TECHNICAL REPORT

ISO/IEC TR 16167

Second edition
2011-09-01

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Emergency calls

Technologies de l'information — Téléinformatique — Réseaux d'entreprise de prochaine génération (NGCN) — Appels d'urgence

Reference number
ISO/IEC TR 16167:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 16167 was prepared by Ecma International (as ECMA TR/101) and was adopted, under a special "fast-track procedure", by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

This second edition cancels and replaces the first edition (ISO/IEC TR 16167:2010), which has been technically revised. This second edition makes a distinction between an answering point and an emergency control centre and clarifies a few other points, in particular to do with interaction with (public) Next Generation Networks.

Introduction

This Technical Report is one of a series of publications that provides an overview of IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on session level communication based on the Session Initiation Protocol (SIP) [5], with an emphasis on inter-domain communication. This includes communication between parts of the same enterprise (on dedicated infrastructures and/or hosted), between enterprises and between enterprises and public networks. Particular consideration is given to Next Generation Networks (NGN) as public networks and as providers of hosted enterprise capabilities. Key technical issues are investigated, current standardisation work and gaps in this area are identified, and a number of requirements are stated. Among other uses, this series of publications can act as a reference for other standardisation bodies working in this field.

Various regional and national bodies address emergency communications, mainly with an emphasis on public telecommunications. In particular, in the United States work is carried out by the National Emergency Number Association (NENA). In Europe, ETSI EMTEL (Special Committee on Emergency Communications) plays a coordinating role, liaising with external bodies (e.g., in the European Commission, CEPT, CEN and CENELEC) as well as overseeing work done by other ETSI Technical Bodies (e.g., TISPAN). This Technical Report focuses on emergency calls as they impact enterprise networks, and therefore is intended to complement the work of those other bodies.

This Technical Report is based upon the practical experience of Ecma member companies and the results of their active and continuous participation in the work of ISO/IEC JTC 1, ITU-T, ETSI, IETF and other international and national standardisation bodies. It represents a pragmatic and widely based consensus. In particular, Ecma acknowledges valuable input from experts in ETSI TISPAN, ETSI EMTEL, 3GPP CT1 and IETF ECRIT.

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Emergency calls

1 Scope

This Technical Report discusses issues related to emergency calls from an enterprise user to a safety answering point (SAP) using the Session Initiation Protocol (SIP) within a Next Generation Corporate Network (NGCN). A SAP can be either a public safety answering point (PSAP) or a private emergency answering point (PEAP). This Technical Report uses terminology and concepts developed in ISO/IEC TR 12860. It identifies a number of requirements impacting Next Generation Network (NGN) standardisation and concerning deployment of enterprise networks.

The scope of this Technical Report is limited to calls from a user of an enterprise network to an authority, where the authority is represented by a SAP (PSAP or PEAP). This includes the special case where a PEAP acts as an enterprise user in making an emergency call to a PSAP. Authority to authority calls, authority to enterprise user calls and enterprise user to enterprise user calls within the context of an emergency are out of scope, with the exception of return calls and verification calls as follow-up to an emergency call from the user to an authority.

This Technical Report focuses on emergency calls within a SIP-based NGCN using geographic location information to indicate the whereabouts of the caller. Emergency calls can originate from devices connected to the NGCN via various access technologies, e.g., SIP over fixed or wireless LAN (Local Area Network), TDM (Time Division Multiplex) networks, DECT (Digital Enhanced Cordless Telephone) networks, PMR (Private Mobile Radio) networks, PLMN (Public Land Mobile Network), etc. SAPs are assumed to be reachable either directly using SIP or via a gateway to some legacy technology (e.g., TDM). Furthermore, SAPs are assumed to be reachable either directly from the NGCN or via a public network accessed from the NGCN using SIP. In the latter case, the NGCN might identify the SAP and instruct the public network to route to the SAP, or alternatively the NGCN might leave the public network to identify the SAP, based on the location of the caller. In all cases the NGCN is assumed to deliver the location of the caller to the SAP, gateway or public network in order to provide appropriate information to the call taker at the SAP.

The handling of incoming emergency calls at a SAP, even when the SAP is provided within an NGCN, is outside the scope of this Technical Report. This includes the case where a PSAP is provided within an NGCN and hence the NGCN can receive emergency calls from public networks. This also includes the case where a PEAP is provided within an NGCN and can receive emergency calls from other enterprise networks or other parts of the same NGCN.

Different territories have different regulations impacting emergency calls, together with national or regional standards in support of these regulations. This Technical Report takes a general approach, which should be largely applicable to any territory. However, detailed differences might apply in some territories, e.g., country- or region-specific dial strings used to identify emergency calls.

The scope of this Technical Report is limited to emergency communications with a real-time element, including but not limited to voice, video, real-time text and instant messaging. The focus, however, is on voice, which in the majority of situations is likely to be the most effective medium for emergency calls. However, it is recognised that some users with special needs will require other modes of communication (e.g., real-time text, fax), as discussed in Annex B of [29], and also different modes can be used for the emergency call and the verification call. The focus is also on calls in which the caller is a human user. There may also be applications

where automatic sensors can make similar emergency calls (subject to regulation), but the special needs of such applications are not considered.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC TR 12860, *Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — General*

3 Terms and definitions

3.1 External definitions

For the purposes of this document, the following terms defined in ISO/IEC TR 12860 apply:

- Domain
- Enterprise network
- Next Generation Corporate Network (NGCN)
- Next Generation Network (NGN)
- Private network traffic
- SIP intermediary

3.2 Other definitions

For the purposes of this document, the following terms and definitions apply.

3.2.1
authority
organisation mandated to receive and respond to reports from individuals of emergency situations involving danger to person or property

3.2.2
emergency call
call from an enterprise user to a private authority or public authority for the purpose of reporting an emergency situation involving danger to person or property

3.2.3
emergency control centre
ECC
facilities used by emergency organisations to handle rescue actions in answer to emergency calls

NOTE This definition is taken from [29].

3.2.4
location
geographic location
geographic position of an entity, in the form of either geospatial coordinates (latitude, longitude, altitude) or a civic address

NOTE A civic address can extend to internal landmarks within a site, e.g., building number, floor number, room number.

3.2.5
location information
location or information from which a location can be derived

3.2.6
private authority
authority mandated by one or more enterprises to receive and respond to reports of emergency situations from enterprise users

3.2.7
private emergency answering point
PEAP
SAP established by a private authority for accepting and responding to emergency calls from users of one or more enterprise networks

3.2.8
public authority
authority mandated to receive and respond to reports of emergency situations from the general public (including enterprises)

3.2.9
public safety answering point
PSAP
SAP established by a public authority for accepting and responding to emergency calls from the general public (including enterprises)

NOTE The term PSAP is defined by the IETF in RFC 5012 [14]. The definition above is used in this Technical Report to stress the difference between a PSAP and a PEAP.

3.2.10
return call
call from a SAP to a caller or device that recently made an emergency call

3.2.11
safety answering point
SAP
answering point established by an authority for the purpose of accepting and responding to emergency calls

3.2.12
verification call
call from a SAP to a person or device that can assist in verifying conditions reported during a recent emergency call

NOTE Verification calls are frequently used when emergency calls have been made by sensor devices. For example, a verification call could be to another device in the vicinity, such as a camera.

4 Abbreviations

A-GPS	Assisted GPS
AOR	Address Of Record
ALI	Automatic Location Identification
CSTA	Computer Supported Telecommunications Applications
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
ECRIT	Emergency Context Resolution with Internet Technologies

ELIN	Emergency Location Identification Number
ECC	Emergency Control Centre
E-CSCF	Emergency Call Session Control Function
GPS	Global Positioning System
HELD	HTTP Enabled Location Discovery
HTTP	Hyper-Text Transfer Protocol
IBCF	Interconnection Border Control Function
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LAN	Local Area Network
LbyR	Location by Reference
LbyV	Location by Value
LCP	Location Configuration Protocol
LIS	Location Information Service
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP Media Endpoint Discovery
LoST	Location-to-Service Translation
NAT	Network Address Translator
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
PAI	P-Asserted-Identity
P-CSCF	Proxy Call Session Control Function
PEAP	Private Emergency Answering Point
PIDF	Presence Information Data Format
PIDF-LO	PIDF Location Object
PLMN	Public Land Mobile Network
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
SAP	Safety Answering Point
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
TDM	Time Division Multiplex
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Universal Resource Identifier
URN	Universal Resource Name
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless LAN

5 Background

General concepts of NGCNs are discussed in ISO/IEC TR 12860. In particular, that document describes use of the Session Initiation Protocol (SIP) [5] for session level communications within enterprise networks and with other domains. It focuses on enterprise networks based on enterprise infrastructure (NGCN), but also covers hosting on other networks, in particular NGNs, using the same infrastructure that supports public networks.

One important use of session level communications is for making an emergency call from an enterprise user to an authority for the purpose of reporting an emergency situation involving danger to person or property. The authority responds typically by dispatching appropriate resources to deal with the situation, perhaps first having taken steps to verify the situation. The authority concerned can be a private authority, dealing with emergency situations involving enterprise personnel or property, or can be a public authority, perhaps established by local or national government and having jurisdiction throughout a fixed geographic area or entire country. A private authority will be concerned only with emergencies arising on premises of the enterprise(s) concerned and perhaps off-premises emergencies involving enterprise personnel or property (e.g., company vehicles). Hence a private authority only handles calls from users of one or more enterprises. On the other hand, public authorities will be concerned with emergencies arising anywhere within the geographic area concerned and will handle emergency calls from the general public, including from enterprises when the emergency is not to be handled by an enterprise authority.

An authority responsible for emergency calls will establish one or more safety answering points (SAP) for answering emergency calls. A private authority will establish a private emergency answering point (PEAP) accessible from the enterprise network(s) concerned, whereas a public authority will establish a public safety answering point (PSAP) reachable from public networks. Emergency calls from enterprise users to SAPs are analogous to citizen to authority calls in public telecommunications. When the SAP is a PSAP, an emergency call from an enterprise user is indeed a citizen to authority call.

A SAP will interact with one or more emergency control centres (ECC) for initiating and controlling rescue actions in answer to emergency calls. However, ECCs, and interactions between SAPs and ECCs, are outside the scope of this Technical Report.

Figure 1 shows an example of an emergency call from an enterprise user to a PSAP (which will forward information about the emergency to an appropriate ECC).

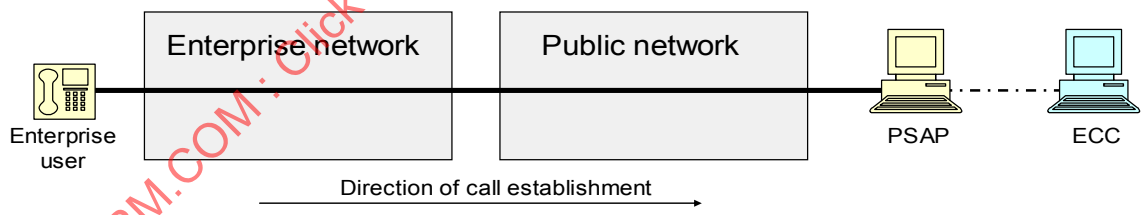

Figure 1 — Example of an emergency call from an enterprise user to a PSAP

Figure 2 shows an example of an emergency call from an enterprise user to a PEAP accessible from the enterprise network.

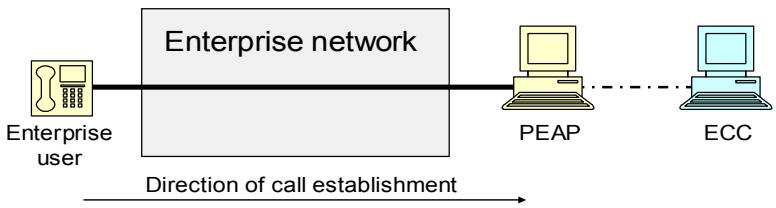

Figure 2 — Example of an emergency call from an enterprise user to a PEAP

A PEAP will typically cover only one or a limited number of sites, and is unlikely to cover sites in different countries. Thus a large enterprise might have several PEAPs. Not all enterprises will operate their own SAPs, and some might operate SAPs only for large or specialised campuses, and not for smaller sites. For example, a chemical factory or airport might operate its own PEAP, which might be better equipped than a PSAP for dispatching specialist units for dealing with the most likely emergencies. Also a very large but non-specialised campus might operate its own PEAP, which might be better equipped in terms of local knowledge, local evacuation procedures or local medical or fire-fighting equipment that can reach the scene of the emergency more quickly. Similarly a hotel might have local procedures and limited equipment for fire fighting, for example. A PEAP might not handle all types of emergency, some being deferred by the PEAP to a PSAP. An enterprise user might even be allowed to select between calling the PEAP or calling a PSAP. Smaller enterprises, and smaller outposts of large enterprises (e.g., local sales offices) are far less likely to operate their own PEAPs.

Furthermore, a single private authority might be responsible for receiving and responding to emergency calls from a number of enterprises. One example is a business park or office block occupied by a number of enterprises and providing a common PEAP. Another example is a hosting organisation that provides communications infrastructure for a number of tenants, together with a common PEAP. Logically, each enterprise has its own PEAP, but physically they are shared. A further consequence is that a PEAP might be outside the enterprise network that it serves. As a result, emergency calls from one enterprise to a PEAP in another enterprise might traverse public networks, which will not necessarily recognise emergency call traffic and provide special treatment.

An emergency call originated by the user of an enterprise network has to be routed to the appropriate SAP, whether this be a PEAP or a PSAP. The appropriate SAP may depend on the caller's location as well as on enterprise policy and possibly on the caller's preference. Also it is important to deliver to the SAP the location of the caller and information to facilitate making a return call. Resources need to be made available to emergency calls to ensure an extremely high probability of success. An emergency call needs to be subject to certain constraints, in terms of codecs used, whether voice activity detection is active, etc.. Finally, there are security considerations.

Perhaps the single most difficult issue is how to deal with roaming users, accessing the enterprise network from outside company premises, potentially anywhere in the world. For these users, connecting to a PEAP within their normal enterprise site or to a PSAP in their home city or country often makes no sense. This and other issues are discussed in the remainder of this Technical Report.

NOTE An emergency call from a user who is geographically on enterprise premises but connected directly to a public network (e.g., a Public Land Mobile Network (PLMN)) (and not connected via Virtual Private Network (VPN) with the enterprise network) will be routed to a PSAP. The possibility for a public network to detect that a user is on enterprise premises and route an emergency call to the enterprise network for further handling (e.g., routing to a PEAP) is not regarded as feasible. This possibility is not considered further in this Technical Report.

Where a PEAP is unable to handle an emergency call itself, it will need to make emergency calls to a PSAP or to another PEAP. For this purpose the PEAP can be regarded as an enterprise user, and hence such a call is might be treated as just another emergency call from an enterprise user to a SAP. In another sense it is an authority-to-authority call, and may require different treatment, e.g., it might be awarded higher priority for access to resources, and might not be subject to any restrictions on call hold or premature disconnection. Such calls are within the scope of this Technical Report only when treated as ordinary emergency calls from an enterprise user. Figure 3 shows an example.

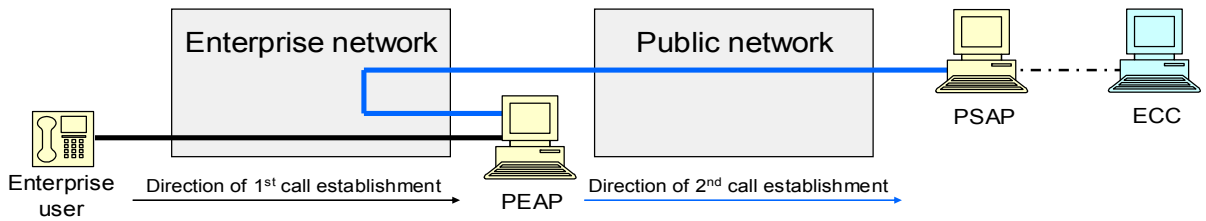

Figure 3 — Example of an emergency call from an enterprise user to a PEAP, resulting in a second emergency call from the PEAP to a PSAP

A slightly different variant on the above is where the PEAP has a direct connection to the public network and might be shared with other enterprises. Figure 4 shows an example of this.

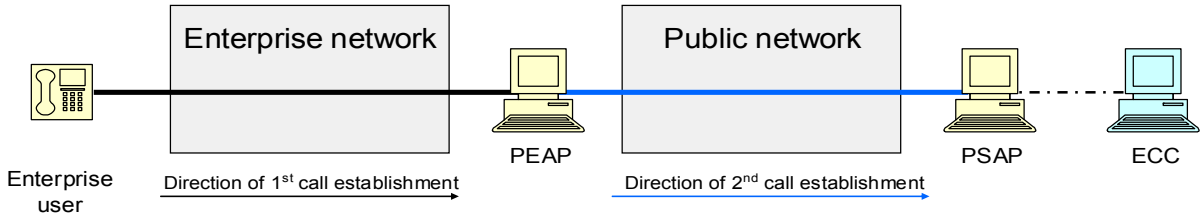

Figure 4 — Example of an emergency call from an enterprise user to a PEAP, resulting in a second emergency call from the PEAP to a PSAP without involving the enterprise network again

It is assumed that an emergency call originates at a SIP UA, i.e., in a device such as a SIP phone. Other equipment behind the SIP UA (e.g., a TDM-based part of the enterprise network) is not considered, but could potentially have an impact (e.g., if it is unable to deliver location information).

This Technical Report considers only cases where emergency calls and caller location are delivered via SIP to a SAP, to a gateway leading to a SAP, or to a public network (e.g., an NGN). It builds on material from the ECRIT (Emergency Context Resolution with Internet Technologies) Working Group in the IETF, in particular the ECRIT framework document [20] and its companion document [21], which defines best practices for end devices, intermediate devices and service providers. While the ECRIT work addresses emergency calling in the Internet, this Technical Report focuses on emergency calling within enterprise networks and from enterprise networks to public networks. The ECRIT work makes substantial use of work from the GEOPRIV (Geographic Location/Privacy) Working Group in the IETF.

Various regional and national bodies address emergency communications, mainly with an emphasis on public telecommunications. In particular, in the United States work is carried out by the National Emergency Number Association (NENA). In Europe, ETSI EMTEL (Special Committee on Emergency Communications) plays a coordinating role, liaising with external bodies (e.g., in the European Commission, CEPT, CEN and CENELEC) as well as overseeing work done by other ETSI Technical Bodies (e.g., TISPAN). This Technical Report focuses on emergency calls as they impact enterprise networks, and therefore is intended to complement the work of those other bodies.

Legacy or interim techniques involving delivery of the call by means other than SIP and/or other means of identifying the location of the caller are outside the scope of this Technical Report. In particular, the following cases are not discussed further in this document:

- legacy TDM (e.g., PSTN) cases where location is pre-configured in an automatic location identification (ALI) database, with look-up based on the calling party number or a special number known as an emergency location identification number (ELIN);
- cases where location is delivered to the SAP or a downstream network separately from call signalling;
- cases where an NGCN delivers no explicit location information to a SIP-based public network, which therefore uses pre-configured location information for the calling party identifier concerned or the NGCN site concerned.

For example, in North America NENA has specified an interim Voice over IP (VoIP) architecture for emergency services, known as NENA i2 [26], in which the SAP is TDM-based and receives location and return call information from the VoIP network (which may or may not use SIP signalling) by non-signalling means. It is assumed that NGCNs will not need to interface directly with these interim solutions, since they are not standardised internationally.

Emergency call support in NGNs is based on IP Multimedia Subsystem (IMS) emergency call support, the architecture for which is specified in [28].

NOTE At the time of publication of this Technical Report, this reference was undergoing revision.

RECOMMENDATION 1: Enterprise networks should make adequate provision for users to make emergency calls, either to a PSAP or to a PEAP within or outside the enterprise network, and instruct users, including mobile and nomadic users, how to make such calls.

6 Technical aspects of emergency calls in enterprise networks

The main technical obstacles to be overcome in providing emergency call capabilities in enterprise networks (and from enterprise networks to other networks) are as follows:

- identifying a call as an emergency call;
- obtaining and delivering the location of the caller, for the purposes of helping to identify the appropriate PSAP and facilitating dispatching assistance;
- routing an emergency call to an appropriate SAP (or gateway);
- delivering information to the SAP to allow a return call or verification call to be made;
- ensuring appropriate resources are available for an emergency call (including overriding call admission restrictions) and any return call or verification call;
- ensuring appropriate media quality during an emergency call and any return call or verification call;
- security considerations concerning emergency calls, return calls and verification calls.

These aspects are each discussed in turn below. Some of these issues are of particular relevance when a user is roaming or hosted outside normal enterprise premises.

For nomadic and mobile users when roaming, there is often the possibility of making an emergency call to a PSAP not via the enterprise network but directly via a visited public network or even directly to the PSAP. This is considered in clause 9. This present clause only considers emergency calls via an enterprise network.

6.1 Identifying a call as an emergency call

6.1.1 User actions

To request establishment of an emergency call, an enterprise user typically keys a special dial string, which is interpreted by the user's device or some other entity as being a request for an emergency call. The user might also have other means available that avoid needing to know and key the appropriate dial string. For example:

- a button, menu item or phone book entry could have been programmed in advance with the dial string, such that on pressing the button or selecting the entry the string is "dialled";
- a button, menu item or phone book entry could be configured to request an emergency call explicitly (without the involvement of a dial string);
- a dedicated (non-configurable) button or menu item could be provided.

Although the use of buttons and other means for quickly making an emergency call, without needing to know and key a dial string, sounds attractive, the disadvantage is that it can be too easy to hit a button by accident, resulting in unintended traffic to the SAP. Often authorities discourage this type of operation, and, in line with requirements from NENA, [20] and [21] recommend against single button operation on general purpose devices. However, such practices are allowed in NGN according to [30]. It is not normally feasible to prevent a user programming a key or phone book entry with a dial string for making an emergency call. For the

purposes of this Technical Report, it is assumed that a user keys a special dial string to initiate an emergency call, but other means are not precluded.

The special dial string could be one of those used in public networks, which are generally country- or region-specific (e.g., 911 in North America, 112 in Europe, 999 in the U.K.), or could be something else, e.g., a dial string specific to the whole enterprise, or to a particular site or region of the enterprise. The use of enterprise-specific dial strings requires the enterprise to take reasonable steps to educate its users (including visitors to company premises). Although placing labels on phones is one approach, this might not be sufficient for visually-impaired users. Therefore the ability to use a dial string known to the general public can have some benefits. Another issue is whether the dial string needs to be prefixed by digits normally used to access a public network. For example, in Europe, often "0" is used to access the public network, and therefore there is an issue whether "112" or "0112" should be dialled. For the benefit of visitors, the dial string without prefix digits should be accepted, but it might also be desirable to accept it with prefix digits. In a European context, it is recommended in [29] that prefixes should not be used.

When a PEAP is available, another issue is whether the call should go to the PEAP or a PSAP. Some enterprises will require all emergency calls to go to the appropriate PEAP, whereas others might allow the user to choose, either by different explicit means (e.g., two buttons), by different dial strings (e.g., the public dial string for the PSAP, an enterprise-specific dial string for the PEAP), or by a combination.

A further consideration is whether the enterprise requires or allows the user to identify different types of emergency (e.g., fire, medical) when making an emergency call, either by different explicit means (e.g., different buttons) or by different enterprise-specific dial strings. Similarly, in some territories, public networks use different dial strings for calling different emergency services.

Considerations as to the appropriate dial string(s) to use are largely a matter of policy for the enterprise concerned and/or national regulation, and are not appropriate for standardisation.

Mobile and nomadic users deserve special consideration, since when roaming they can find themselves in different geographic regions and different networks, where different dial strings might apply. A user might enter a dial string applicable only to her home region (home dial string), but this still needs to result in a successful emergency call when visiting other regions. On the other hand, she might enter a dial string for the region she is visiting (local dial string), and that too would need to work. Local regulations might even require the ability to accept the local dial string. Local dial strings that clash with other strings in the enterprise dial plan are problematic, however. An explicit means of invoking an emergency call has attractions for mobile and nomadic users, and is even mandated in [27] for mobile endpoints. On the other hand, concerns about accidentally generating unwanted traffic to the SAP apply if the procedure is too easy, as stated earlier.

The choice of dial string when roaming might also influence or be influenced by the possibility of by-passing the enterprise network and establishing an emergency call directly to a PSAP or via a public network (see clause 9).

Sometimes a user may use special applications (e.g., web-based) to drive a device such as a phone, and therefore may need to be able to make emergency calls using such applications. Similar considerations apply.

RECOMMENDATION 2: Enterprise networks should make available suitable dial strings for emergency calls for use when devices do not provide a more explicit means of calling. Where necessary, separate dial strings should be made available for different types of emergency and/or where discrimination by the user between PSAPs and PEAPs is required. Any special needs of mobile and nomadic users should be taken into account.

6.1.2 Signalling impact

The standardised means for explicitly denoting an emergency call in SIP is by placing an 'sos' Universal Resource Name (URN) [15] in the request line of the SIP INVITE request. The 'sos' URN is a particular instance of a service URN. Service URNs are also specified for specific emergency services. The following are examples of SIP request lines carrying service URNs:

INVITE urn:service:sos SIP/2.0

INVITE urn:service:sos.fire SIP/2.0

NOTE It is not expected that a user be able to enter a service URN.

Currently defined service URNs do not permit discrimination between an enterprise emergency service and a public emergency service. Therefore cases mentioned in 6.1.1 where a user might wish to state a preference are not catered for. There might be a need to register additional service URN values for enterprise-specific use.

STANDARDISATION GAP 1. There are currently no service URNs defined for use where enterprise-specific emergency services need to be identified separately from public emergency services.

Alternatively, the Request-URI can contain an emergency dial string, either explicitly identified as a dial string (but not explicitly identified as an emergency dial string) or simply as a user part known to be interpreted as a dial string by the identified domain. The following are examples of SIP request lines carrying emergency dial strings (where example.com is the enterprise domain name):

INVITE sip:911;phone-context=+1@example.com;user=dialstring SIP/2.0

INVITE sip:112@example.com SIP/2.0

NOTE Even if service URNs are not used in the SIP Request-URI, service URNs are needed for routing an emergency call to an appropriate SAP (see 6.3).

A UA that provides the user with an explicit means of initiating an emergency call can place the appropriate service URN in the request line of the INVITE request. When the user keys an emergency dial string, a UA with dial plan information may be able to detect that this is an emergency call and include the appropriate service URN in the request line of the INVITE request. Otherwise, the UA will have to place the dial string in the request line of the INVITE request and rely on a SIP intermediary to detect that this is an emergency call and take appropriate action. The SIP intermediary may then substitute the appropriate service URN for the dial string when forwarding the INVITE request, so that downstream entities will see that this is an emergency call without having to interpret a dial string.

NOTE A UA or SIP intermediary that merely forwards the dial string without recognising that this is an emergency call might fail to meet other requirements for emergency calls, such as provision of location information and ensuring appropriate resources are available.

In the case of a nomadic or mobile device, it is important that the UA be able to detect an emergency call initiated using the local dial string of the visited country or region when roaming. The configured dial plan might include some additional dial strings used in other countries or regions, but in general this cannot be assumed. Alternatively a UA can obtain the local dial string for emergency calls by interrogating a Location-to-Service Translation (LoST) server (see 6.3). If the local dial string for emergency calls conflicts with other strings in the normal dial plan, the emergency dial string should take precedence. Detection of an emergency call at the UA is essential if such calls are to be treated differently, e.g., by routing directly to a PSAP or via a public network (see clause 9).

Where an enterprise network routes an emergency call to a public network, if the public network is accessed by SIP it may prefer or require to receive a service URN in the request line rather than a dial string. This would always be the case for an IMS-based NGN. However, if a dial string is sent to a public network using SIP or to a TDM-based network, the enterprise network should still recognise the call as an emergency call in order to handle it correctly (provided any enterprise-specific dial string has been converted to that expected by the

public network). A service URN could be used for routing through the enterprise network, and then translated to an appropriate dial string for forwarding to the other network.

Figure 5 shows an example where the user enters a dial string and there is no dial plan interpretation in the UA, and therefore the string is transmitted to the first SIP intermediary in the enterprise network. This translates the string to a service URN and routes to a public network with the service URN in the INVITE request. The public network uses this to route to a PSAP.

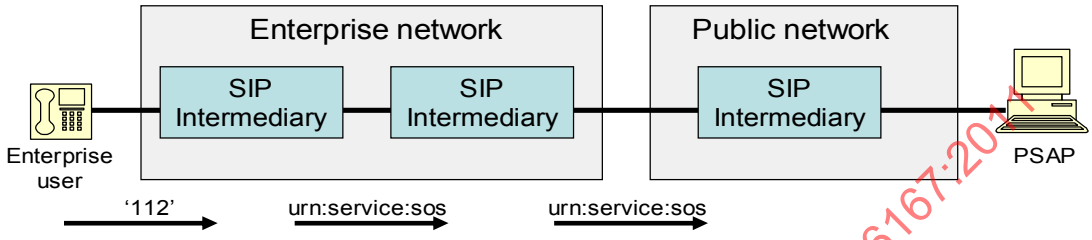

Figure 5 — Example of an emergency call starting with a dial string and submitting a service URN to a public network

Figure 6 shows an example where the calling UA submits a service URN, having interpreted a dial string. The enterprise network uses this to route to a PEAP.

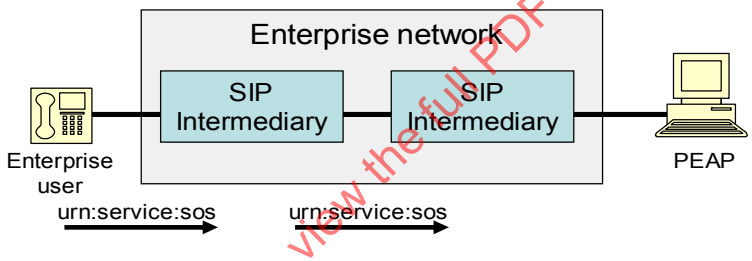

Figure 6 — Example of an emergency call using a service URN

Figure 7 shows an example where the calling UA submits a service URN, which is translated to a dial string for routing to a TDM network and onwards to the SAP.

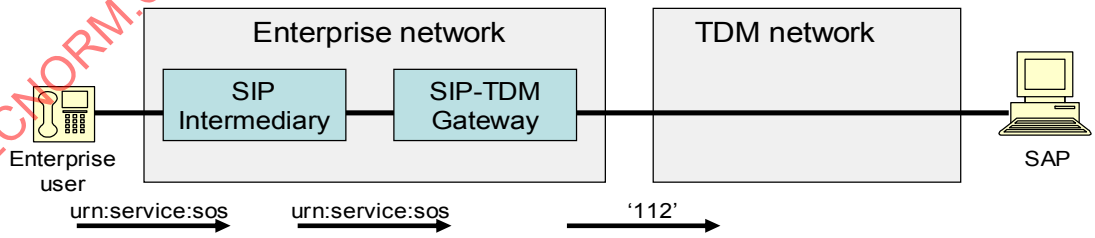

Figure 7 — Example of an emergency call starting with a service URN and submitting a dial string to a TDM network

When a user initiates an emergency call from an application separated from the SIP UA, that application will need to communicate the desire to make the emergency call to the SIP UA or some other SIP entity such as a Back-to-Back User Agent (B2BUA). One means for doing this is Computer Supported Telecommunications Applications (CSTA) [2].

6.1.3 Unauthenticated access

Regulations in some countries might require a public network to handle emergency calls from devices that have not undergone the authentication necessary for access to other telecommunications services. This capability may also depend on network policy. It may also depend on factors such as whether a device is fitted with a Subscriber Identity Module (SIM), even though the SIM does not have the correct credentials for the network concerned. Such calls would be treated as having an anonymous caller. The device concerned would either not be registered or would need to undergo an emergency (unauthenticated) registration. It is unclear whether such regulations would apply also to NGCNs, requiring NGCNs to provide unauthenticated access for the purpose of making emergency calls. The following situations can arise.

1. A device is not allowed access to the NGCN transport infrastructure (e.g., LAN or Wireless LAN (WLAN)), either because it does not have the appropriate credentials or because it is otherwise deemed insecure (e.g., lacking the appropriate operating system patches or lacking up-to-date anti-virus software). It would be exceedingly difficult to accept such a device onto the transport infrastructure and limit its use to emergency calls, without risk of compromising the infrastructure.

2. A device has access to the NGCN transport infrastructure but lacks credentials for authenticated registration with the NGCN SIP registrar. This could be because the device has not been configured, has an obsolete configuration, or requires the user to supply credentials before use (e.g., a phone at a hot desk). For such cases, NGCNs may need to make provision for an unauthenticated device to establish an emergency call. This may require that the device first perform an emergency (unauthenticated) registration, in order to assign a temporary identifier to facilitate return calls. See also 6.7 for security considerations.

RECOMMENDATION 3: Enterprise networks should make provision for emergency calls to be made from unregistered phones such as hot desk phones that have not been activated with a user's credentials, if required by enterprise policy.

3. A device has access to the NGCN transport infrastructure and is registered with the NGCN SIP registrar, but its user interface is locked to prevent unauthorised use. Devices capable of establishing audio calls should have an override facility to allow emergency calls to be made (and return calls to be answered) without unlocking the remainder of the user interface. However, this might not be feasible with general purpose devices (e.g., personal computers), where the locking mechanism is part of the operating system rather than part of the SIP application. See also 6.8.2 on guest users.

6.2 Obtaining and delivering the location of the caller

The location of the caller plays a vital role in emergency calling. First, the choice of SAP is likely to depend on the caller's location, in particular when the call is to be routed to a PSAP. Routing to the wrong SAP, because of missing or inaccurate location information, can lead to significant delays in dispatching assistance. Therefore SIP entities need location information in order to route correctly. Secondly, the SAP needs accurate location information in order to send assistance to the right place. Therefore a SIP entity that routes a call to a PSAP needs to deliver location information to that PSAP. Often the second purpose requires more precise information than the first purpose. Any error or inaccuracy in the location information provided can lead to delays in reaching the correct SAP or dispatching assistance to the correct location.

Automatically obtaining and delivering accurate location information is the core issue to be solved for emergency calling in enterprise networks. Users are no longer constrained to being in the same building or on the same campus as the PBX, but in principle can be connected to the enterprise network from anywhere in the world.

A comprehensive analysis of location information standards for use in the context of emergency call support and their use in an NGN context is available in [31] from ETSI TISPAN. This also contains information on the regulatory and deployment situation in various countries and regions in the world. In [32], ETSI TISPAN makes a recommendation to model the provision of location information in support of emergency services in NGN on existing 3GPP and IMS standards. This places the emphasis on network-provision, rather than terminal-provision, of location, and therefore differs in this respect from the NENA approach, which is based more closely on IETF protocols. Notwithstanding this, an NGCN that submits emergency calls to an NGN

would still be required to supply the caller's location information, and therefore in this respect the differences between the NENA/IETF and 3GPP/TISPAN approaches are unimportant. However, there will be impact when an enterprise device uses an NGN or 3GPP network for accessing the enterprise network, and such cases are discussed below and also in clause 9.

6.2.1 Format of location information

The IETF has defined a data format for a location object, specifying the location of an entity. Based on the Presence Information Data Format (PIDF) [10], the Location Object (PIDF-LO) [11][19] can contain either a geospatial location or a civic location. The format for a civic location is updated in [16]. A geospatial location can simply specify the location of a point (latitude, longitude and optionally altitude) or more complex features, but for the purposes of emergency calls a point should be sufficient. A civic location can contain conventional street address information, plus building number, room number, floor number etc.. For larger structures, the identification of an interior location (e.g., floor, room, cubicle) is generally important.

Although database look-up can be used to convert between geospatial and civic and vice versa, for emergency call purposes it is preferred that the original format be used as the basis for routing and delivered to the SAP, rather than attempting conversion and increasing the risk of error.

6.2.2 Obtaining location information for delivery

This topic is discussed extensively in [20], and therefore below is just a summary along with enterprise-specific considerations.

6.2.2.1 Where location information is obtained

According to [20], caller location information should be obtained by a SIP entity topologically as close to the source of the call as possible and passed on by any downstream SIP intermediaries. Ideally the calling device (the SIP UA) should obtain this information, but if it is unable to do so or if it does not recognise the call as an emergency call, a SIP intermediary topologically as close as possible to the UA (e.g., the outbound proxy) should obtain the information, since SIP entities further downstream are less likely to have access to accurate information. In principle a device can include location information with all calls and would not need to recognise an emergency call, but for privacy reasons this is unlikely to be acceptable. For calls originating in a TDM part of the enterprise network, the gateway acting as SIP UA should ideally obtain location information.

6.2.2.2 How a device obtains location information

There are basically four ways for a device to obtain its location:

- by manual configuration;
- by means of an integral location measurement mechanism;
- as a service from the access network;
- by means of a location configuration protocol (LCP).

6.2.2.2.1 Manual configuration of a device

Although suitable for a device that remains in a single location, manual configuration is unlikely to be suitable for wireless devices or for wired devices that frequently move between parts of a network or between networks. It is also subject to error, either through failure to re-configure when the device is moved or through supplying invalid, wrong or inaccurate information. Being prone to error is particularly the case if configuration is left to the user, rather than being controlled by enterprise administration. Manual configuration is a good fall-back for cases where automatic location determination is not available or would give misleading data (e.g., when the user is a relatively long distance from a wireless network's wired access point whose location is determined automatically). Also a user can use manual configuration to override information obtained by other means when known to be inaccurate. In this situation there may be justification for providing both locations for

routing and delivery purposes. See 6.2.2.5 for considerations concerning the provision of multiple locations. Manual configuration can be acceptable if the user is likely to be in the same place for a long time (e.g., a home worker). The user should configure location on arrival, and not wait until an emergency arises.

It is also possible that a device obtains its information from an external application that has obtained it by some means (e.g., manual configuration) and delivered it to the device somehow (e.g., via CSTA). The device can treat this as manually configured information.

6.2.2.2.2 Integral location measurement

A common integral location measurement mechanism involves the use of satellites, e.g., the global positioning system (GPS) or the European Galileo system. Such capabilities are generally provided only on mobile devices and are not available or not reliable in many buildings or underground. Also the time taken to obtain a measurement from a cold start (time to first fix) may be prohibitively long, but on the other hand battery considerations on mobile devices might prevent the system being kept permanently active.

A wireless device (e.g., WLAN, cellular, Bluetooth) may also be able to employ timing techniques, with or without the use of triangulation, in order to obtain its rough position or locus of possible positions relative to access points. Unfortunately such information is of no use for emergency calling without access to access point mapping information. In general this is unlikely to be available from cellular, Generic Access Network (GAN) or hotspot operators, although it might be a possibility for access points within the enterprise. No standards are available for dealing with information on position relative to access points. For example, if a device could convey this information in SIP, a SIP intermediary in the enterprise network might have access to building plans, from which it could derive a civic location including building, room and floor.

STANDARDISATION GAP 2. There is no standardised means of conveying information on position relative to access points in SIP.

6.2.2.2.3 Location configuration protocols

LCPs allow a device to obtain its location from the access network, based on pre-configured wiring information, which needs to be maintained manually when fixed wiring or wireless access points are moved. For wireless devices this information might be augmented with information about the device location, as obtained by triangulation. Protocols available include:

- Dynamic Host Configuration Protocol (DHCP);
- Link Layer Discovery Protocol (LLDP);
- HTTP Enabled Location Delivery (HELD);
- Location as a service from the access network (see 6.2.2.2.4);
- Proprietary protocols.

DHCP can provide location either civic location [13] or geospatial location [7]. LLDP [4] with Media Endpoint Device extensions [3] can provide either civic or geospatial location. These protocols provide location in a similar format, which can easily be converted to PIDF-LO format. Both DHCP and LLDP-MED are based on layer 2 mechanisms and do not use the IP address of the device as input to the database look-up.

HELD [22] is an Hyper-Text Transfer Protocol (HTTP)-based mechanism for interrogating a Location Information Service (LIS) to obtain location information in PIDF-LO civic or geospatial format. The LIS uses the source IP address of the HTTP request as input to the database look-up, and therefore can provide misleading information where the device is behind a Network Address Translator (NAT) or VPN. HELD can provide location by reference (LbyR) (see 6.2.3) as an alternative to location by value (LbyV). When using HELD, the client can specify whether the purpose is for emergency routing (requiring a faster response but coarser accuracy) or emergency dispatch (requiring greater accuracy). A DHCP option [23] can provide a URI for a LIS.

HELD has the advantage over DHCP and LLDP that it is readily available to an application on any operating system. General purpose operating systems, such as used on PCs, might not provide access to these link level functions.

Sometimes a device can obtain its location by means of a proprietary protocol, e.g., from a proprietary configuration server.

An LCP is frequently the best solution for use within buildings, being more accurate than GPS, more dependable than GPS, and faster from a cold start.

RECOMMENDATION 4: Enterprise networks should make provision for devices directly attached to the enterprise network to obtain their best effort location using a suitable LCP.

6.2.2.2.4 Location as a service from the access network

Access networks can determine a device's rough location by timing / triangulation techniques and make this available to the device as a service. With a technology known as Assisted GPS (A-GPS), a cellular access network can provide rough location to the device and then, if the device has an integral GPS capability, the device can submit a GPS-derived location to the access network. From this and its own information, the access network derives a more accurate location and downloads it to the device. A-GPS also has the ability to reduce the cold start time for GPS, since the rough initial location from A-GPS can be used until a satellite fix is obtained. The rough location can also be used indoors or underground, where GPS does not work.

A rough location provided by an access network, in the absence of GPS, is generally sufficient for routing to an appropriate SAP, although not ideal for submitting to the SAP for dispatching assistance. If GPS measurements are available later in the call, a more accurate location can be transmitted to the SAP.

Such techniques do not in general provide altitude or the floor of a building.

Normally there will be a flat-rate charge for such services. If the service is not needed for business-related purposes, enterprises might be reluctant to pay.

6.2.2.3 When to obtain location information

For a UA to obtain location information when it detects that an emergency call is being made can be problematic, either because it takes too long or because the LCP server is temporarily not available. Therefore, except in the case of manual configuration, the UA should attempt to obtain location information on start-up and refresh it periodically. The frequency of refresh will be subject to considerations such as whether the device is relatively fixed, load on the server and impact on the battery. When an emergency call is attempted, the device should attempt to refresh the location information, but should not delay call establishment unduly. For routing purposes (selection of an appropriate SAP), location information does not need to be so accurate, so a small movement of the device since the last refresh might not matter. However, for dispatching assistance, the information needs to be as accurate as possible, so if the call is established before updated location information is available, the updated information should be submitted during the call.

6.2.2.4 Obtaining location information at a SIP intermediary

Where a SIP intermediary close to the caller needs to obtain location information for an emergency call (in the absence of information from the SIP UA), it can often do so by reference to a local database (e.g., based on wiring information), for example using the IP address of the SIP UA as index. There are no standards for this. In many situations this will yield sufficiently accurate location information, but not in the case of nomadic or mobile devices, which should supply their own location information. If information is not available about the location of the particular device, the SIP intermediary may have to insert default location information for the enterprise site, although this could be extremely inaccurate in the case of a remote device. Likewise, if the NGCN routes an emergency call to a public network without caller location information, the public network would have to use default location information for the NGCN, which again is likely to be inaccurate in the case of large campuses, multi-site NGCNs and roaming devices.

If location information is already supplied by the SIP UA, it is questionable whether a SIP intermediary should also provide location information, in addition to or as a replacement for UA-supplied location information. Generally replacing information provided by the UA is bad, because UA-provided information is likely to be more accurate. See 6.2.2.5 for considerations concerning the provision of multiple locations.

RECOMMENDATION 5: Enterprise networks should make provision for SIP intermediaries to obtain the best effort location of a device on behalf of any device that is unable to provide this information.

6.2.2.5 Providing location information from multiple sources

In some circumstances there may be more than one source of location information available, e.g., obtained by the calling device from different sources, or location information obtained by the SIP UA and location information obtained by a SIP intermediary. Providing location information from multiple sources is not necessarily helpful, because it is not clear which to use for routing or for dispatching assistance. On the other hand, location information from a second source can provide a fallback if location information from one source turns out to be false. It should therefore be left as an enterprise policy matter, although this may be influenced by regulatory considerations. However, see also 6.2.3 concerning location conveyance in SIP.

6.2.2.6 Use cases for obtaining location information

Of the variety of methods available for obtaining location information, the most appropriate will depend on the particular type of device and circumstances. In general a device should be able to discover what means are available for obtaining location in a given situation, although in some cases a device might need to be configured specially (e.g., to provide a manually-configured location).

6.2.2.6.1 Desk phone on enterprise fixed LAN

For a desk phone on an enterprise fixed LAN, an LCP is generally the best approach. There is little to choose between the different standardised LCPs (DHCP, LLDP-MED and HELD), except that HELD could be problematic when there is a NAT between the device and the HELD server, in which case the location given will be based on the IP address of the NAT, rather than the device, and generally this will be wrong or insufficiently accurate.

The device should obtain its location on start-up, and if possible should cache it across start-ups in case the location server is not available. When an emergency call is made, a refresh attempt could be made, but this should not be allowed to delay call establishment.

Manual configuration is also sufficient for this situation, provided reconfiguration occurs during office moves.

Similar considerations apply to a soft phone on a desktop PC connected to a fixed LAN.

6.2.2.6.2 Desk phone on enterprise WLAN

For a desk phone (or soft phone on a desktop PC) connected to an enterprise WLAN, considerations are similar to those for a desk phone on an enterprise fixed LAN (see 6.2.2.6.1), provided the coverage area of the WLAN access point is fairly small. Otherwise considerations are as for a hand-held phone on an enterprise WLAN (see 6.2.2.6.3).

6.2.2.6.3 Hand held phone on enterprise WLAN

Where each WLAN access point has a sufficiently small coverage area, an LCP can be sufficient, since it should reveal the location of the access point being used. However, in addition to obtaining location on start-up, it is important that the device attempt to refresh its location when moving between access points and when establishing an emergency call.

Because GPS does not work well indoors and A-GPS is not available on WLANs, the only solution for obtaining a more accurate location than that available from an LCP would be for the device to measure its

position relative to access points, as described in 6.2.2.2.2. However, frequently the access point location is sufficient.

Manual configuration is generally unsuitable.

6.2.2.6.4 Home worker's desk or hand held phone

This includes soft phones on laptop and desktop PCs, as well as hand held devices. Connection to residential broadband access is by fixed LAN or WLAN. Generally the location of the residence is sufficient, and this might be obtainable using an LCP. However, if the broadband access provider does not support an LCP, manual configuration would have to suffice.

If emergency calls are made directly to a public network, rather than via the enterprise network, there are no enterprise considerations (see clause 9).

6.2.2.6.5 Mobile or nomadic device at a hotel, hotspot, etc.

This includes soft phones on laptop PCs, as well as hand held devices. Connection is to a fixed LAN or WLAN. The device needs to be able to use any standardised LCP to obtain its location, unless it is able to use integrated measurement techniques. As a fallback, manual configuration may be required.

If emergency calls are made directly to a public network, rather than via the enterprise network, there are no enterprise considerations (see clause 9).

6.2.2.6.6 Mobile device on PLMN

This generally applies to hand held devices. If the device does not have GPS available, A-GPS or other triangulation-based services can provide a rough location. If the device has GPS available, a more accurate location can be obtained (but probably only after a delay). With both GPS and A-GPS a yet more accurate location can be obtained (again perhaps subject to delay). It is not anticipated that an LCP will be available. As a fallback, manual configuration may be required, but this is only suitable while stationary for a while in a known location.

If emergency calls are made directly to a public network, rather than via the enterprise network, there are no enterprise considerations (see clause 9).

6.2.2.6.7 Dual mode mobile devices

Dual mode mobile devices are able to access WLAN, when available, or a cellular network at other times. WLAN can give cost and/or performance benefits. When accessing a cellular network, the considerations of 6.2.2.6.6 apply. When accessing a WLAN for normal traffic, it might be beneficial to use the cellular network for emergency calls, particularly if the device does not have GPS, because of the cellular network's internal ability to determine position with sufficient accuracy. Also the cellular network may give greater robustness if the caller moves during the call. If emergency calls are made via the WLAN, however, the considerations of 6.2.2.6.3, 6.2.2.6.4 or 6.2.2.6.5 apply. Note that dual mode phones that require a user to use a different dial plan, depending on which network is being used, might have undesirable consequences for a user establishing an emergency call.

6.2.2.6.8 Legacy phone connected via gateway to enterprise fixed LAN

For a legacy phone (including, for example, an analogue or ISDN phone, or a DECT or Bluetooth class 1 device) connected via a gateway (adaptor) to the enterprise fixed LAN, the device itself will not be able to supply its location, but the gateway, acting as UA, should be able to obtain its own location by manual configuration or via an LCP. The accuracy of this location information will depend on how distant the phone is from the gateway.

6.2.3 Location conveyance in SIP

Having obtained the caller's location, the information needs to be conveyed to the SAP, and also needs to be made available to intermediaries that can make use of it for routing the call towards the correct SAP. For calls established using SIP, this means conveying location information in the SIP INVITE request, so that it is available to SIP intermediaries for routing purposes and is delivered to the SAP. Where the SAP is reachable only by TDM, the gateway will need to convert from SIP to some other format for delivery to the SAP (e.g., DTMF tones).

A location can be conveyed in SIP using the Geolocation header field, as specified in [25]. Using this mechanism, an entity that has obtained the caller's location (the UA or a SIP intermediary) can insert it into the SIP INVITE request.

A location can be conveyed in SIP either by value (LbyV, in which the Geolocation header field points to a body part containing the PIDF-LO) or by reference (LbyR), in which the Geolocation header field contains a URI that, when dereferenced, will provide an authorised entity with the PIDF-LO). For LbyR, a presence server must be provided and the URI scheme must be SIP, SIPS [5] or PRES [8], the last of these resolving either to a SIP or SIPS URI or to some other URI scheme. The SIP SUBSCRIBE method [6] and the presence event package [9] are used for dereferencing a SIP or SIPS URI. It is important that the referenced resource be reachable from the SAP (e.g., not blocked by firewalls or NATs).

The HELD protocol is able to provide a location by reference. Compared with LbyV, LbyR leads to a more compact SIP message, and also has the advantage that more up-to-date information may be available at the time of dereferencing. Also there is no need to send refreshes via SIP since the SAP can dereference at intervals (within the lifetime of the URI) to obtain changed or more accurate information or, if the dereferencing protocol is SIP, the SAP will receive NOTIFY requests when a location changes, as long as the subscription is kept alive. However, for an emergency call, where location is needed by SIP intermediaries for routing purposes, as well as by the SAP, dereferencing can add delays and can also be a point of failure. Moreover, the server has to be reachable from any entity that needs the location information, e.g., a SIP intermediary in a public network or a PSAP.

With these considerations in mind, there does not seem to be a compelling case for using LbyR in enterprise networks for emergency calls.

RECOMMENDATION 6: Enterprise networks should use LbyV for location conveyance in SIP for emergency calls.

According to [25], it is recommended that a SIP message should convey only a single location. Therefore if a SIP intermediary is able to provide a location and there is already a location present from an upstream entity (e.g., the SIP UA), it is a matter of policy which location to pass forward in the SIP request and use for routing.

During an emergency call, the calling UA can submit a location refresh using a SIP UPDATE or re-INVITE request. This can convey changed or more accurate location by value.

6.3 Routing an emergency call to the appropriate SAP

Given a service name in the form of a service URN and a location in the form of a PIDF-LO, the Location-to-Service Translation (LoST) protocol [17] provides a means to query a server to obtain the URI of an appropriate PSAP. A DHCP option [18] provides a means of discovering a LoST server. The result of a successful query, in addition to containing the PSAP URI, will indicate the services available from that PSAP, the extent of the service area for that PSAP (so that a client knows whether to query again when the location changes), and the special dial string used in the geographic area concerned. A server that is not responsible for the location concerned can either forward the request or redirect the client to another LoST server.

For example, if a roaming user connected via a VPN tunnel to an NGCN supplies a location for country A, and the NGCN based in country B uses a LoST server for country B, the expectation is that the LoST query would be redirected or forwarded to a LoST server for country A.

In an enterprise network, emergency calls may need to go to a PEAP rather than to a PSAP. Conceivably an enterprise could set up its own LoST server, such that it would return the URI of a PEAP if appropriate. The enterprise LoST server could interrogate a public LoST server if there is no PEAP for the location concerned, or it could redirect the client to a public LoST server. The enterprise LoST server would need to reflect enterprise policy, such as any restricted hours of operation for PEAPs. Alternatively proprietary means could be used for routing to a PEAP.

RECOMMENDATION 7: Enterprise networks should make provision for accessing a public LoST server for routing or, if PEAPs are to be used, provide a private LoST server or equivalent means of achieving routing.

The URI obtained from the LoST server (or by other means) is placed in the Route header field of the SIP INVITE request (the service URN being in the Request-URI field) and normal SIP routing applies from that point onwards.

In the event of failure to obtain a URI (e.g., unable to discover a LoST server, unable to access a LoST server, no location available or no URI available for the location concerned), the enterprise network should fall back to routing the call to a default destination, which could, for example, be a TDM destination. In multi-location enterprise networks, one of multiple default TDM destinations should be selected based on the caller's location, when possible.

RECOMMENDATION 8: Enterprise networks should provide a default route for emergency calls for use when unable to contact a LoST server.

6.3.1 Routing by the calling device

According to [20] and [21], the calling device should obtain the URI of a LoST server at start-up time and then perform a LoST lookup and cache the result, for use in the event of an emergency call. Also, by cacheing the returned local dial string, emergency calls using the local dial string, as opposed to any pre-configured dial strings, can be recognised.

The address of a LoST server can be discovered using DHCP, by manual configuration, or by Domain Name System (DNS) using Service (SRV) records.

Information obtained from the LoST server should be refreshed periodically or if the device is known to have moved outside the service area of the selected SAP. Information returned by the LoST server includes a time to live and the boundary of the service area.

In the event of an emergency call, the cached routing URI can be used if the LoST server is not available at the time or if a further interrogation takes too long. If no routing URI is available, the device can simply omit this from the Route header field and leave it to a SIP intermediary to route to a SAP.

It is debatable whether the use of LoST by an enterprise device is appropriate. Advantages of a device using LoST include:

- the device can see if a civic location is invalid and seek correction from the user;
- the device can make use of the local dial string delivered by LoST;
- any device compliant with [21] will attempt to do it anyway (although will give up if it can't discover a LoST server);
- the device can use cached information.

Concerning the last point, a SIP intermediary may also be able to use cached information, but in a different way (see 6.3.2).

Possible disadvantages are as follows:

- enforcement of enterprise policy on choice of SAP might better be performed at an enterprise SIP intermediary;
- enterprise policy on use of PEAPs would need to be reflected by making an enterprise LoST server available to the device, whereas a SIP intermediary could use other solutions;
- the impact of periodic LoST information refreshes on batteries.

RECOMMENDATION 9: Enterprise networks should allow policy to govern whether devices are allowed to contact a LoST server rather than leaving this as a task for SIP intermediaries in the enterprise network.

Additional considerations for mobile and nomadic users are given in clause 9.

6.3.2 Routing by enterprise SIP intermediary

In the absence of routing information inserted by the calling device (SIP UA), an enterprise SIP intermediary, having recognised an emergency call by explicit signalling (service URN) or by dial string, needs to perform routing. Three circumstances can lead to this:

- the device has not recognised the dial string but the SIP intermediary does so;
- the device has recognised the dial string and placed a service URN in the Request-URI field, but has failed to supply a location in the Geolocation header field;
- the device has recognised the dial string and supplied its location, but has failed to supply a valid URI for the SAP in the Route header field.

Even if the device has performed routing, the enterprise SIP intermediary could override this. One possibility is that the device has used a public LoST server (which fails to take account of enterprise policy) and the SIP intermediary needs to assert enterprise policy.

An enterprise SIP intermediary needs to choose whether to route to a PEAP (and if so, which one) or to a particular PSAP. It can do this either by reference to an enterprise LoST server or by reference to locally configured information.

A call will need to be routed to a PSAP under any of the following circumstances:

- there are no PEAPs for answering the emergency service concerned;
- there are no PEAPs available at this particular time of day; or
- there is no PEAP serving the calling device's location (e.g., because caller is off-premises or because the site concerned is not covered by a PEAP).

In these circumstances, the enterprise SIP intermediary can either route the call to a public network (without attempting to route to a particular PSAP) or can use LoST, or locally configured information, to identity a PSAP and use normal routing. That routing may be via a public network or via a direct SIP connection from the enterprise to the PSAP in accordance with a peering arrangement. Where an enterprise LoST server is used, a single interrogation could provide a URI for either a PEAP or a PSAP. The choice of whether to route directly to a PSAP or via a public network may depend on local regulation. Also, some countries might not allow a public network to route an emergency call from a caller outside that country, in which case it might be essential for the NGCN to route directly to the PSAP or via a public network in the country of origin.

An enterprise SIP intermediary can cache information it receives from a LoST request, since this may be of use for future emergency calls from callers within the service area indicated within the cached information. In

fact, an enterprise SIP intermediary could, on start-up and at intervals, perform LoST queries for the locations it serves and cache the results. Then it would only need to perform further LoST queries for emergency callers outside the locations it serves (e.g., mobile or nomadic users).

6.4 Delivering information to the SAP to allow a return call or verification call to be made

Whilst delivery of location information to the SAP allows assistance to be dispatched, delivery of information identifying the calling device is generally required in order to facilitate the establishment of a return call. A return call from the SAP or ECC may be needed if the emergency call is disconnected prematurely (e.g., because of a fault, because of a misunderstanding, or because the caller accidentally presses the disconnect button, see also 6.6). It may also be needed if the SAP or ECC operator discovers that more information is needed from the caller, e.g., if the delivered location information turns out to be invalid. The need for a return call is typically only in the first hour (say) following the emergency call, although local regulations vary.

Information delivered for facilitating a return call can also facilitate a verification call.

In addition, identification of the calling user or device may be used for deriving location information, if this is not otherwise available or if legacy equipment is unable to make use of the location information provided.

6.4.1 Delivery of caller identification

SIP allows caller identification (i.e., the Address Of Record, AOR, of the caller) to be delivered using the From and/or PAI header fields. For a call to a PSAP, the NGCN should provide caller identification, rather than relying on the default for the NGCN inserted by a public network. The default is likely to be insufficiently accurate, although the public network may deliver that in addition. Any privacy considerations that normally would suppress caller identification should be overridden for emergency calls. Since an AOR has a long lifetime, caller identification can be useful for establishing a return call when specific device identification is not available or is no longer valid. However, when a call is made from an unauthenticated or unregistered device, caller identification might not be possible unless a temporary identifier has been assigned (e.g., during an emergency registration process). Such an identifier is effectively a device identifier and is likely to have a finite lifetime.

RECOMMENDATION 10: Enterprise networks should deliver caller identification with emergency calls if possible, overriding any restrictions that apply to normal calls.

6.4.2 Delivery of device identification

Normal caller identification does not identify the particular device in the case where several devices are registered against the same AOR. To cater for this, device identification needs to be delivered and used as the preferred destination for the return call. The SIP contact URI is the means to achieve this. For this purpose the contact URI needs to be globally routable and have a lifetime that extends sufficiently beyond the end of the original call (subject to the device not disconnecting within that time). Frequently devices are unable to provide globally routable contact URIs themselves, but can obtain them from the SIP registrar using the Globally Routable UA URI (GRUU) mechanism specified in [24]. Alternatively the local SIP intermediary can map a local contact URI to a globally routable contact URI. Provision of a temporary globally routable contact URI is required particularly for unauthenticated devices if no caller identification is available.

RECOMMENDATION 11: Enterprise networks should provide sufficient information to allow a return call to be made to the same device, where possible.

If a return call to the delivered device identifier fails, the SAP or ECC can attempt a return call based on caller identification, if available.

6.4.3 Identifying a return call or verification call

Although an authority-to-citizen call, a return call is closely related to an emergency call and therefore worthy of brief consideration. An NGCN SIP intermediary or a device may need to recognise a call as a return call from a SAP or ECC for the following purposes:

- call admission control purposes (e.g., to override the barring of incoming calls to an unauthenticated device, or to override any policy concerning calls directly to the device rather than to the user's address of record);
- to ensure the override of incoming call features (e.g., do not disturb, call forwarding);
- to allow the interruption of another call occupying the device or other resources;
- to ensure other considerations to do with unauthenticated devices are taken into account (e.g., their inability to authenticate a BYE request).

One means of identifying a return call might be to remember the remote contact URI from the emergency call and match that with the remote contact URI of an incoming call. However, this may fail because other SIP intermediaries map contact URIs, or because the return call originates from a different device at the SAP or ECC.

Another approach might be to ensure that connected identification is provided on the original call and that this be matched with caller identification on an incoming call, although it is not clear this would work when the return call comes from an ECC rather than the SAP.

Similar considerations apply to verification calls, with the additional issue of correlating a verification call with an earlier emergency call.

STANDARDISATION GAP 3. There is currently no reliable means (in SIP or in IMS) of identifying a return or verification call from a SAP or ECC and correlating a verification call with an earlier emergency call.

6.5 Ensuring appropriate resources are available for an emergency call, return call or verification call

NGCNs may need to make special provision for ensuring that appropriate resources are available for emergency calls, including return calls and verification calls.

The possible need to allow access by unauthenticated and/or unregistered UAs for the purpose of making an emergency call and receiving a return call is already discussed in 6.1.3.

When an emergency call is requested, an NGCN may need to override normal call admission control procedures, for example:

- by admitting calls from users with no authority to make calls to public networks;
- by allowing a user access to media transport resources not normally available to the user (e.g., additional bandwidth to avoid using a compressed audio codec).

Where appropriate resources are occupied by other (non-emergency) calls, not necessarily involving this same user, it might be necessary to clear down an existing (non-emergency) call or reduce its capabilities, in order to make resources available to an emergency call, including a return call or verification call. Examples of situations where this might apply include:

- all available bandwidth on a route is occupied by other calls (some of which are non-emergency);
- all trunks at a PSTN/ISDN access are occupied by other calls (some of which are non-emergency).

Some NGCNs may deploy a more general purpose resource priority mechanism, support for which in SIP is specified in [12]. This can ensure that higher priority calls can receive the resources they need at the expense of lower priority calls. Where such a scheme is deployed, emergency calls can be given a relatively high priority. Where such a mechanism is not deployed, NGCNs will at least need to mark emergency calls as such for the duration of the call, so that they are not inadvertently cleared to make room for other emergency calls.

Where PEAP resources are not available, the NGCN may have a policy of forwarding emergency calls to a PSAP instead.

As mentioned in 6.4.3, return calls and verification calls might also need to be given priority treatment.

More details on this topic, as it applies to NGN, are given in [34]. Brief prioritisation requirements for Europe are given in [29].

6.6 Ensuring appropriate media quality during an emergency call

Media quality is important during an emergency call, including a return call or verification call, because the caller and answerer need to understand each other clearly and in a timely manner. In the case of voice, this means clear and uninterrupted speech in both directions, thereby avoiding the need for one party to ask the other party to repeat a statement or question.

This can be partly addressed by providing appropriate network resources (e.g., bandwidth) to an emergency call, as discussed in 6.5. There are also certain measures that a calling device can take to help ensure good quality, assuming the device is aware that a call is an emergency call.

By offering only good quality audio codecs, the distortion introduced by some compressed codecs can be avoided. G.711 should be sufficient and will almost certainly be accepted by any SAP.

Voice activity detection, whereby packets are not transmitted during periods of "silence", can be harmful, since it may cause meaningful sound signals to be dropped. For example, the answerer may be able use background noise to judge the circumstances at the scene of the emergency, or the caller might need to talk in a whisper. In either case, sounds below the threshold will be dropped if voice activity detection is used.

Some authorities mandate or recommend that a user should not be allowed to place a call on hold during an emergency call. This is a legacy from the days of TDM. For a SIP device, hold means stopping transmission and reception of media, which can be achieved in a number of ways, e.g., pressing a special call hold button, performing hold implicitly in the context of some other feature such as call transfer or conference, or turning down the speaker volume and/or muting the microphone (or simply covering them). Although the requirement is well-intended (i.e., to guard against accidental use of hold), it can also be harmful (e.g., by preventing a user using normal capabilities of the device for a sensible purpose during an emergency. Also some devices may be unable to prevent hold (for example, in the case of a standard TDM phone plugged into a SIP terminal adaptor, the SIP terminal adaptor is unlikely to have any control over the phone's microphone and speaker).

Some authorities mandate or recommend that a user should not be allowed to disconnect an emergency call until the call taker disconnects (premature disconnection). This too is a legacy from the days of TDM and SIP signalling does not provide a means of preventing premature disconnection. Moreover, prevention of premature disconnection can be harmful in some situations. For example if the caller cannot hear the call taker, it might be reasonable to disconnect the call and make a second call, hopefully this time by-passing any faulty equipment on the media path. If and how to deal with premature disconnection is still under discussion in the IETF.

Devices will be deployed in different jurisdictions with different requirements, particularly concerning call hold and premature disconnection. Mobile and nomadic devices will move between jurisdictions. In the absence of signalling to instruct a device how to behave during an emergency call, device designers will need to take sensible measures, taking into account particular designs of user interface, and hope that these measures will be acceptable in a wide range of jurisdictions.

Similar considerations apply to return calls and verification calls.

Different considerations will apply to other media, in particular in support of users with special needs, e.g., real-time text. Also other considerations will apply to automata, e.g., sensors that establish a call and transmit a recorded voice message, without the capacity to receive media.

6.7 Security considerations

Security in NGCNs is discussed in [1]. This focuses on session level security, both signalling security and media security.

Concerning signalling security, for emergency calls ideally all signalling hops should be secured using Transport Layer Security (TLS). This is particularly important since location is conveyed by value in SIP messages. However, it is even more important for an emergency call to succeed, and therefore if it is not possible to use TLS on a particular hop, the call should be allowed to proceed on an unsecured transport. The SIPS URI scheme should not be used, since that would cause the call to fail if TLS is not available. For return calls and verification calls, the use of TLS on signalling hops would be desirable, but again the SIPS URI scheme should not be used.

In practice, emergency calls will probably use the same transport as any other call. In networks where TLS is used on all hops, emergency calls will enjoy the desired security. In networks where TLS is not used, emergency calls will most likely not use TLS. In particular, any delay in establishing a TLS connection specially for an emergency call might be undesirable.

In providing information to the SAP to allow a return call to be made, the mechanisms described in [1] can be used to provide authenticated identification of the caller, and likewise authenticated identification of the SAP for a return call or verification call. Any privacy policy associated with the caller that prevents the disclosure of caller identification to the called user should be overridden.

Concerning media security, although this might be desirable, it is important that an emergency call should succeed even if media security is not available. Also, if the use of media security involves increased call establishment times (for key negotiation, certificate validation, etc.), it is probably better not to use media security.

For LCPs, security will depend on the particular protocol used, but ideally the client should authenticate the server (to ensure it receives the correct information) and the server should authenticate the client (to ensure it does not divulge information to the wrong entity). Location information should be encrypted and integrity protected.

LoST should ideally use HTTPS (rather than HTTP) as transport, which will allow the client to authenticate the server (to ensure it receives the correct information) and will provide encryption and integrity protection of data.

Denial of Service (DoS) is an issue, since an excessive number of emergency calls could overload the SAP or network resources and thereby deny service to other emergency callers. Because of the requirement to allow easy access to emergency calls, prevention of DoS is difficult, although certain measures can be taken, for example:

- avoid including a SAP URI or emergency service URN in an exploder list;
- do not allow automatic forwarding to a SAP (except in the context of a SAP forwarding to another SAP).

There are risks in allowing unauthenticated devices to make emergency calls, since they can be used to mount DoS attacks. Different countries take different views on this, some allowing unauthenticated access and others not. Enterprises similarly may have different policies.

6.8 Other aspects

6.8.1 Hosted users

In a hosted enterprise environment, hosted users will need the ability to make emergency calls. By default, emergency calls might be handled in accordance with policy of the hosting infrastructure. For example, for a hosting NGN infrastructure, calls would be routed to the appropriate PSAP, although some enterprises might impose a different policy. Where normal public network dial strings for emergency calls conflict with the enterprise dial plan, different dial strings might be required.

6.8.2 Guest users

Guests on enterprise premises should be able to use enterprise devices to establish emergency calls. Devices that are able to be locked, to prevent normal use by unauthorised users, should allow emergency calls to be made without unlocking, as described in 6.1.3. Also it should be possible to answer return calls from SAPs without unlocking the device.

Some enterprises might provide facilities for guest users to attach their own devices (e.g., PCs) to the LAN or WLAN, typically using a guest VLAN or guest Service Set Identifier (SSID). Normally this provides guest users only with Internet access, without support for session-based services. Support for emergency calls might be limited to LoST server discovery and location discovery (e.g., via DHCP).

RECOMMENDATION 12: Enterprise networks should provide LoST server discovery and location discovery facilities on guest LANs.

7 NGN considerations

NGNs need to accept emergency calls from NGCNs destined for PSAPs.

NGCNs connect to NGNs in accordance with [33] using either subscription-based business trunking (in which case the NGCN attaches to the P-CSCF) or peering-based business trunking (in which case the NGCN attaches to the IBCF). The P-CSCF already has the capability for detecting emergency calls and invoking the E-CSCF to provide special handling. It is unclear whether the lack of corresponding functionality in the IBCF is an issue, or whether, for peering-based business trunking, the role of E-CSCF is always performed by the NGCN. At the time of publication of this Technical Report, this matter was being discussed in 3GPP SA2.

NGNs can be expected to recognise emergency calls when received across the NGCN-NGN interface as public network traffic. Recognition of emergency calls when received as private network traffic will depend on bilateral agreement.

Ideally emergency calls to PSAPs should be received with a service URN in the Request-URI, but dial strings could be used by mutual agreement **when using the subscription-based business trunking approach** [33].

REQUIREMENT 1: An NGN shall support emergency calls from an NGCN to a PSAP, such calls being identified by a service URN or, by mutual agreement when using the subscription-based business trunking approach [33]**, dial string.**

NGNs also need to accept emergency calls from NGCNs to PEAPs outside the enterprise network. These will need to be identified to the NGN as emergency calls if the NGN is to provide special capabilities (e.g., assignment of special resources, or transparent conveyance of location information). The means of identification will need to be subject to bilateral agreement and might be dependent on the availability of unique service URNs.

REQUIREMENT 2: An NGN shall support emergency calls from an NGCN to a PEAP.

NGNs should be capable of receiving location information from an NGCN in an INVITE request for an emergency call and in subsequent mid-dialog requests. This information should be passed on to the PSAP or PEAP and should not be overridden by (but may be supplemented by) location information available at the NGN concerning the NGCN site.

An NGCN can appear to an NGN as a User Equipment (UE) if connected by means of subscription-based business trunking. According to [28], an NGN may ignore location information received from a UE if it has obtained location information by other means. In the case of an NGCN as UE, it is important that the NGN does not ignore NGCN-provided location information, since the caller could be outside the premises known to the NGN.

REQUIREMENT 3: An NGN shall support the receipt of location information from an NGCN in the context of an emergency call from an NGCN, and not override with NGN-supplied location information.

NGNs should be capable of routing to a PSAP based on information already supplied by the NGCN in the Route header field. However, in the absence of this, or by mutual agreement, NGNs should be capable of determining the route to the appropriate PSAP, based on location information from the NGCN if available. In any case, an NGN can ignore information in the Route header field and perform its own LoST query to determine the route.

REQUIREMENT 4: An NGN shall be able to route an emergency call from an NGCN to a PSAP based on information supplied by the NGCN.

An NGN can sometimes return a 3xx response to an INVITE request for an emergency call, requesting redirection to the circuit-switched domain or a different IP connection. It is assumed that this would be suppressed (e.g., by configuration) for business trunking.

An NGCN should deliver caller identification information and/or device identification information (contact URI) to the NGN when establishing an emergency call. The NGN needs to be able to use this information to route return calls to the caller or calling device in the NGCN.

REQUIREMENT 5: An NGN shall be able to make use of caller identification information and device identification information to facilitate the establishment of a return call.

An NGN that supports the hosting of enterprise services should be capable of handling emergency calls in accordance with enterprise requirements. Where the use of a PEAP is required, the NGN should support calls to PEAPs as private network traffic between NGCN sites or from hosted enterprise users.

REQUIREMENT 6: An NGN that offers hosted enterprise services shall be able to route calls to PEAPs if required by the enterprise.

An NGN that supports hosted enterprise users should support the use of emergency dial strings that fit the enterprise dial plan, independent of whether emergency calls from hosted enterprise users are to go to a PSAP or to a PEAP.

REQUIREMENT 7: An NGN that supports hosted enterprise users shall be able to allow the use of emergency dial strings that are compatible with the enterprise dial plan.

An NGN that supports the hosting of enterprise services or the establishment of emergency calls from NGCNs to PEAPs outside the enterprise network will need to support service URNs for enterprise emergency services, subject to a mechanism being defined for defining such service URNs (see 6.1.2).

REQUIREMENT 8: An NGN that supports the hosting of enterprise services or the establishment of emergency calls from NGCNs to PEAPs outside the enterprise network shall support service URNs that might be defined for enterprise emergency services.