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).

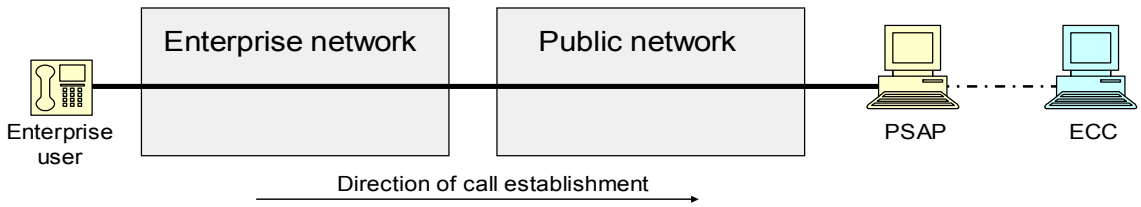

Figure 1 — Example of an emergency call from an enterprise user to a PSAP

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

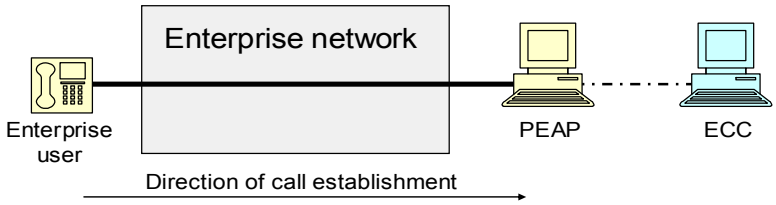

Figure 2 — Example of an emergency call from an enterprise user to a PEAP

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.

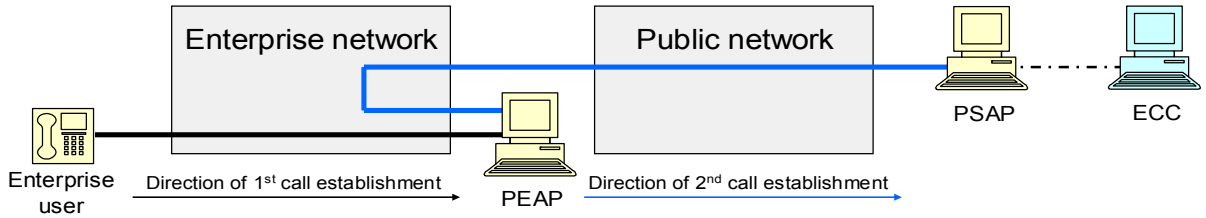

Figure 3 — Example of an emergency call from an enterprise user to a PEAP, resulting in a second emergency call from the PEAP to a PSAP

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.

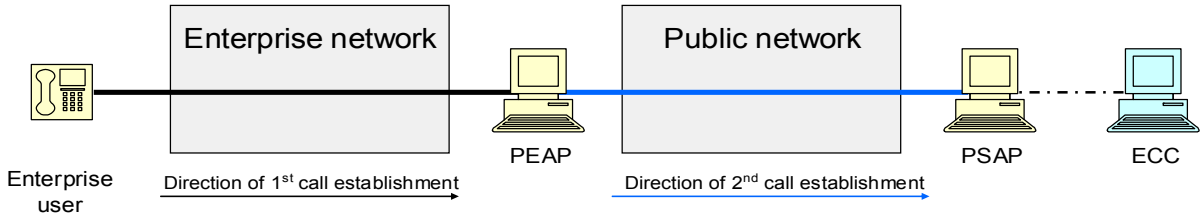

Figure 4 — Example of an emergency call from an enterprise user to a PEAP, resulting in a second emergency call from the PEAP to a PSAP without involving the enterprise network again

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].