**)	RelayUK App and VoIP service, tablet or laptop uses NGT Lite (forerunner of RelayUk App) and VoIP Service. Textphone uses VoIP service (testing shows may be some issues)	Relay UK App and Textphone assumed to be linked with VoIP, so VSP records with same limitations as for Res VoIP user above	Included above	Included above
Text Relay end user – mobile or nomadic* **	Smartphone or Laptop/tablet	Mobile CP or VoIP VSP [See mobile and nomadic cases above]	Mobile CP or VoIP VSP [See mobile and nomadic cases above]	Mobile IMS or Wi-Fi provider [See mobile and nomadic cases above]	Smartphone uses SMS or RelayUK App and mobile voice. Tablet or laptop uses NGT Lite (forerunner of RelayUk App) and VoIP service	SMS - GMLC location using Mobile CP plus Device's GNSS/Wi-Fi (AML) Relay UK App assumed to be linked to mobile CP (as VSP) or VoIP VSP - same location options and limits as for Mobile/Nomadic users above	Included above	Included above

* Implementation of ES 203 283 would allow location to be provided in more use cases so that more calls may be made for use cases that would otherwise be avoided by VSPs.
** There may be different Service Providers for physical connectivity (Access Network Provider, ANP) and IP connectivity (ISP) to User Equipment at any location. The ISP can confirm the location where it is providing service to an end user from information provided by the ANP - interfaces between these organizations are not covered in ETSI ES 203 283 being left as a matter of contractual relations between the parties.

*** Code 18000 is used as an emergency number for UK citizens with hearing or speech impairment. 18000 calls are currently treated in the same way as other 999 calls within the PSTN (see TSG022) but initially terminate on one of four Next Generation Text (NGT) Service nodes. The use of the 18000 access code for

emergency calls supports in-band modem tones generated by specialised textphones (that use ITUv21, e.g. a Minicom or Uniphone) over the circuit-switched voice channel from originating end user terminals to communicate with Text Relay Assistants (TRAs) who answer calls within the Relay UK call centre. The TRAs can then relay text-to-voice to allow a customer who uses text to communicate with the 999 operator and then with the emergency services, with the voice link to 999 automatically initiated by the NGT platform to reach the 999 operators.
An Emergency SMS service is operated to allow deaf, hard of hearing and speech-impaired people in the UK to send an SMS text message to the Relay UK Service, from where a voice emergency call is set-up to the UK Stage 1 PSAP. This link allows content of the SMS message to be relayed to Stage 1 and 2 PSAPs, and questions and answers are then relayed between Stage 2 PSAP and the originator of the text by the TRA. This service is not aimed at use as a general alternative to the voice service. It requires registration of the mobile phone number with the Text Relay Service before use.
Relay UK App – the App enables users to type and read over a separate data link via the internet to the NGT nodes in parallel with an 18000 voice call. When using the Relay UK App the caller can simultaneously type, read, speak, or hear depending on their individual communication needs.
See https://www.relayuk.bt.com/ for details.

NOTE 16: For VSPs connecting to an IP PSAP, alternative methods exist in standards for real time text, using SDP options, and there is a need for future study on the best way forward, for example migrating away from textphones/specialised terminals and emergency SMS toward solutions using terminals using SIP sessions and real time text (see ETSI TS 103 479, which also discusses a simple Instant Messaging approach). The future regulatory position for the 18000 service also needs to be taken into account. Until any replacement service is agreed, then VoIP VSPs need to route 18000 calls made in the UK to the NGT nodes which use TDM.
There is IETF activity to allow this to be explored further:

https://datatracker.ietf.org/doc/charter-ietf-rum/
https://tools.ietf.org/html/draft-ietf-rum-rue-01

ANNEX B: Emergency Authority Stage 2 PSAPs

There are currently 139 stage 2 PSAPs, with separate ones for the Police, Ambulance, Fire and Coastguard. These will be moving from ISDN access to SIP trunks over the next few years – with all expected to move by 2025.

The Stage 1 PSAP will be able to connect voice calls to both PSTN and SIP based stage 2 PSAPs, and also be expected to continue to transfer location using its out-of-band EISEC service using a different path to the voice.

As more Stage 2 PSAPs and interconnecting networks move to be fully SIP based, the option should become available of simplifying the transfer of location to simply use the SIP Location headers in the same SIP session as the voice.

For the foreseeable future both options need to be supported.

NOTE 17*: EISEC may still be the preferred option long term - there are complexities in how long it takes an end user device to establish its location, which may mean that in order not to delay voice set-up, and avoid any mid-call transactions affecting calls, SIP messages arrive at PSAPs with simply a network location and any device location is sent out of band (e.g. as at present for AML).*

ANNEX C: Organisational and commercial considerations

In current (11/2018) UK regulation the General Conditions of Entitlement (GCs) place the obligation to provide end-users with access to the emergency services, and in association with that to provide to the emergency services, where technically feasible, information on the end-user's location, on the legal entity providing the end-user with the calls service (the Voice Service Provider). However, M493's raison d'être is that the Voice Service Provider (VSP) does not necessarily know the location of the end-user due to the nomadic potential of VoIP services.

The deployment of the ETSI ES 203 178 standards indicates that provision of such location information is technically feasible but requires the involvement of ISPs, which in turn requires new working/commercial relationships between VSPs and ISPs, and ISPs and PSAPs. These relationships will need to make it clear as to where legal responsibility lies for the accuracy of location information and the speed of its delivery to the emergency services.

It is unclear whether such new relationships can be expected to be widely and readily established within normal working relationships under the current regulatory environment.

Further there will be additional costs for VSPs, ISPs and PSAPs in developing, deploying and in operating any implementation of the M493 approach.

The implementations will need to meet the normal challenging 999 standards for security, performance and audit trails.

History

Document history		
Version	Date	Milestone
1.1.1	26th January 2022	Initial issue