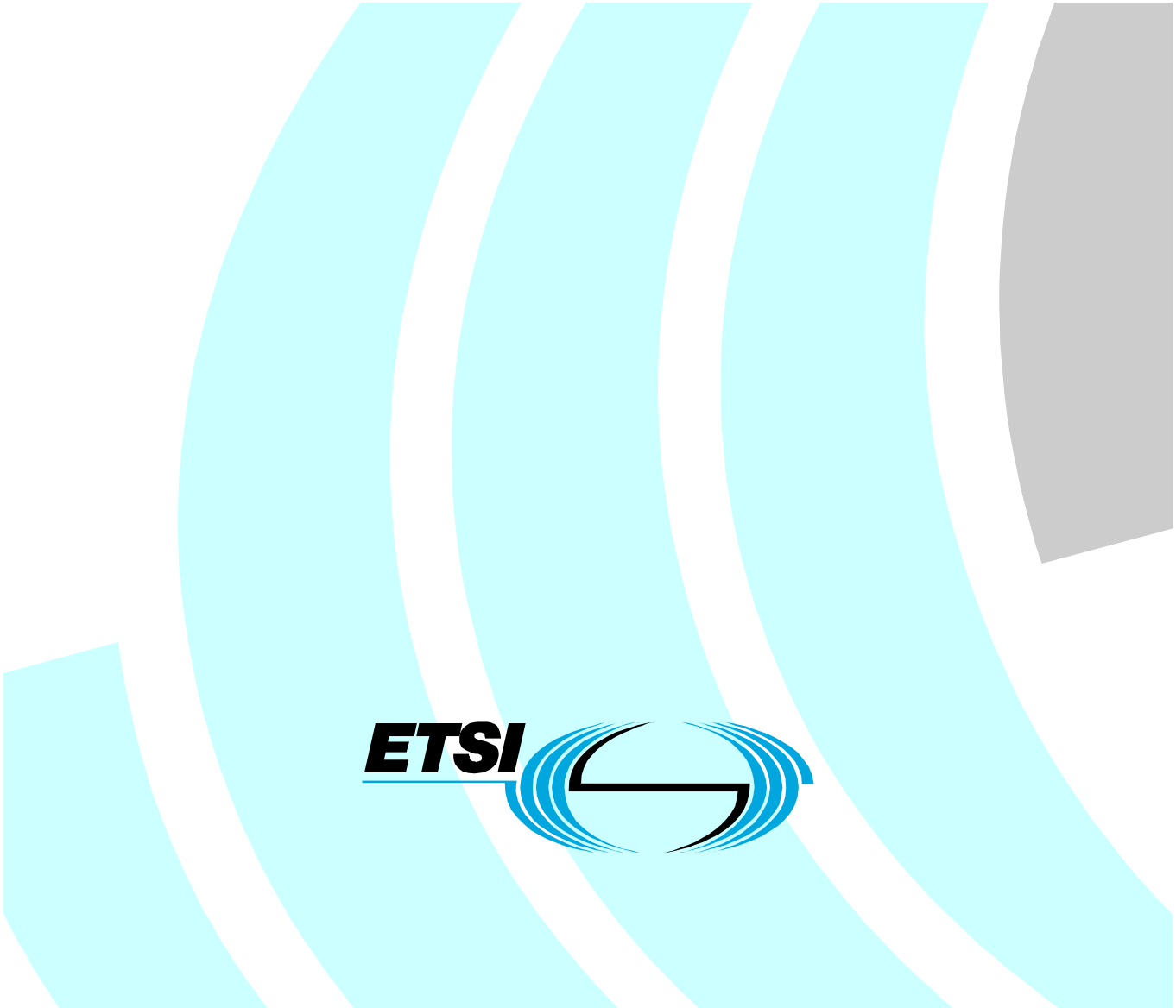
ETSI TR 103 180 V1.2.1 (2005-11)

Technical Report

Access and Terminals (AT);
Study on Emergency Communications;
Aspects related to fixed line terminals



Reference
DTR/AT-040006

Keywords
access, terminal, emergency

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Access and Terminals (AT).

Introduction

The present document identifies the terminal characteristics and the access network behaviour that relates to emergency situations.

This study results from a need recently identified to evaluate the support of Telecommunications infrastructures and services to citizens in emergency situations. A number of Telecommunications Authorities are studying the situation and the OCG co-ordination group on Emergency Telecommunications initiated a study (SR 002 180 [1], TS 102 181 [2], TS 102 182 [3], TS 102 410 [4], SR 002 299 [5]) with the intention of stimulating Telecommunications experts in the most relevant areas.

The present document is related to above mentioned study and covers terminals and access aspects of technologies used for the commonly fixed Telecommunications networks' technologies. It discusses the behaviour of emergency requests within the user facilities such as installations, terminals, home networks and the related access aspects. Aspects such as outgoing and incoming emergency calls, dependence on power supplies will be discussed and studies on POTS/PSTN, ISDN, Cable Modems, xDSL, Power Line, fixed radio access, cordless or fibre technologies will be included.

The conclusions under the present market situation and with the multitude of simultaneously available technologies and applications on the market are likely to be significantly different from the times where monopoly regimes were dominant and the POTS/PSTN terminals were nearly the only Telecommunications infrastructure available for the population.

This study is at the present unlikely to have impact on regulation but may, in the future, have relevance for a possible revision of the regulatory framework related to emergency in telecommunications services and equipment.

1 Scope

The present document identifies, for the commonly fixed telecommunications networks' technologies used in access and terminals, the terminal characteristics and the access network behaviour that relates to emergency situations.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ETSI SR 002 180: "Requirements for communication of citizens with authorities/organizations in case of distress (emergency call handling)".

[2] ETSI TS 102 181: "Emergency Communications (EMTEL); Requirements for communication between authorities/organisations during emergencies".

[3] ETSI TS 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organisations to the citizens during emergencies".

[4] ETSI TS 102 410: "Emergency Communications (EMTEL); Requirements for communications between citizens during emergencies".

[5] ETSI SR 002 299: "Emergency Communications; Collection of European Regulatory principles".

[6] ETSI TBR 021 (1998): "Terminal Equipment (TE); Attachment requirements for pan-European approval for connection to the analogue Public Switched Telephone Networks (PSTNs) of TE (excluding TE supporting the voice telephony service) in which network addressing, if provided, is by means of Dual Tone Multi Frequency (DTMF) signalling".

[7] ETSI TBR 038: "Public Switched Telephone Network (PSTN); Attachment requirements for a terminal equipment incorporating an analogue handset function capable of supporting the justified case service when connected to the analogue interface of the PSTN in Europe".

[8] ETSI ES 201 970: "Access and Terminals (AT); Public Switched Telephone Network (PSTN); Harmonized specification of physical and electrical characteristics at a 2-wire analogue presented Network Termination Point (NTP)".

[9] ETSI EG 201 120: "Public Switched Telephone Network (PSTN); Method of rating terminal equipment so that it can be connected in series and/or in parallel to a Network Termination Point (NTP)".

[10] ETSI TBR 003/A1: "Integrated Services Digital Network (ISDN); Attachment requirements for terminal equipment to connect to an ISDN using ISDN basic access".

[11] ETSI TBR 004: "Integrated Services Digital Network (ISDN); Attachment requirements for terminal equipment to connect to an ISDN using ISDN primary rate access".

[12] ETSI TBR 008: "Integrated Services Digital Network (ISDN); Telephony 3,1 kHz teleservice; Attachment requirements for handset terminals".

[13] ETSI EG 202 132: "Human Factors (HF); User Interfaces; Guidelines for generic user interface elements for mobile terminals and services".

[14] ETSI TR 102 125: "Human Factors (HF); Potential harmonized UI elements for mobile terminals and services".

[15] ETSI EG 202 325: "Human Factors (HF); User Profile Management".

[16] ETSI ES 202 076: "Human Factors (HF); User Interfaces; Generic spoken command vocabulary for ICT devices and services".

[17] ETSI ES 202 020: "Speech Processing, Transmission and Quality Aspects (STQ); Harmonized Pan-European/North-American approach to loss and level planning for voice gateways to IP based networks".

[18] ETSI EN 300 401: "Radio Broadcasting Systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers".

[19] ETSI TR 101 806: "Human Factors (HF); Guidelines for Telecommunication Relay Services for Text Telephones".

[20] ETSI TS 102 302-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Emergency Priority Telecommunications Service (EPTS); Part 1: Requirements analysis".

[21] ETSI EG 202 339: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Definition of requirements on the functional architecture for supporting Emergency and Priority user services".

[22] ETSI EG 202 116: "Human Factors (HF); Guidelines for ICT products and services; "Design for All".

[23] ETSI TR 103 073: "Universal Communications Identifier (UCI); Improving communications for disabled, young and elderly people".

[24] ETSI TR 102 133: "Human Factors (HF); Access to ICT by young people: issues and guidelines".

[25] IEEE 802.3af: "Power over Ethernet".

[26] ETSI EN 300 175 series: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI)".

[27] ETSI EN 300 176-1: "Digital Enhanced Cordless Telecommunications (DECT); Test Specification; Part 1: Radio".

[28] ETSI EN 301 655: "Private Integrated Services Network (PISN); Specification, functional models and information flows; Call priority interruption and call priority interruption protection supplementary service [ISO/IEC 15991 (2003), modified]".

[29] ETSI TS 101 909-2: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".

[30] ETSI TS 101 909-10: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 10: Event Message Requirements for the Provisioning of Real Time Services over Cable Television networks using cable modems".

[31] ETSI TS 101 909-18: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 18: Embedded Media Terminal Adapter (e-MTA) offering an interface to analogue terminals and Cable Modem".

[32] ETSI TS 101 909-24: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 24: MTA Basic Access ISDN Interface (MTA-ISDN)".

[33] ETSI TS 101 909-17: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 17: Inter-domain Quality of Service".

[34] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification".

[35] ETSI TS 122 016: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); International Mobile Equipment Identity (IMEI)".

[36] ETSI EG 202 067: "Universal Communications Identifier (UCI); System framework".

[37] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".

[38] ETSI ES 201 910: "Access and Terminals (AT); Digital Access to the Public Telephone Network; Line power requirements for IP terminals".

[39] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).

[40] ETSI ES 201 912: "Access and Terminals (AT); Short Message Service (SMS) for PSTN/ISDN; Short Message Communication between a fixed network Short Message Terminal Equipment and a Short Message Service Centre".

[41] ETSI EG 202 423: "Human Factors (HF); Guidelines for the design and deployment of ICT products and services used by children".

[42] ETSI TS 102 164: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Emergency Location Protocols".

[43] ETSI TS 103 021 series: "Access and Terminals (AT); Harmonized basic attachment requirements for Terminals for connection to analogue interfaces of the Telephone Networks; Update of the technical contents of TBR 021, EN 301 437, TBR 015, TBR 017".

[44] ITU-T Recommendation E.106: "International Emergency Preference Scheme for disaster relief operations (IEPS)".

[45] ETSI EN 301 406: "Digital Enhanced Cordless Telecommunications (DECT);Harmonized EN for Digital Enhanced Cordless Telecommunications (DECT) covering essential requirements under article 3.2 of the R&TTE Directive; Generic radio".

[46] IEEE 802.3: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications". .

[47] IEEE 802.1Q (2003): "IEEE Standards for Local and metropolitan area networks - Virtual Bridged Local Area Networks".

[48] CEN/CENELEC Guide 6: "Guidelines for standards developers to address the needs of older persons and persons with disabilities".

[49] IEEE 802.1p: part of the publication: 15802-3: 1998 IEEE Standard for Information technology--telecommunications and information exchange between systems--Local and metropolitan area networks--Common specifications--Part 3: Media Access Control (MAC) Bridges

NOTE: The standard 15802-3 incorporates ANSI/IEEE Std 802.1D, 1993 Edition, IEEE p802.1p, IEEE Std 802.1j-1996, IEEE Std 802.6k-1992, IEEE Std 802.11c-1998 and IEEE P802.12e. The specification IEEE 802.1p adds traffic classes to the IEEE 802.1D bridging standard.

[50] CENELEC EN 50174 (series): "Information technology - Cabling installation".

[51] ETSI TS 101 952 (series): "Access network xDSL transmission filters".

[52] ETSI ETR 056: "Digital Enhanced Cordless Telecommunications (DECT); System description document".

[53] CENELEC EN 50173 (series): "Information technology - Generic cabling systems".

[54] ETSI EN 300 176-2: "Digital Enhanced Cordless Telecommunications (DECT); Test specification; Part 2: Speech".

[55] ETSI EN 300 824: "Digital Enhanced Cordless Telecommunications (DECT); Cordless Terminal Mobility (CTM); CTM Access Profile (CAP)".

[56] ETSI TS 123 040: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical realization of Short Message Service (SMS) (3GPP TS 23.040 Release 6)".

[57] ETSI TS 123 041: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041 Release 6)".

[58] ETSI ETR 034: "Business Telecommunications (BT); Approval requirements for complex customer premises apparatus and installations connected to the Public ISDN (including principles for the application of the essential requirements to any apparatus)".

[59] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[60] Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Emergency Control Centre (ECC): facilities used by emergency organizations to accept and handle emergency calls

Emergency Call Post (ECP): facility that on lifting the receiver connects the emergency service user directly with a PSAP

Public Safety Answering Point (PSAP): physical location where emergency calls are received under the responsibility of a public authority

NOTE: See Commission Recommendation C(2003)2657.

3.2 Abbreviations

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

ATA	Analogue Telephone Adaptor
BWA	Broadband Wireless Access
CBS	Cell Broadcast Service
CEC	Commission of the European Community
CLI	Calling Line Identification
CMS	Call Management Server
CPE	Customer Premises Equipment
DDI	Direct Dial In
DECT	Digital Enhanced Cordless Telecommunication
DSL	Digital Subscriber Line
DUST	Duplex Universal Speech and Text communication project
ECC	Emergency Control Centre
ECP	Emergency Call Post
EMC	ElectroMagnetic Compatibility
EMS	Enhanced Message Service
EMTEL	EMergency TELecommunications
ESD	Electro Static Discharge
FTTH	Fibre To The Home
FTTK	Fibre To The Kerb
GPS	Global Positioning System

GSM	General System for Mobile communication
HFC	Hybrid Fibre Coax
HN	Hone Network
IC	Identification Code
ICT	Information and Communication Technologies
IMEI	International Mobile station Equipment Identity (check)
IMS	Internet protocol based Multimedia core network Subsystem
IMSI	International Mobile Station Identity
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ISIM	IMS SIM
IVR	Interactive Voice Response
LU	Loading Units
MAC	Medium Access Control
MAN	Metropolitan Area Network
MGCP	Media Gateway Control Protocol
MMS	Multimedia Message Service
MSISDN	Mobile Subscriber ISDN
MTA	Media Terminal Adapter
NAT	Network Address Translation
NCS	Network Call Signalling
NGN	Next Generation Network
NTP	Network Termination Point
PAS	Public Access Service
PBX	Private Branch eXchange
PIN	Personal identification Number
PLMN	Public Land Mobile Network
PLT	Power Line Telecommunication
PN	Private Network
POTS	Plain Old Telephone Service
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PUA	Personal User Agent
QoS	Quality of Service
RFID	Radio Frequency IDentification
SC	Service Centre
SDH	Synchronous Digital Hierarchy
SIM	Service Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SMS-SC	Short Message Service-Service Centre
SP	Service Provider
TE	Terminal Equipment
TSG-T	Technical Specification Group-Terminals
UCI	Universal Communication Identifier
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Networks
WLL	Wireless Local Loop
xDSL	Generic designation for DSL technologies

4 Emergency communications, frame conditions

The aspects of emergency communications are widely being studied. ETSI activities can be tracked using the "status Report" web page (regularly updated): http://portal.etsi.org/emtel/status.asp

SR 002 180 [1] (communication from the citizens to the authorities) gives substantial guidance on the present clause. When completed TS 102 182 [3] (communication from authorities to the citizens) and TS 102 410 [4] (communication among the citizens) will also provide important information impacting the scope of the present document.
TS 102 181 [2] (communication among authorities) is likely to have a more indirect impact (if any) in the present document.

It is important to differentiate two types of communications related with emergency situations:

- Voice calls addressed to 112 or any other emergency call number intended to bring the Public Safety Answering Point (PSAP) and the person suffering from emergency situation or his representative in direct, bi-directional, voice contact.

- The alarm message and other communications used to transmit complementary or supplementary data to the PSAP or Emergency Control Centre (ECC) in order to enhance the trust or description of the emergency situation.

NOTE: The second category includes communications from surveillance systems that might be connected to specialized organizations, which might, in turn, generate calls of the first category to PSAPs or ECCs. It also may include additional information directly associated with category one calls (for example SMS, or simultaneous voice and data).

4.1 User expectations on emergency situations (SR 002 180)

The European citizen expects in general to make an emergency call at any time, free of charge, using any of the most common telephony terminals connected to a public network. This implies that these terminals and corresponding access networks, except in well-justified cases, are expected to be operational for emergency calls when:

- The access to the Public Network has been barred (for example because of non-payment of bills).
- The coin and card payphones in restaurants, bars and other public and private places did not recognize the payment or identification means normally required to operate.
- The main power supply failed for less than a reasonable time interval.

NOTE 1: Calls may not be possible in cases where the network is already fully committed with priority traffic including pre-existing emergency calls) or congestion barring has been applied by the network operator.

NOTE 2: In some countries, some privately operated legacy payphones may not be technically capable of connecting emergency calls free of charge; regulatory intervention may be required to overcome this problem.

For mobile devices the principles are similar. Access networks are expected to be operational for emergency calls to pre-determined numbers (for example "112") also when:

- The mobile equipment or SIM card is protected by a password.
- A SIM card has not been activated or not been inserted into a mobile phone provided it is permitted by the operator and the national regulator.
- The emergency caller using a mobile phone is not located within the coverage area of his mobile operator or its roaming partners, provided the area is covered by another mobile network operator and the mobile phone is technically compatible with that network operator's facilities provided it is permitted by the operator and the national regulator.

NOTE 3: These features are not equally required in all countries and in some countries SIM-less calls are not permitted by network operators or the regulator.

Most popular technologies are PSTN analogue and digital connected terminals and PLMN terminals. Voice services related to emergency numbers, for example 112, are identified as the most important.

User's expectations related to voice emergency call are studied in draft EG 202 132 [13] and TR 102 125 [14].

4.2 Requirements of European regulation (SR 002 299)

Directive 2002/22/EC [39] requires that in addition to any other national emergency call number specified by the national authorities all end users of publicly available telephone services are able to call the emergency services, free of charge by using the single European emergency call number "112".

The present document details technical aspects and identifies possible solutions for identified weaknesses. Some additional information, not necessarily directly related to the "112" voice emergency calls (normally not in the regulatory domain) is suggested in order to overcome the difficulties associated with such weaknesses.

A more extensive reference to most relevant regulatory documents is available in SR 002 299 [5].

4.3 Services

Many communication services (based on telecommunications, broadcasting, radio, wired or other technologies and systems) may be extremely helpful in emergency situations. The first priority for the communications from the citizen to the authority, according European regulation and SR 002 180 [1], is nevertheless the voice services addressed to 112 and to any other identified emergency number, associated with the caller location information.

Everything possible should be done to give absolute first priority to this type of service in case of emergency and facilitate the easiest and most harmonized procedures, so that the citizen, in case of need will use the emergency facilities available without the need for special instructions or skills.

Data or video transmission systems have the potential of being extremely useful in an emergency situation and could facilitate remote control or surveillance in environment where humans might no longer be able to work.

Presentation methods on the terminal available to the operator in the PSAP should make available the maximum possible set of trusted information in the most appropriate manner. Neither public nor private network operators or service providers should delete or change any available numbering or location information whether or not they are able to validate it prior to its presentation to the PSAP.

Information provided to the PSAP has different levels of trust. Public operators and service providers have particular responsibilities in this context and the information delivered by them corresponds to high levels of trust. On the other hand, information provided by private networks is not submitted to the same degree of scrutiny and may correspond to lower levels of trust. Nevertheless this second type of information is expected to be of very high importance and may help to filter different types of emergency, detect false alarms and detail available data, for example location information or medical data.

NOTE: ITU-T recommendation E.106 [44], International Emergency Preference Scheme (IEPS) for disaster relief operations, describes an international preference scheme for the use of public telecommunications by national authorities for emergency and disaster relief operations. The International Emergency Preference Scheme for Disaster Relief Operations (IEPS) is needed when there is a crisis situation causing an increased demand for telecommunications when use of the International Telephone Service may be restricted due to damage, reduced capacity, congestion or faults. In crisis situations there is a requirement for IEPS users of public telecommunications to have preferential treatment. This is likely to have only an indirect impact (if any) in the present document.

4.4 Features and functions in Terminal Equipment (TE)

4.4.1 General aspects

Voice communication terminal equipment should be designed in such a way that emergency communication is always possible even if the terminal is PIN-coded or is dependent on an external power supply. In case of PBX, Home Networks or private networks in general, a high traffic or intensive use of the system should also not prevent the emergency communication to be successful. This could be achieved, for example by reducing the set of features of the terminals, home systems and Private Networks (PN) to the minimum necessary to always allow at least voice calls to the designated emergency call numbers. No terminal equipment feature should prevent emergency communication from being made.

Some public terminals are subject to special risks, for example automatic bank machines. The keys (help and/or survey and/or others) suggested in this clause could easily, where appropriate in future developments, be integrated in many of them and be for example associated with microphones or video devices allowing the activation of a remote surveillance in case of need. The deployment of such facilities should normally follow corresponding standards in order to have a positive impact, since citizens might find it hard to understand significantly different implementations. Where standards are not available, they should be produced prior to any large-scale deployment.

4.4.1.1 Emergency call terminals and specific posts

SR 002 180 [1] suggests a special feature in which all voice terminals connected directly to a public network or to a PSAP and having the facility to make emergency calls are expected to be able to make emergency calls free of charge and without the need for the citizen to know the emergency call numbers. Such call facilities are expected to be easy to use and not require specific language knowledge.

Terminals dedicated to specific emergency services, particularly those addressing highly centralized services, for example, E.112, and not used for other purposes may be recommended in some circumstances. Lifting the receiver, opening a cover or pressing a specially designated key may initiate the connection to the PSAP or other specialized emergency centre. Procedures for testing the functionality of these terminals regularly without producing false alarms should be devised (this requirement is listed in clause 6.3).

It is easy to imagine a wider coverage and general support of emergency communications to the citizens if, for example the HELP and other SURVEY keys are made popular by some manufacturers, operators or distribution channels.

4.4.1.2 "HELP" key for 112 service on terminals with voice application

This could be implemented if, for example telephone sets or other terminals introduced a "Help" key, which, when activated would initiate an automatic call to 112, sending the geographical location of the set and a number of characteristics common to all access technologies (ISDN, POTS, GSM, etc). Further issues regarding the implementation of SOS keys including the mapping to location based emergency numbers and other general guidance for mobile terminals are discussed in greater detail in EG 202 132 [13].

It is recommended that emergency call terminals are designed to be used for other services, so that any failure will be likely be detected during a non-emergency situation. The terminal's basic functions will therefore be tested every time it is used.

It is suggested that the "red HELP" key should be red should be put in a "easy to reach", evident place and be larger than other keys. The size, the marking and the overall specification should facilitate the clear identification of the key for all kind of citizens, including children, elderly people or citizens with any kind of impairment.

To prevent false alarm situations, it is suggested that this key not to be too sensitive in order to limit the risk of being activated in unwanted circumstances; a longer activation time or other measures could help reducing the probability of false alarms.

Details of the performances and behaviour(s) associated with this feature may have to be studied in more detail and specified in specific deliverables to be initiated if appropriate.

4.4.1.3 Other emergency keys for non-112 service

Additionally to the "red HELP 112 key", when recommended by national authorities, other keys might be associated with memories programmed with numbers related to other specific emergency services. Different types of text, data or voice messages to be transmitted in case of emergency might also be kept in memory. These other keys should easily be understood by the citizen as different from the "red HELP 112 key" and should not be designated "help key". Their designation should address clearly the emergency service they are associated with.

The use of the facilities suggested in the present and next clauses may often need to be associated to the E.112 service but in a co-ordinated manner and probably not directly, to prevent information overflow in the PSAP. In some cases, depending from the architectural concept associated to the deployment of the service, it may even be reasonable to foresee the connection of such alternative and complementary emergency services to a surveillance central point close to the emergency location, staffed by special skilled personal and not necessarily to a PSAP. Local solutions may in some circumstances be preferred to facilitate more effective, better co-ordinated inputs to emergency centres.

4.4.1.4 "SURVEY" key for discrete remote surveillance

The "red HELP 112 key" function as described above should be strictly reserved for the situation where the citizen wishes to communicate with the PSAP via voice. In cases were a citizen may wish to alert an organization of some emergency without generating noticeable signals at the place where the emergency occurs a "yellow SURVEY key" should be considered. The number to be dialled by that key should be configurable. The person responsible for the surveillance should configure the devices to call the number to the appropriate surveillance centre and to deliver any relevant data.

On activation, such a "silent alert" may be directly connected to a PSAP or ECC or first be routed to an emergency response organization that could verify the urgency and accuracy of the alert including associated data (for example location information) before contacting the appropriate ECC.

The SURVEY key, depending on the parameters to be observed and the functionality requested, may be associated with the use of microphones (more commonly), video cameras (frequently) or other transducers (fire, flood, chemical, etc.).

4.4.2 Categories of telephones and other terminals

Telephones may be classified in different ways:

- Accessibility:
  - Public.
  - Private (with restricted access, for example family members).
- Charging:
  - Pay phones.
  - Standard telephones.
- Connectivity:
  - Directly connected to a public network.
  - In a private network (for example PBX).
- Other restrictions (telephones restricted for example by passwords or PIN codes).

No matter what type of telephone, emergency calls should be possible at any time, free-of-charge. For access limited telephones, coin and card payphones, particularly those available on public sites, is recommended to integrate the features described in clause 4.4.

The classification can be extended to other terminals. However, special attention was paid to the voice service. The following clauses describe the most important cases in more detail.

4.4.2.1 Public pay telephones

Directive 2002/22/EC [39] requires that it be possible to make emergency calls from public pay telephones using the single European emergency call number "112" or any other emergency number, all free of charge and without having to use any means of payment. The citizen expects the same behaviour in private telephones.

4.4.2.2 Private pay telephones

Private coin and card payphones in restaurants, bars, etc. should allow emergency calls to be made free of charge without the assistance of an operator and without having to use any means of payment.

4.4.2.3 Telephones in private networks

If access to the public emergency services is allowed or nationally required from telephones in a private or residential network, then the Calling Line Identity (CLI) presented to the PSAP is normally the CLI of the attendant of the PN. Provision of the two number CLI service at the access to the public network allows the provision of a user provided CLI that may be useful or required by the emergency services. PN operators should, wherever possible, route outgoing emergency calls to the PSAP which would normally serve the locality in which the presented CLI is located unless otherwise required by relevant authorities.

In some private networks, emergency calls may initially be supported internally and decisions made by a local attendant on how and where they should be forwarded to a relevant PSAP; any such calls should have all available location information forwarded to the PSAP. In addition to the present routing aspects please refer to clause 6.3.6 regarding the level of trust which can be attributed to the localization information.

In such cases the operator of the PN is responsible for any fraud or misuse when calls are placed to the emergency services. For this reason emergency calls placed via PN access are often routed via an attendant for verification or are monitored by the PN. Services such as lift alarm systems are considered to be PN and are monitored, managed and maintained locally. They are not part of the emergency network but their use may result in requests for assistance from the emergency services.

PN should also be able to correctly support emergency calls at an acceptable quality level even in the case of power failure, high traffic or intensive use of the system. Where appropriate, this may be facilitated by reducing the system capability to the minimum required to allow voice calls to the emergency call numbers (recognizing that it may not be technically possible to differentiate analogue modem and fax calls from voice calls). No user or network feature should prevent an emergency call from being made.

4.4.2.4 Other access limited telephones

Some telephones may have their operation limited by a password or some other kind of special identity recognition. In all cases, whether privately or publicly available, they should allow emergency calls to be made without need for such recognition, free of charge and without having to use any means of payment.

NOTE 1: The CLI is a mandatory requirement in many countries. Therefore, anonymous E112 calls may not be allowed. That is why SIM-less emergency calls are not allowed in some countries. This is a result of trying to stop hoax E112 calls and prosecute hoaxers.

NOTE 2: Voice applications supported by a computer may not be accessible when the computer is secured by a PIN or has other security controls preventing connectivity with its supporting network. Wherever possible, it is recommended that an on-screen message should advise users of this limitation when the terminal is disabled.

4.4.3 Messaging in emergency situations

Generally, message services such as Short Message Service (SMS), Enhanced Message Service (EMS, which is a sub-set of SMS), Cell Broadcast Service (CBS), and Multimedia Message Service (MMS) may be useful for emergency communication. Recognizing that there are technical differences between these services, for convenience the present document will refer only to SMS (inherently including EMS) and CBS. Two different types of messaging communication scenarios are envisaged:

- Communication from authorities to citizens.
- Communication from citizens to authorities.

The first type of communication would typically be a CBS message to a certain area to warn or inform citizens about an incident. The second type of communication would typically be SMS/EMS and may be useful when no emergency voice calls are possible. 3GPP specifies the SMS/EMS and CBS in TS 123 040 [56] and TS 123 041 [57] respectively. Informative annex B to the present document contains a contribution of 3GPP in regard to SMS/EMS and CBS. Possible future solutions for fixed networks should be compatible with the ones of 3GPP.

NOTE 1: SMS and EMS are supported by almost every mobile network but EMS is not widely supported on many mobile terminals. CBS is not widely supported by mobile networks and also not particularly well supported on mobile terminals.

Some particular difficulties associated with SMS and EMS relate to its being a "store-and forward" service; therefore no real-time bi-directional connection is established. The difficulties are that there may be delayed message delivery, particularly if the receiving device is a mobile terminal in poor coverage or not active and that there may not always be confirmation of message delivery.

Nevertheless:

- SMS/EMS messages may sometimes succeed when voice calls are not possible or difficult, for example during poor radio conditions due to lower bandwidth requirements than voice or in case of unavailability of some voice communication components.
- SMS/EMS messages can be used in both directions but not in real time.
- SMS/EMS can provide confirmation of message delivery but this feature is not supported by all networks and, even if supported by the network, may or not be read by the user
- SMS/EMS messages can be used to transmit additional information about the emergency.

NOTE 2: To facilitate the writing of SMS/EMS messages and for more efficient handling in the PSAP, standard message formats may be defined. In this regard similar solutions should be standardized for fixed and mobile networks.

Special routing profiles might be required for emergency SMS/EMS messages. The contribution of SMS/EMS to E112 services may also be possible but needs further study.

In some mobile systems CBS can be used to alert subscribers within a given geographical area by activating a pre-selected group of base stations to broadcast an emergency message. A similar situation may be foreseen if the suggested extension of the CBS services to the fixed network is implemented based on ES 201 912 [40]. This extension is nevertheless to be studied with particular care before implementation due to facts inherent to relevant technologies, such as the difficulty of exactly identifying at present all the lines connected to terminals in a certain geographical area, both due to the increasing mismatch between geographical addresses and line identity (due to number portability) and to the nomadic facilities used on the IP based technologies. An additional difficulty is related to the fact that in the mobile world terminals are often provided with displays and displays are not so frequently available on standard terminal devices of the fix network.

In the case of a called subscriber ignoring the urgent aspect of a CBS message for some reason, it would be useful to be able to trigger the terminal to alert the citizen in some way, for example a special ringing cadence, to understand the emergency situation and follow the guidance in the message. For non-SMS terminals, other alarm messages have to be used, e.g. pre-memorized or synthetised voice statements, some sort of text-to-speech service or in some cases fax messages may need to be provided.

All such features and special services should be under the strict control of recognized authorities to prevent spamming effects or abuse for commercial purposes.

Telecommunications voice terminals have a distinct advantage over broadcasting receivers in that they can be alerted (ringing function) at any time whilst in the idle status. For complex messages, a co-ordinated information system could well make use of the SMS/ EMS and CBS messages and invite the citizen to obtain further information from some other specified medium, for example TV, radio or a web site.

SMS/EMS and CBS Emergency Messaging is not considered a priority service by 3GPP and most Public Land Mobile Network (PLMN). On fix networks the situation is similar and the assigned priority is probably lower. No country mandates a requirement for its use or behaviour. The latency (time to deliver) of text messages is unreliable and not guaranteed. Citizens should rely on such a feature only at their own risk.

4.4.4 Text telephones and fax devices

Users of text telephones should be able to access the emergency services either directly or via a relay service. Guidance on the use of relay services for text telephones in the Public Switched Telephone Network (PSTN) can be found in TR 101 806 [19].

Within ETSI work is in progress on the Duplex Universal Speech and Text communication Project (DUST) to identify a strategy and outline protocol design for conversational text telephony to be deployed on Internet Protocol (IP) networks and in the Next Generation Network (NGN). Further details of this work can be obtained from TC HF.

Fax services routed to emergency and alarm centres normally need a different number from the voice service. Nevertheless it is suggested that fax calls detected incoming on lines assigned for voice calls should re-routed to the appropriate addresses without seizing lines dedicated to the voice service. Both conversational text and fax facilities may be useful for disabled people and as a source of complementary information.

4.4.5 Voice initiated call to 112

Voice activated devices used in emergency calls should comply with ES 202 076 [16].

ETSI (STQ) has produced speech recognition standards and their use is recommended.

4.4.6 Special terminals

Certain special terminals for elderly and other people with special are connected to specialized centres. These centres monitor the persons' well being and, if necessary, will initiate an emergency call. In this context see clause 4.5.

4.4.7 Multipurpose facilities

Multi-purpose call facilities (for example customer assistance for vehicles and accidents) should, as far as possible, separate their operational modes in order to avoid unjustified calls to public emergency services.

NOTE: The European eCall initiative has the goal to facilitating the possibility of initiating emergency communications when being in a car and/or having it initiated automatically by the car in case of accidents.

4.4.8 Services that could be deployed by emergency authorities

Some applications may envisage the programming of a fixed telephone number (ITU-T recommendation E.164) or a fixed internet address to special centres in charge of some types of services and which could be used in case of emergency, for example some special medical or police services allowing a remote surveillance of the location. These are not considered as first priority services in the context of the present document, but devices supporting such services should benefit at least from some parts of the present document.

4.5 Usage by disabled, elderly and young citizens

Guidance in this area is offered on SR 002 180 [1], clause 6 and annex B.

EG 202 116 [22] does not specifically mention design for emergency situations, however it provides guidance to designers of ICT products including design for products for disabled people.

ETSI is contributing to EG 202 423 [41]. The work is based on TR 102 133 [24]. It will take an approach similar to that of CEN/CENELEC Guide 6 [48] but applied to children.

TR 103 073 [23] gives some information for young people contacting emergency services. It points out some issues that arise when the person initiating the communication may be in a state of distress or shock and be incoherent.

NOTE: EG 202 320, due for publication in October 2006, will give information on the handling of text calls by emergency services and on the use of relay services.

4.6 Types of identification in communications systems

4.6.1 General

The overview in the present clause aims to facilitate and to clarify the discussions on the emergency communications needs of caller identification and his location. The most commonly used identification parameters in modern communications systems are briefly described in the following clauses of the present clause.

Public telecommunications systems use a number of identification parameters. These facilitate the legitimate requirements of their users. PSAPs require in this context three types of identifications:

- The user line (mobile or fixed) identification to allow the caller to be called back by the PSAP call-taker.
- The caller identification (discussed in clause 6.3.5 of the present document) allows:
  - the call-taker to be responsible for the communication session and track hoaxers or other inappropriate users;
  - an alternative communication method with the user.
- The identification of the exact geographical position of the caller (discussed in clause 6.3.6 of the present document) to allow:
  - session routing to the appropriate (normally the closest) PSAP;
  - to facilitate the correct PSAP decision.

In the future, if proposals such as the one suggested in clause 4.4.1.2, "HELP" key for 112 service on terminals with voice application are successful, the corresponding standards may associate with this key some form of identification in order to identify the citizen and his location. Technologies to enhance the identification functionality may be implemented for example via an end-to-end protocol. Technologies to obtain location information may include GPS/Galileo or RFID. It may also be possible that further enhanced functions establish a data channel within the voice communication connection and transmits some or all of the parameters described below and eventually other useful data.

In all cases, the identification of the calling line and the session initiating party is important. The designers of new features, devices or home systems are encouraged to create easy means for the PSAP to trace the caller in emergency situations.

4.6.2 Identification in the PSTN - CLI

The CLI was initially adopted to identify the subscriber to the Calling Line, even if it does not completely map to the caller, since a number of persons (a family or a small business) often shared the same telecommunications line. In fixed networks the CLI became a parameter to identify the caller from the calling line and therefore, in normal cases, with some precision also the location of the caller.

The development of VoIP has resulted in the emergence of PSTN-like services, which no longer need be associated with any particular location. These services are capable of CLI delivery but this in no longer of any significance for caller localization since the service can be invoked from anywhere a broadband IP connection is available. It is possible to locate the service by tracing its IP address, but even then the nomadic user may be behind a PN gateway making accurate localization nearly impossible. Some network operators block calls to emergency numbers for VoIP customers to avoid this problem.

Conclusion:

- CLI identifies the Calling Line.
- CLI can provide a tentative identification of the Caller location.
- CLI can provide a tentative identification of the Caller by identifying the subscriber.

4.6.3 Identifiers in the PLMN

With the emergence of PLMN new identifiers have been introduced. As described in TS 123 003 [34] they are:

- Mobile Subscriber ISDN (MSISDN) number.
- International Mobile Station Identity (IMSI).
- International Mobile Station Equipment Identifier (IMEI).

Regarding the identifiers the following applies:

- The MSISDN number identifies the E.164 address that is associated with a particular subscriber.
- The network associates the MSISDN with the IMSI of the (U)SIM.
- The IMSI is a unique code identifying the (U)SIM.
- The (U)SIM is one possible application of the IC card that belongs to the subscriber.
- The IMEI only identifies the equipment, the mobile phone itself independently of the (U)SIM.

Since the user of the telephony service has to identify himself with a PIN Code to the (U)SIM the network may trust the mobile equipment about the identity of the user. Furthermore, the association of the IMSI with the MSISDN is a stable long term relationship. As a consequence, the MSISDN number may be used to retrieve the identity of a service user; some exceptions include a mobile phone lent to another person or a switched-on and stolen mobile device.

It can be concluded that the MSISDN number, as the CLI in the PSTN, indicates the subscriber SIM card services. However, there is no physical calling line, as there is in the fixed network. Therefore, there is no indication of the location of the caller.

NOTE: Some SP enter dummy CLI of base station (BS) to calls in order to support approximate location information.

The IMEI identifies the equipment. The relationship to the user is similar to the one of the calling line in the fixed networks case. Thus, no identity information about the subscriber or user may be obtained. Furthermore, it is mainly used in order to detect stolen mobile phones and is of limited use for emergency telephony. In case of SIM-less emergency calls it would be the only identifier available, as stated in TS 122 016 [35], which also specifies that calls to emergency services should be available for mobile phones listed on the so-called "black-lists".

4.6.4 IP address identification

Generally, an IP address maps to one host or node. If all of these nodes were in fixed locations, this would imply the identification of individual devices and their locations. However, there are several technologies that allow a dynamic allocation of IP addresses and a certain degree of mobility. This implies that location and terminal equipment may not be easily related.

These technologies include Dynamic Host Control Protocol (DHCP) and may be applied to:

- Network Address Translation (NAT).
- Mobile IP.
- VPN.

With regard to identification, the use of IP addresses alone is of little value. However, the combination of the IP address, MAC address and time of allocation identifies a specific terminal at a specified time.

- The IP address identifies the terminating node.
- The MAC address identifies the equipment.
- The time specifies the period during which the association of equipment with IP address was valid.

SPs can record the assignment of IP addresses to the registering equipment during a particular period and may be able to retrieve and reveal this information (subject to data protection laws).

Therefore, depending on the type of usage, fixed or mobile terminal, a more or less valid assumption about the user of the equipment can be made. A fixed terminal would generally allow access by more people; except for applications with some kind of personal authentication mechanism. Mobile terminals are used by a smaller group of people. Here also, mobile equipment with integrated authentication modules allows positive identification of the citizen. However, such authentication is made independently of any IP address knowledge, although, it may subsequently be associated with it by the SP.

4.6.5 Media Access Control (MAC) identifications

The MAC address identifies an Ethernet network adaptor, which may be part of a more complex hardware device on a network, and is unique. The MAC address on its own does not identify a particular person or location. It may identify a person in a scenario as mentioned in the previous clause where a device is associated with a person (for example through the means of authentication and access control, where only that person is allowed to use the device) and the IP address. Only if a device is bound to a location the information the MAC address may be used as location information.

NOTE: MAC addresses can be spoofed readily with software and therefore does not guarantee identification even of the network adaptor.

4.6.6 Application level identification

Application level identification methods are addressing mechanisms for IP based communications technologies. They include, for example:

- SIP addresses.
- IMS SIM (ISIM) identifiers, as specified in TS 123 003 [34].
- H.323 addresses.
- Telephone numbers, in systems using NCS or MGCP, such as IPCablecom™.

They all identify the terminating application of the communication service. The nature of the application defines whether the user of a service may be identified or not. It depends on the:

- Accessibility of the application.
- Authentication of the user to the application.

A user may be subscribed to a communications service with an assigned identifier. The identity of the citizen will be known to the communications system if the citizen is required to authenticate to the application. Otherwise, the application identifier needs to be configured in the application. This corresponds to the CLI in the PSTN. If access to the device is limited to a particular citizen, identification is also possible.

4.6.7 Universal Communication Identifier (UCI)

According to EG 202 067 [36], UCI is the concept of a single, unique identifier for a citizen. All communication is controlled by a single personal user agent (PUA). Since the citizens have to register at their PUAs in order to get access to the service, their identity is, guaranteed in each individual communication session. In contrary to the addressing mechanisms above, UCI is able to identify the individuals. The identifier delivered can be trusted. However, UCI systems do not reveal any type of location information. For this purpose other mechanisms should be used.

4.6.8 Biotechnologies to identify citizens

One common method of authenticating to an application is some kind of code, for example a PIN code. Another solution is the use of biometrics, the identification of an individual according to his physiological or behavioural characteristics. EG 202 116 [22] lists the following biometric technologies:

- Face.
- Fingerprint.
- Hand geometry.
- Iris.
- Retinal scan.
- Signature.
- Voice print.
- Facial Thermogram.

Instruments to scan or measure these metrics need to be implemented in the devices that also hold the communications applications. The identification of the individual depends on the accuracy of the application evaluating the biometric data. In any case it should be higher than any other identification method. However, these methods are usually only implemented in highly sensitive security areas. Their use for the identification of citizens is therefore not likely. Public concerns and arguments against the implementation of biometrics range from cost effectiveness to privacy concerns of citizens. Biometrics do not provide any location information unless the location of the sensing device can be accurately verified.

5 Emergency communications needs and market aspects

5.1 Types of emergency communications

5.1.1 Communication from citizens to authorities

The most typical application for this type of emergency communication includes the situation of a citizen issuing an emergency call. A further possible scenario might be some kind of automatically issued emergency call or alarm for example because of some certain situation or parameter, for example personal characteristics, might be used in immediate medical support for elderly people to pre-recognize and alert the appropriate specialized centre in an upcoming possible emergency situation. This will help the eventual 112 or the emergency call to be trusted and more efficient.

Data transmission functionality can be used in security affected situations such as banks, so that an employee in an emergency case has the possibility to issue an alert based on earlier, trusted information obtained from a number of consistent alerts. In this case the data transmission functionality may be connected directly or indirectly to the PSAP. In the indirect case the alarm is dealt with by an intermediary organization for example a specialized security service. "Silent alert" is an example for this type of service.

In general, the requirements for communication from citizens to authorities in case of distress as specified in SR 002 180 [1] should be followed.

5.1.2 Communication between authorities

A terminal used in this case of communications should have an intuitive user interface, which enables the operator to collect and organize collected data in an appropriate way. The personnel using such terminals is well trained in contrast to a citizen making an emergency call. Furthermore, terminals should support also the transmission of this collected information to another PSAP.

TS 102 181 [2] gives an overview over the requirements for communications between authorities. Terminals should support all required functionality to satisfy the requirements listed therein.

Examples are:

- Conferencing functionality.
- Push-to-Talk.
- Further simultaneous and non-simultaneous voice and data communication.
- The security services required for the level of sensitivity of the communication data.

5.1.3 Communication from authorities to citizens

Authorities use this form of communication to broadcast warnings and alerts, as a notification system. In this form of communication mainly broadcasting is used as an informative tool. TS 102 182 [3] specifies operational and organizational requirements for a common notification system.

Terminals used by authorities should implement means for distribute information, notifications, alerts or warnings according to the requirements stated in TS 102 182 [3]. Terminals used by citizens should support the functionality required in order to receive this data.

Special attention should be put on the fact that deaf or impaired citizens are serviced properly. Here, the implementation of a combination of audio, video and/or text service on terminals may be necessary.

5.1.4 Communication amongst affected citizens

TS 102 410 [4] specifies requirements for communication between citizens in the case of emergencies. Terminals should support the required functionality to satisfy these requirements.

The report also mentions communication means such as SMS. Standardization of MMS for fixed-line is done in TC TISPAN Project F-MMS.

Special focus in the report is also put on resilience of TE as mentioned also in clause 6.3.2.

5.2 Multiplicity of solutions on the market

A number of solutions is available on the market; they have to be carefully selected for each application.

To implement standardized solutions for basic services and the widest coverage of the population, the E112 voice service is the obvious choice and is strongly recommended.

5.3 Population needs coverage by existing solutions

As the first priority is to ensure the wider population is well served by emergency communication and as the E.112 service was identified as the most relevant, it seems obvious that the most popular and harmonized terminals (analogue and digital PSTN terminals) should be the first to benefit from the recommendations in the present document.

Non-voice services are not considered in the first priority but they can contribute complementary information in order to facilitate the most appropriate intervention from the requested authorities.

The development of technical solutions deviating from the harmonized ones may only create difficulties to the effectiveness of the emergency services. This has to be taken into consideration and is discussed in more detail in clause 6.

5.4 Relationship between mobile and fixed equipment

A customer of a telecommunications service expects similar behaviour of a service no matter which type of network or technology he uses. Therefore, it is of great importance that mobile and fixed networks offer the same type of basic services with similar, well accepted, user interfaces. This is particularly important to enable the citizen facing an emergency situation to act quickly and correctly. ETSI TC HF deals with these issues.

For civil alerts and communication from authorities to citizens over a wide area, the SMS broadcasting feature described in clause 4.4.4 is an example where the procedure requested from and guidance given to the citizens should be consistent in mobile and fixed networks. Ongoing work on standardized user profiles at ETSI (in EG 202 325 [15]) aims to produce guidelines in this area.

5.5 Top-view EMTEL architecture

See appropriate information on annex A of SR 002 180 [1].

6 General technology aspects

6.1 General aspects of the network access

Analogue or digital PSTN (POTS or ISDN) Terminal Equipment (TE) connected over cable, xDSL or fixed radio links technologies are increasingly being used in the access networks. Policy makers generally support such initiatives in that the usage of the existing wire and radio infrastructures is optimized and competition is promoted. This means that the same service, as seen by the user, may present different characteristics, for example related to "life line" or CLI functionalities, which are of central importance in emergency situations. These issues can only be solved by National Regulatory Authorities. Nevertheless the use of harmonized solutions for the user network interface (UNI) is strongly recommended. It should be ensured that as far as possible basic network functionalities are maintained even if its main power supply is interrupted. A design survival period for the power supply of at least one hour has been suggested, but this needs to be further studied in connection with existing network design standards, user expectations and the performance of power distribution networks.

Some networks, notably the PSTN, may have built-in network protection mechanisms or be self-limiting, such that in the case of an emergency covering a wide area (for example, an earthquake or terrorist incident) citizens may be denied access to the network due to the levels of traffic. Such denials may be on an operator-assigned "user-priority" basis or simply on a "first-come, first-served" basis, where no dial tone is presented to a PSTN user or where no IP address, gateway channel or bandwidth is available to an IP-connected customer.

Such non-availability of service cannot usually be overridden by users since this would leave it open to abuse and negate the purpose of the network protection it should provide. Its consideration is outside the scope of the present document.

6.2 General aspects of terminals and home installations

6.2.1 Cabling and installations aspects

All cabling and installation work should be carried out in full accordance with recognized specifications, national standards and operator defined practices. In particular, special attention should be paid to the security of primary and secondary power supplies and their distribution. It is essential to ensure that all equipment is operating within its specified environmental parameters and that it is in a physically secure location. Building access cables should also be routed in such a way that they cannot easily be maliciously disrupted.

6.2.2 Simple devices

Failure of power supplies is the single greatest cause of telecommunications systems non-availability. To ensure a maximum of efficiency in emergency situations it is recommended that simple devices are power supply independent and that wherever possible more complex devices retain their basic functionality during power failures.

6.2.3 Featured devices

To ensure their maximum possible efficiency in emergency situations it is recommended that featured devices offering support to emergency communications, in case of emergency and in the case of power failure, suspend all non-emergency related functions and ensure their basic operation for the maximum possible time to facilitate operation of the emergency related features.

6.2.4 Data and video devices

The principle recommended in clause 6.2.3 is also applicable. The surveillance key feature is one of the solutions recommended in clause 4.4.2. It may have many applications, for example in case of video surveillance cameras a special surveillance key may direct the attention of the surveillance centre operator to a particular point. Also a well-coordinated set of data messages (SMS, e-mails or others) may be very useful.

6.3 Emergency communications aspects

Many of the technical requirements discussed in the present document are valid for both TE and the supporting network. In most cases the requirements cannot easily be separated due to the inter-dependence of the network and the TE. Formally the Network Termination Point (NTP) for publicly offered interfaces is the point at which the network operator offers a connection to the consumer and which connects TE to the network. This is the point where the equipment is no longer TE and is part of the public network.

Different services, even when carried on the same physical medium, may offer different NTP having different technical characteristics. The present document covers only TE, user and CPE equipment, and its access requirements. TE may incorporate (private) network equipment. These technical requirements are examined from the TE point of view. Network aspects are mainly studied in ETSI TC TISPAN (covering services and protocols aspects) and in ETSI TC TM (dealing with transmission, physical layer aspects). For ISDN, existing standards still apply and reasonably cover emergency services aspects.

This clause highlights important technical properties of emergency services, which include the following:

- Performance.
- High reliability and availability.
- Priority for emergency services.
- Identity of emergency service user.
- Location Information.
- Security services for emergency communication.
- Testing of route to emergency service operator.

Many items of the list above are also defined as requirements by SR 002 180 [1] and are described in more detail in the following clauses.

6.3.1 Equipment performance

The huge majority of available TE is designed to commercial standards and will normally suffice for emergency communications when used in the protected environment of a home or office. Where TE is routinely used in a more hazardous environment, care should be taken to ensure that it is appropriate to the circumstances. For example, it should be spark-proof when used in explosive atmospheres or water-resistant for use outdoors.

Design considerations for equipment dedicated to emergency communication, for example public emergency call posts, should in addition to the base standards pay particular attention to the climatic conditions, additional protection from electrostatic discharge (ESD), mechanical and thermal shock, and vandalism. The ElectroMagnetic Compatibility (EMC) design considerations should take into account the harsh environment to which the TE may be subjected, particularly in a roadside situation. Its operation should be as simple as possible, perhaps restricted to pressing a button to activate two-way voice communication. Terminals intended for emergency services support, should be able to operate appropriately without the need of external power supply. Where line-powering proves impracticable, due to line length or power requirements, roadside call posts may be provided with batteries recharged from co-located solar cells or even wind-generators.

In all the cases the performance of the terminal should be appropriate in the environment he will be used. Special environmental conditions (humidity, radiation, heath) request special studies on the dependency of the TE performance.

6.3.2 High reliability and availability

Reliability and availability issues are very important for emergency communications. Fast and immediate delivery of emergency services is only possible if "always-on" means of communication exist. However, not all technologies and equipment support such capabilities by default, sometimes because they have not been incorporated in the systems development from the beginning. SR 002 180 [1] also stresses the importance through stating that Network Termination Points (NTP) of public or private networks should supply TE with a minimum power supply in case of local power failures, although it is recognized that this will not always be possible.

The availability of "always-on" equipment largely depends on the capability of maintaining functionality in case of interruption of power supply. Unfortunately, crisis and disaster are often accompanied by power supply outages. Typical solutions may include:

- Battery-Back-up-Packs for terminal equipment (TE).
- Uninterruptible Power Supply (UPS).
- Connection to alternative power circuits.
- In-line power supply.

The application of these depends on the desired service and on the cost for the infrastructure, including the terminals. Examples for in-line power supply are the "life-line" functionality of PSTN terminals and Power over Ethernet (PoE). PoE is covered in IEEE 802.3af [25]. ES 201 910 [38] specifies the requirements for line powering of IP Terminals connected to IEEE 802.3 [46] interfaces.

A further issue is the reliability of the connection of TE to the telecommunication infrastructure. This especially includes cabling and plugs.

6.3.3 Void.

6.3.4 Priority of emergency services

Besides availability and reliability the priority of emergency communications as described in SR 002 180 [1] is vital. According to it all network operators should accord emergency communication priority over all other traffic. ETSI TC TIPHON highlights the vital role robustness of such networks in TS 102 302-1 [20].

Examples of how priority may be ensured are:

- The use of separate telecommunication infrastructure for emergency services (prioritized routing).
- An *a priori* reservation of channels or bandwidth.
- "On-the-fly" prioritization.

"On-the-fly" prioritization may either be done by the network or by the TE depending on the kind of technology. It utilizes the QoS mechanisms available in certain network infrastructures to ensure that emergency services are conducted with priority.

6.3.5 Identity of a citizen

The identity of the citizen using the emergency communication service is another important property. However, its determination is very difficult. Absolute identification is not very likely without the use of biometrics and these technologies are not yet widely used at the consumer level.

Some identifiers used in telecommunications systems are discussed in clause 4.6 together with risks of inaccurate caller identification. Generally, the identity of the citizen may be used to:

- Return a call in case of communications interruption.
- Find alternative communication methods in case of emergency communications break-down.
- Hold the citizen responsible in case of emergency communications misuse.

According to SR 002 180 [1], clause 4.2.1.1, it is strongly recommended that the PSAP should be able to return a call to the calling party. It is important for the PSAP to be able to re-initiate communication (call back) to the citizen in case the initial communication session is interrupted. If the initial communications medium is still available the identity of the calling line is sufficient, otherwise it is necessary to identify the citizen in order to find alternative communication media.

In the case of misuse of the emergency communications service, the PSAP may have on-line access to identity information. Most SP's store session information whether or not there are regulatory requirements. It can usually be obtained off-line but is subject to data protection legislation. However, whether such mechanisms deliver accurate identity information depends on the technology used.

For PSTN based calls to emergency services, E.164 numbers can be used as identifiers of the calling party and these numbers are delivered to the PSAP. However, calls made using some other technologies that use other communication identifiers require alternative means for the collection of identity information.

6.3.6 Location Information

In order to direct emergency relief teams to the place of emergency the citizen's location is of vital importance. Besides that it may also allow the PSAP to detect malicious calls. Geographic numbers and location information databases allow a cross checking with the location given by the calling party. This mechanism may also be helpful in cases where the calling party is not able to name its location, for example children and also for automatically initiated emergency communication sessions as might be the case with special emergency key functionality as described in clause 4.4. Location Information may be obtained by TE or home devices for example via GPS functionality or by the network for example via a location information database. All network related issues fall under the responsibility of TC TISPAN for fixed networks and 3GPP for mobile networks and are therefore not discussed in detail in the present document.

A further application of the location information is the routing of incoming emergency communication to the PSAP located nearest to the citizen. This is a network matter and therefore falls under the responsibility of ETSI TC TISPAN.

6.3.6.1 Caller localization issues for nomadic TE

For nomadic IP terminals the location information may not be obtainable in a straightforward way. Possible solutions depend on a system's architecture and offered services and may even involve user interaction. Examples for solutions are:

- Citizen informs PSAP personally in case of an emergency.
- TE detects relocation.
- Restricted nomadicity.
- In-built GPS functionality.

It should be noted that TS 102 164 [42] is being revised to handle geodetic co-ordinates for geographic position, postal co-ordinates, IP addressing and GPS.

One possibility to overcome the lack of location information might be for featured terminals to detect if their connection has been interrupted at any time and therefore that their location might have been changed. If this is the case the citizen could be prompted to enter the changed location information or confirm that the previous information remained valid.

Also the nomadicity of a terminal may be restricted to a small, defined area, or global positioning system (GPS) data may be used to gain location information.

An emergency communication application requires the knowledge of the TE's features together with the permission of the citizen to use and transmit the obtained information.

6.3.7 Services to protect the emergency communication

EG 202 339 [21] defines the service requirement of secure and confidential communication between authorized users in emergency operation.

In order to prevent emergency communication from misuse, authenticity and integrity for communication need to be verified by appropriately secure means. For example, the PSTN is relatively secure by its nature. The access network delivers the CLI from the PSTN. This may be used by the PSAP for Ring-back or for tracing malicious calls. IP as transport mechanism presents a number of possible security weaknesses. Depending on the technologies the means to secure communication differs and individual analysis is required.

6.3.8 Testing of route to emergency service operator

It should be possible to test for a working emergency communications service. This should be done in a way that does not occupy any resources of the PSAP and should in no case initiate a false alarm. One solution to this problem could be a special communication identifier reserved for testing purposes, which invokes some kind of standard response (for example Interactive Voice Response (IVR)).

7 Network connectivity

This clause describes the properties of important access technologies in regard to emergency communication. Figure 1 illustrates the relationship between those technologies in a kind of layered structure.

NOTE: This listing only focuses on the most important technologies from the point of view of the terminal equipment and only shows an overview. It is not possible to define the borders of the layers in a strict fashion.

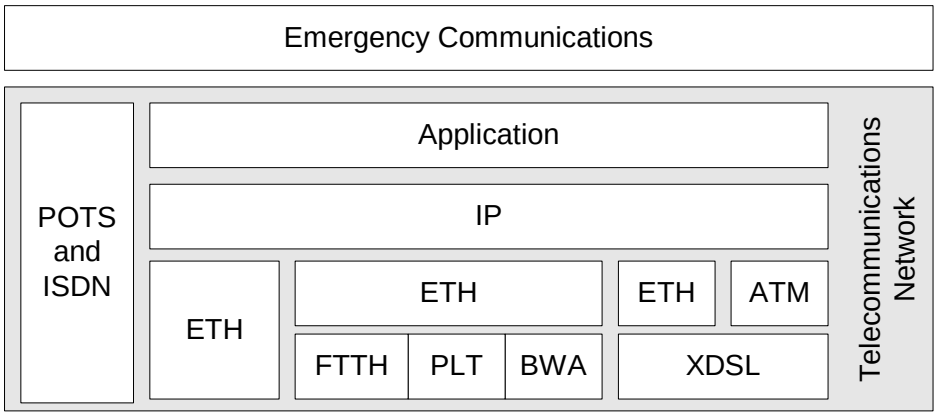


Figure 1: Relationship of access technologies

7.1 POTS, the analogue legacy interface of the PSTN

7.1.1 General aspects

In the present clause only the analogue legacy interface of the PSTN is discussed. Gateways from alternative technologies (cable, xDSL, fibre, WLL, etc.) offering analogue PSTN interfaces, should nevertheless, as far as is reasonable, fulfil the guidance and the standards applicable to this popular, widespread technology to limit the risk of incompatibilities.

In Europe and worldwide, the PSTN analogue terminal is probably the most common and one of the best fixed telecommunications devices for supporting emergency situations. Voice services related to emergency communications, including CLI features, are supported and a wide range of data functionalities are available. The network normally provides "life line" functionality. Simple terminals normally do not need local power supply. More complex (featured) terminals may or may not have the capability of receiving, continuing or initiating a call in the case of power supply failure.

Data or video transmission systems associated with this interface have the potential of being extremely useful in an emergency situation and could facilitate remote control or surveillance in environments where humans might no longer be able to work.

7.1.2 Terminal Equipment (TE)

TBR 21 [6] and the TS 103 021 series [43] of specifications are no longer mandatory documents under EU regulation, but they describe the large majority of POTS/PSTN terminals in Europe and many other countries. Furthermore, these standards are widely recognized as the most used for this legacy technology, therefore they can, at least for the European market be considered as the most representative.

For analogue PSTN voice terminals with a handset the reference standard should be TBR 38 [7], which though not of regulatory value, has a wide acceptance in the market and matches the international harmonized transmission plan specified in ES 202 020 [17].

7.1.3 Access

ES 201 970 [8] is included by the Commission of the European Community (CEC) in the list of standards under the Framework and the Universal Service Directives. This recommendation may, according the Directives, become mandatory if CEC or the national authorities decide it is appropriate. This standard specifies a harmonized solution, is widely used and was designed to support terminals meeting harmonized standards (TBR 21 [6], the TS 103 021 series [43] and TBR 38 [7]). The interfaces offered to terminals should follow ES 201 970 [8]. By doing so, any new facility designed for emergency communications will have a maximum of impact in the shortest time and at the lowest cost. Additionally, it is recommended that the interface should supply power to the terminal in the case of failure of the mains power supply.

7.1.4 Installations

TBR 21 [6], now updated in the TS 103 021 series [43] of standards, created the concept of "Loading Factor" explained in EG 201 120 [9]. This concept was later applied to ES 201 970 [8] where the operator is required to indicate the loading capability of the interface offered to terminals.

Devices fulfilling the requirements of TBR 21 [6] and TS 103 021 series [43] should offer loading factors of less than 100 Loading Units (LU). Interfaces meeting ES 201 970 [8], may offer a loading factor of more than 100 LU. Users should be aware that connection of too many telephones to a single line might impair its performance and possibly disrupt communications. Inappropriate installation at the "do-it-yourself" level, may introduce additional risks to the quality and availability of the telecommunications service. Any such problems should become obvious during use of the terminals for routine, non-emergency calls.

7.2 ISDN, the digital interface of the PSTN

7.2.1 General aspects

In the present clause only legacy ISDN terminals connected to the PSTN will be discussed. Minority applications provided via alternative technologies (cable, xDSL, fibre, WLL, etc.) and offering ISDN-like interfaces, should nevertheless, as far as is reasonable fulfil the guidance and the standards applicable to this technology to limit the risk of incompatibilities.

In Europe and worldwide, ISDN voice terminals have a relatively limited deployment. Voice services related to emergency communication, including CLI features, are supported and a wide range of data functionalities are available. The network may be regarded as providing "life line" functionality, although local powering of terminals is required in certain instances.

Data or video transmission systems associated with this interface have the potential of being extremely useful in an emergency situation and could facilitate remote control or surveillance in environments where humans might no longer be able to work.

7.2.2 Terminal Equipment (TE)

TBR 003 [10] for ISDN basic access and TBR 004 [11] for ISDN primary rate access are no longer mandatory documents under EU regulation but they and the associated ETSI standards continue to represent the large majority of ISDN terminals in Europe.

For ISDN voice terminals with handset the reference standard is TBR 008 [12]; this is also no longer of regulatory value but continues to have a wide acceptance in the market and matches the international harmonized transmission plan specified in ES 202 020 [17].

7.2.3 Access

ISDN service is not included by CEC in the list of standards under the Framework and the Universal Service Directives; its provision is not therefore mandatory according to the Directives. Deployment of ISDN services varies considerably in European countries. Any further developments should take into account the requirements for support of emergency telecommunications.

Additionally, it is recommended that the line interface should supply power to at least one terminal in the case of failure of the mains power supply.

7.2.4 Installations

The installation should be in accordance with ETR 034 [58], which covers the requirements for complex customer premises apparatus and installations connected to the public ISDN (including principles for the application of the essential requirements to any apparatus).

The installation will usually require the availability of a mains power supply, but otherwise should not normally have an impact on the effectiveness of a possible emergency call. With the increasing number of telecommunications applications on the terminals and the decreasing level of prices, the citizen may frequently not notice that the capabilities offered by the network interface may well be exceeded by the requirements of his installation. Inappropriate installation at the "do-it-yourself" level, may introduce additional risks to the quality and availability of the telecommunications service. Any such problems should become obvious during use of the terminals for routine, non-emergency calls.

7.3 DECT

7.3.1 General aspects

DECT is a well known cordless technology in Europe at present. For DECT devices, and additional to the interface and basic voice standards, the reference standards should be the ETSI DECT Harmonized Standard EN 301 406 [45].

DECT technology is used in:

- Public Access Service.
- Business Cordless Telecommunications.
- Residential Use.

It is important that the devices supporting emergency features respect all appropriate requirements. However, not all products on the market do implement the emergency telephony service as provided by the DECT standard series EN 300 175 [26]. For those can be said:

- Roaming between public access networks or between residential and public networks is not always provided.
- EN 300 175-5 [26] specifies a mechanism to allow emergency communications even with unauthenticated hand-sets. Due to concerns about the abuse of the emergency system this facility is not implemented. Emergency calls are therefore only possible from authenticated hand sets.
- Depending on the implementation access for emergency calls may not be guaranteed; a base station has a limited number of channels. If no channels are preserved for accepting further calls, the portable part cannot access the base station.
- Depending on the implementation no priority facility may be available for emergency calls; in that case calls are handled on a "first come, first served" basis.
- In PAS Systems no user identity is available, only the cell information and the terminal identity; therefore no additional information about the citizen can be transmitted over the air interface.

The application layer identifier for DECT Systems is the CLI. The properties in regard to identification issues are analysed in clause 4.6. EN 300 175-5 [26] clause 13.4 specifies procedures for the handling of location information. In order to provide the most precise location information both the fixed and portable parts in a DECT system should implement these procedures. The only location information may be the one from the base station where the portable is registered. The portable part is located in these area that the base station may cover.

7.3.2 Simple Terminal Equipment (TE)

It is recommended that DECT terminals fulfil the requirements for speech performance as described in EN 300 176-2 [54]. DECT public systems, in addition, should support EN 300 824 [55], which puts extra requirements on external handover requirements and emergency calls.

In conventional residential DECT systems all authenticated portables ring simultaneously in case of an incoming call. ISDN based DECT systems may differentiate between portables due to individually assigned terminal identifiers (numbers). Thus, the latter provide better support for call-back requirement of emergency communications. A possible solution for conventional DECT systems might be that the base station maintains details of all outgoing emergency calls and uses this information to decide where to route subsequent incoming calls. Alternatively the PSTN network might supply an additional digit, which could be mapped from the base station to a portable in a similar manner to that used for PBX DDI.

7.3.3 PBX and complex Terminal Equipment (TE)

In business environments DECT PBX systems are used, having one DECT base station with multiple radio end points or a number of DECT base station connected together. The network provides routing, roaming and hand over capability using CENTREX functionality. All DECT portables in such business DECT systems are pre-authenticated by the manufacturer. It is possible to initiate emergency calls with these portables. However, it also should be possible to make emergency calls from non-authenticated terminals.

In business environments a special emergency service that is not generally defined (manufacturer dependent) can be deployed. Generally, in DECT PBX systems no priorities for special calls are defined, but it might be possible that manufacturers implement special message elements in the base stations in such systems to classify emergency calls, as proposed in EN 300 175-5 [26], clause 9.8.

In DECT PBX systems there is no location information available to identify the citizen. Only the radio that is used by the DECT portable is known (for example the user is expected to be somewhere in radius of about 300 m around the radio). In case of an emergency call the citizen should specify his location and this information has to be accepted and trusted by the PSAP.

In business environments DECT PBX systems may have a mapping and routing functionality (Direct Dial In) implemented so that in case of an incoming call the right portable is ringing. Therefore, calling back a citizen is possible, where this feature is implemented.

7.3.4 Access

In order to achieve best QoS DECT standardizes a technique called dynamic channel selection.

7.3.5 Installations

In ETR 056 [52] annex A clause 3.4 various scenarios of DECT systems are explained in more detail.

EN 300 176-1 [27] specifies limiting values of environmental conditions such as temperature and power supplies. Also in EN 300 175-2 [26] clause 5.2.3 requirements for minimum power under extreme conditions for transmission of physical packets are defined.

7.3.6 Other aspects

Proprietary, hybrid cordless telephone sets are beginning to emerge. Essentially these operate as DECT telephones when within range of their home base station and as mobile (GSM) telephones when out of range but within a subscribed mobile network coverage. Details of the functionality available on such terminals are not yet clear but for emergency communications purposes they should have all the facilities available to a normal GSM handset when connected to a mobile network and the full DECT feature set when operating to its home base station.

7.4 Telecommunications over cable TV infrastructures

It should be noted that this clause refers only to telecommunications services provided over the Broadband Cable (usually Hybrid-Fibre Coax - HFC) networks operated by cable TV network operators. Some cable TV network operators run what are essentially legacy POTS networks over a parallel network, usually using SDH access technology, but providing near identical services to those provided by other operators over the copper access network.

7.4.1 General aspects

Voice services over Cable TV infrastructures use VoIP techniques. In this case the telephone interface can be analogue (POTS), legacy digital (ISDN) or IP based. These services do not provide "life line" functionality unless an UPS system is installed at the user facilities due to the need for power supply for the associated cable modem.

Data or video transmission systems associated with this interface have the potential of being extremely useful in an emergency situation and could facilitate remote control or surveillance in environments where humans might no longer be able to work.

The traditional broadcasting function for radio and TV is a central support to the communication between authorities and citizens also in the cases where telecommunications services are available.

7.4.2 Terminal Equipment (TE)

Cable TV systems are based on a cable modem located at the customer premises. The CPE is connected to the cable modem. Therefore the location of the citizen in case of an emergency is normally well known unless the user takes advantage of the nomadicity feature of IP based systems. This feature may be blocked in some cases to prevent the uncertainty determined in the caller localization procedure. The architecture normally used in CATV based telecommunications networks was originally developed by CableLabs™ in the USA is known as IPCablecom™, the European version of which is specified in the TS 101 909-2 [29]. TS 101 909 parts 10 [30] (Event Message Requirements for the Provisioning of Real Time Services) and 18 [31] (MTA offering an interface to analogue terminals) and TS 101 909-24 [32] (MTA Basic Access ISDN Interface) specify relevant aspects in this context. IPCablecom supports priority mechanisms of emergency services as described in TS 101 909-2 [29], clause 4.4.2.

IPCablecom™ defines the possibility to adjust QoS parameters during a call. This is especially valuable in case of an emergency. When an emergency situation happens and all resources are blocked the CMS can use this feature to reduce the bandwidth available to normal calls in favour of emergency calls. IPCablecom™ has to support a list of element messages including those to emergency services as described in TS 101 909-10 [30], clause 7.1.

In most cases an emergency call is an on-net to off-net call. This means that the citizen is located in the cable network and the PSAP is connected to the PSTN or an alternative IP based network. In this case the emergency call is routed via the relevant gateways to the PSAP. In IPCablecom™ networks TS 101 909-10 [30], clause 9.2.1 defines that special trunks should be used for emergency calls and explains how this feature is used by the CMS.

The availability of calls to the emergency services is also very important. TS 101 909-17 [33], clause 8.1.7 describes a pre-emption technique where the access network is able to issue a pre-emption priority element to free busy resources in favour of emergency calls. It should be noted that it is the access network and not the MTA that is able to provide pre-emption priority elements.

NOTE: User controlled pre-emption is normally prohibited in public networks since end users cannot generally be trusted to determine their own priority.

7.4.3 Access

A possible solution in offering emergency services to the customer other than by dialling an emergency number is to implement a "red button" or "panic button" on the terminal device. This might be done either by implementing an additional button in newly manufactured analogue (POTS) or legacy digital (ISDN) phones or to assign the emergency number to an existing button. If the customer presses this button a string of digits representing the emergency number is sent to the CMS and the CMS provides the necessary services such as pre-reservation of bandwidth, routing to special emergency trunks and ultimately connection to the PSAP.

7.4.4 Installations

In general the cable modem located at the customer premises does not have a backup battery or UPS included. Line-power feeding the cable modem is not practicable and therefore it is not operational in case of power loss. This aspect is very critical in regard to emergency calls and if "life-line" service is necessary, installation of a UPS is essential. In TS 101 909-24 [32] clause 7 and TS 101 909-18 [31], clause 5.2 the implementation of backup batteries and minimum requirements for availability are recommended.

7.5 CATV infrastructures without telecommunications

7.5.1 General aspects

Cable TV networks were originally designed as broadcast media, providing one-way transmission from the head end to the many customers. Whilst most networks have been upgraded to provide bi-directional communications, some networks continue to operate in the broadcast only mode. This traditional Broadcasting function for Radio and TV is still a vital tool in communications between authorities and citizens in the event of a major and widespread disaster, for example, a flood, earthquake or terrorist incident.

More details can be found in clause 8.2.3 of EN 300 401 [18] and in clause 6.2.2 of EN 300 468 [37].

7.5.2 Terminal Equipment (TE)

Cable TV networks not supporting telecommunications can be used for broadcasting warnings and emergency related information in the same way as terrestrial broadcasting services. The architecture of such CATV systems offers only the possibility to carry information to the citizens but no interaction with them is possible because of the absence of upstream capabilities.

The possibilities of sending downstream information in CATV systems are explained in EN 300 468 [37], clause 3.1. The citizen has only to provide a DVB receiver, with or without a conditional access module, complying with the specifications provided in EN 300 401 [18] and EN 300 468 [37].

In EN 300 468 [37], clause 6.2.10 a country availability descriptor is described, providing the possibility for operators, working on behalf of the emergency authorities, to use this descriptor to make emergency warnings or information available only to a defined region. Since both DVB and DAB are broadcasting services no location and no identity information of the citizen is available; It is possible to use DVB or DAB receivers with or without a conditional access module. It is therefore strongly recommended that in case of an emergency the alerting information should not be scrambled, so that every DVB/DAB receiver can receive the broadcasted emergency information, regardless of its CA status.

EN 300 468 [37], clause 6.2.3 defines an announcement descriptor that can be used for emergency warnings and also gives the possibility of specifying the transport method. Use of these features can be valuable to support and reach endangered people in case of an emergency. It is possible to broadcast a text and/or video message and an additional audio message in case of an emergency.

7.5.3 Access

Standard receivers are used for receiving broadcast emergency information. Citizens need to connect additional television or audio equipment to watch or listen to the broadcast information. There can be no guarantee of reaching all (or indeed, any) of the intended targets in case of an emergency since their equipment may be switched off.

7.5.4 Installations

It is almost impossible to provide an always-on functionality for every one; although it may be recommended to provide a backup battery in every receiver so that all broadcasts can be received, this would represent a huge initial cost, an on-going cost of keeping the batteries charged and contribute significantly to national power consumption, and ultimately to global warming.

7.6 Ethernet

7.6.1 General aspects

Ethernet is widely used as a transfer technology/interface. Several other access network technologies, for example Broadband Cable, xDSL and Power Line Telecommunications (PLT) use the Ethernet interface to supply the connection towards the CPE.

Metropolitan Area Network (MAN) services using the Ethernet protocol are also emerging. Here IEEE 802.3 [46] CSMA/CD protocol is used for communication. In this case transport media such as fibre and twisted pair copper links and the corresponding standards are used.

Voice over Ethernet technology systems often use VoIP techniques. In this case the telephone interface usually is analogue (POTS), legacy digital (ISDN) or IP based. The application cannot be seen as a "life line" service unless a UPS or a battery back-up pack is installed at the user facilities. Ethernet allows the feeding of a single relatively small consumer load by using Power over Ethernet IEEE 802.3af [25], which allows the supply of a terminal with power from the next network node. Nevertheless remote power supply is a problem because the network nodes, for example switches need a back-up battery, an UPS or a connection to an alternative power circuit in case of electrical power outages.

In the context of the present report, Ethernet is seen as access network technology and the terminal is the PSTN voice terminal connected to an MTA or a directly connected IP phone.

7.6.2 Terminal Equipment (TE)

Ethernet systems are based on delivering connectivity for the CPE, which in most cases is running an IP based service such as VoIP. There is a broad range of CPE that may be connected, for example personal computers, IP phones, single line VoIP adaptors, etc.

7.6.3 Access

Ethernet networks form the transporting medium for higher layer applications using IP. Therefore, not all requirements of the Universal Service Directive 2002/22/EC [39] are applicable. Only the case where Ethernet is used as the access network is considered in the following clauses; cases where Ethernet is the link between different access network technologies and the CPE are not further discussed.

7.6.3.1 Performance

Ethernet is based on the usage of a shared medium with different available bandwidths depending on the physical media used to provide services. By default Ethernet provides a best efforts mechanism for all traffic, which means that all transported packets are treated in the same way. Additional Ethernet standards such as IEEE 802.1Q [47] (Virtual LAN) and IEEE 802.1p [49] (Traffic Class Expending) introduce QoS to the network. To best use the QoS capabilities of the Ethernet network, a network wide emergency VLAN could be provisioned by the network operator. The VoIP telephone or Analogue Telephone Adaptor (ATA) needs to be able to identify an emergency call and use this VLAN to initiate the call. This procedure will ensure QoS up to the first router. Beyond this point QoS is based on IP mechanisms.

7.6.3.2 High reliability and availability

The Ethernet network infrastructure is highly dependent on its power supply. In case of electrical power outages the network will normally fail. For core network components, a UPS or a connection to an alternative power circuit is a solution, but might be problematic since the Ethernet network has many more nodes than an ISDN or POTS network. Power over Ethernet (IEEE 802.3af [25]) is applicable only for feeding remote CPE with relative small power consumption, for example IP telephones; other CPE cannot be supplied and would therefore need either a battery-back-up-pack or a UPS as well.

7.6.3.3 Priority of emergency services

In Ethernet networks prioritization is possible and can be realized provided that the CPE can support existing standards such as IEEE 802.1Q [47] (VLAN) and 802.1p [49] (Traffic Class Expending).

7.6.3.4 Identity of citizens

Combining the information, which is held by both the access network and service provider, is the only way to confirm the identity of the citizen. The likelihood of malicious use is higher because just the endpoint terminal is authenticated in contrary to POTS and ISDN. Therefore a stolen account could be used to misuse emergency communication.

7.6.3.5 Location information

Location services can be provided but may be uncertain, because of the possibility of nomadic use. If the access provider is not the provider of the VoIP service, access to relevant information held by several operators may be required; this could introduce additional delays.

7.6.3.6 Security services for emergency communication

Since the Ethernet network is simply "transporting" the VoIP emergency call security is not an issue.

7.6.3.7 Testing of route to emergency service operator

Testing emergency services is also a service issue. It is not necessary to distinguish between real emergency communication and a test on the Ethernet network.

7.6.4 Installation

Since Ethernet is using different physical media, for example fibre and twisted pair copper, the relevant standards are the same as mentioned in clause 7.1.

7.7 xDSL technologies

7.7.1 General aspects

Voice over xDSL technologies systems often use VoIP techniques. In this case the telephone interface may be analogue (POTS), legacy digital (ISDN) or IP based. None of these cases will normally be seen as providing a "life-line service" unless a UPS is installed at the user facilities.

Data or video transmission systems associated with this interface have the potential of being extremely useful in an emergency situation and could facilitate remote control or surveillance in environments where humans might no longer be able to work.

In the context of the present report, the xDSL technologies are seen as access network technologies and the terminal as the PSTN (analogue or digital) voice terminal.

7.7.2 xDSL technologies associated with splitters

xDSL technologies associated with splitters share the physical infrastructure and therefore the power feeding circuits of other technologies such as PSTN analogue or digital access. XDSL splitters should not significantly disturb the power feeding of analogue and digital access to PSTN. The TS 101 952 series [51] describe the relevant technical requirements for splitters and DSL filters.

There is some interest in the market to develop users' xDSL splitters fed by the telephone line. At the present there seems to be no acceptance for a simple usage of the legacy remote feeding, unless the operators' xDSL splitters can offer an intelligent way of supplying power without affecting the feeding conditions of the legacy terminals.

7.7.3 xDSL technologies not associated with splitters

xDSL technologies not associated with splitters do not share the physical infrastructure with other technologies. In this case a remote power supply may be offered if the cable network used between central exchange and users' facilities allows. In other cases local power supplies will be required; a UPS or battery will be needed to support any possible life-line services.

7.7.4 Terminal Equipment (TE)

The TE associated with the xDSL service will depend on the required application and may range from modem supporting a single GUI-based terminal to a LAN consisting of a significant number of devices.

On xDSL services employing splitters, the TE on the physical connection to the central exchange will usually be an analogue telephone and the comments in clause 7.1.4 will apply. This telephone will normally have power feeding from the exchange and thus support lifeline services without dependence on local power.

On xDSL service without splitters, there will be no TE relying directly on the physical connection. Some power feeding capability may exist but this is unlikely to be sufficient to support more than the modem and a simple TE such as a VoIP telephone. Any additional equipment connected to the modem will require local power with battery back-up or UPS for critical applications.

7.7.5 Access

The xDSL access will usually be carried on the copper-based local loop from the user's premises to his local telephone exchange; there are no special requirements other than certain distance limitations that are dependent on equipment types, line loss and cross talk.

7.7.6 Installations

The user installation will normally require one or more splitters to separate the voice frequency signal from the high frequency xDSL signals present on the serving copper pair. Depending on the network operator's requirements, a single "high-pass/low-pass" splitter may be used at the NTP and the voice and xDSL cabling separated from that point to each of the CPE locations. Alternatively, each telephone can have a splitter associated with it, the xDSL modem being connected to the "high-pass" side of one of these splitters, as appropriate to its location (only one xDSL modem may be connected to the service).

The installation should not normally have an impact on the effectiveness of a possible emergency communication but, with the increasing number of telecommunications applications on the terminals, the citizen may frequently not notice that the capabilities offered by the network interface may well not be as high as the total loading factor of his home installation. Inappropriate installation at the "do-it-yourself" level, may introduce additional risks to the quality and availability of the telecommunications service.

7.8 Power Line Telecommunications (PLT)

7.8.1 General aspects

Power Line Telecommunications (PLT) is a part of an access network, carried on the low voltage (230/400 volts) distribution network between the transformer station and the customer. It is organized in a cell structure, which means that several end user's modems are connected to one head end by using the same media. This fact implies that the bandwidth provided from the head end is shared between all active end users.

As physical interface towards the backhaul and the users CPE Ethernet (10/100 Base-T) is used. Towards the end user a USB interface is also possible. For the Ethernet network the PLT network acts as a transparent Ethernet bridge.

Voice over PLT technology systems often use VoIP techniques. In this case the telephone interface is usually analogue (POTS), legacy digital (ISDN) or IP based. The application is not normally seen as a "life line" service unless a UPS or a battery back-up pack is installed at the user facilities.

Data or video transmission systems associated with this interface have the potential of being extremely useful in an emergency situation and could facilitate remote control or surveillance in environments where humans might no longer be able to work.

In the context of the present report the PLT technologies are seen as access network technologies and the terminal is the voice band PSTN (analogue or digital) voice terminal.

7.8.2 Terminal Equipment (TE)

PLT systems are based on a PLT modem located at the customer premises. The CPE is connected to the PLT modem. Therefore the location of the citizen in case of an emergency is normally well known unless he takes advantage of the nomadic feature of IP based systems. This feature may be blocked in some cases to prevent the uncertainty determined in the caller localization.

Since the PLT modem offers IP connectivity it is necessary to use an additional adapter (MTA) to connect analogue (POTS) or legacy digital (ISDN) phones to the PLT network. Otherwise it is possible to use an IP phone that is connected directly to the PLT modem using the IP interface.

7.8.3 Access

The PLT network represents a part of the telecommunication chain, which is needed to provide emergency calls. Therefore not all requirements of the Universal Service Directive 2002/22 EC [39] are applicable. The following sub clauses give an overview on issues related to emergency communications requirements (see clause 6.3).

7.8.3.1 Performance

PLT is using a shared access medium to provide different services; therefore an obligation for emergency communication needs to be defined which includes the fact that all emergency communications have to be treated with the highest possible priority.

7.8.3.2 High reliability and availability

PLT networks rely on the low voltage power distribution network, which is frequently a meshed network to provide a degree of resilience, but this arrangement is not standardized in all low voltage networks and cannot be guaranteed. Also, local power failures due to incidents in the household may have an impact on reliability and availability. Battery-back-up-packs or a UPS can solve this problem.

7.8.3.3 Priority of emergency services

In PLT networks prioritization is possible and already realized, but the transfer of the priority request from the endpoint (for example VoIP phone) to the PLT network and from the PLT network to the backhaul has to be standardized. Possible solutions to this issue are the use of existing Ethernet standards such as IEEE 802.1Q [47] (VLAN) and IEEE 802.1p [49] (VLAN prioritization). These or equal techniques can be used to ensure that the priority requirements of emergency communication are fulfilled by the PLT access network.

7.8.3.4 Identity of citizens

The identity of the citizen can only be retrieved by combining the information that is held by both the access network and service provider. The likelihood of malicious use is higher because just the endpoint terminal is authenticated in contrary to POTS and ISDN. Therefore a stolen account could be used to misuse emergency communication.

7.8.3.5 Location information

Location services can be provided but may be uncertain, because of the possibility of nomadic use. PLT networks can be set-up in a way that the citizen can take his modem and plug it in any socket in a fully developed area to get service. In this case the location information stored in the access provider's database is no longer valid. If the access provider is not the provider of the VoIP service, the access to the relevant information held by several operators may be required; this could introduce additional delays.

7.8.3.6 Security services for emergency communication

Since the PLT access network is just "transporting" the emergency communication security is not an issue in this context.

7.8.3.7 Testing of route to emergency service operator

Testing emergency services is also a service issue. It is not necessary to distinguish between real emergency communication and a test on PLT networks.

7.8.4 Installations

Theoretically PLT modems can be used in every socket in the costumers building. Therefore installation should not be an issue. In reality a PLT modem works in approximately 90 % of all sockets in a household. In this case it might happen that an emergency call attempt cannot be initiated because of the absence of the uplink.

7.9 Fibre to the kerb/home

7.9.1 General aspects

Optical fibre may be used as an access technology, either providing connectivity from the network operator's central facility to a shared distribution node close to the end-user's premises (FTTK) or as a dedicated connection to his home or business (FTTH).

In the case of FTTK, the network operator will be responsible for the secure powering of the distribution node and may provide power to the end customer's terminal devices. FTTH solutions require customer provided power, not only for the terminal devices but also for the network termination equipment. For emergency communications purposes, such power supplies need to have a minimum standby capacity to maintain full network connectivity for the maximum time expected to taken by the subsequent emergency calls, and preferably until the likely arrival of the emergency services. The end-user's requirement for standby capacity for business continuity reasons will, however, usually be greater than this.

7.9.2 Terminal Equipment (TE)

TE used in FTTK/FTTH is essentially similar to that having the equivalent functionality on networks using other access technologies. The operation of and the facilities provided by the terminals will be identical to those on other networks, limited only by any restrictions in the services provided by the network operator. Voice terminals requiring line power will normally be fed from the line card in the network termination equipment whether it is located in the street or at the customer premises.

7.9.3 Access

The FTTK or FTTH network termination equipment itself has no bearing on the present document and is generally recognized as being part of the access network, providing the appropriate network interfaces, as required for the end-user's services. The network operator usually provides it whilst the end-user provides the terminal equipment.

7.9.4 Installations

Installation of the end-user TE on FTTK/FTTH access networks will follow normal user requirements. Installation of the network termination equipment in the FTTK case will be in accordance with the network operator's normal practices. FTTH network termination equipment needs to be installed in a dedicated, secure environment, protected from possible attack by anyone wanting to disrupt communication from the premises and the greatest extent possible from such perils as flood, fire, etc. As noted in clause 7.7.1, arrangements should be made for a secure power supply to the equipment. In practice this will usually mean dedicated primary power feeds to duplicated rectifiers charging a standby battery, with appropriate secondary distribution arrangements.

7.10 Broadband Wireless Access (BWA)

7.10.1 General aspects

Broadband Wireless Access (BWA) is one of the access technologies shown as BWA in the figure 1. BWA represents a range of fixed wireless access technologies either providing connectivity from the network operator's central facility to a shared distribution node close to the end-user's premises or as a dedicated connection to his home or business. There is a variety of such systems operating in licensed and unlicensed frequency bands, over a range of bandwidths and using a number of different modulation techniques. Such systems may operate on a point-to-point basis or as point-to-multipoint networks but all may be regarded for the purposes of the present document to provide access network connectivity and are transparent to the type of traffic being carried.

Wireless solutions invariably solutions require customer provided power, not only for the terminal devices but also for the network termination equipment. For emergency communications purposes, such power supplies need to have a minimum standby capacity to maintain full network connectivity for the maximum time expected to taken by the subsequent emergency communication and preferably until the likely arrival of the emergency services. In the case of point-to-point systems, which are more generally used for business customers, the end-user's requirement for standby capacity for business continuity reasons will, however, usually be greater than this. Point-to-multi point systems serving multiple customers should always be provided with a standby power system of adequate capacity.

7.10.2 Terminal Equipment (TE)

The TE used in fixed radio access networks is essentially similar to that having the equivalent functionality on networks using other access technologies. The operation of and the facilities provided by the terminals will be identical to those on other networks, limited only by any restrictions in the services provided by the network operator. Voice terminals requiring line power will normally be fed from the line card in the network termination equipment whether it is located in the street or at the customer premises.

7.10.3 Access

The fixed radio access network termination equipment itself has no bearing on the present document and is generally recognized as being part of the access network, providing the appropriate network interfaces, as required for the end-user's services. The network operator usually provides it whilst the end-user provides the TE.

7.10.4 Installations

Installation of the end-user terminal equipment in fixed radio access networks will follow normal end-user requirements. Fixed radio access TE needs to be installed in a dedicated, secure environment, protected from possible attack by anyone wanting to disrupt communication from the premises and the greatest extent possible from such perils as flood, fire, etc. Such equipment is often in rooftop cabins, adjacent to the necessary antenna systems. As noted in clause 7.9.1, arrangements should be made for a secure power supply to the equipment. In practice this will usually mean dedicated primary power feeds to duplicated rectifiers charging a standby battery, with appropriate secondary distribution arrangements.

7.11 Other less deployed terminal access technologies

The emergency features as described in clause 4.4.2 can be deployed in terminals with other access technologies. It is nevertheless recommended to deploy these features primarily in terminals with harmonized interfaces in widespread use, such as those referred to in clause 7. This will facilitate the earlier deployment and a wider coverage, therefore better service for a wider population.

NOTE: Technologies using IP based communication are normally interconnected to traditional technologies, in particular to the analogue PSTN terminals. These interconnections should strictly respect the needs reflected in the standards describing the interfaces offered to such popular terminals. Many of these standards specifying such popular interfaces are cited in the present document.

8 Service connectivity

8.1 General

This clause analyses the impacts of the service requirements already discussed and examines the user expectations for service connectivity in emergency situations. The technical and functional requirements for terminals as described in clauses 4.4 and 6.3, whilst this clause describes the network issues required to support them. The various technologies employed introduce a wide range of possible network implementations that are partly analysed in clause 9.

8.2 Availability

Availability is important for all types of terminals, as are the mechanisms to ensure that terminals continue to be operable in disaster situations. Local power outage is a notorious cause of failure and the use of line fed equipment is desirable since the central location is likely to have a relatively robust source of power. The measures for protection of IP based terminals against power failure are the same as those described in clause 7 for the various technologies.

8.3 Robustness

Publicly available terminals such as roadside emergency telephones should be as robust as possible to deter vandals and should be easy to use, perhaps having only RED and YELLOW buttons activating a hands-free communication channel. TS 102 302-1 [20] specifies this requirement for an emergency telecommunications network.

8.4 Reliability

TE reliability should be maximized by careful electrical and mechanical design; in the case of publicly available terminals proper consideration of their adverse environment should be taken into account. Networks should be arranged to provide diverse routing wherever practicable and to be equipped with adequate back-up power supplies.

8.5 Routing

Emergency communications should be correctly routed, preferably with network diversity, to the appropriate PSAP, which may not always be the physically nearest one. In the event of network failure or PSAP overload, adequate arrangements should be made for diversion of traffic to an alternative centre.

8.6 Priority of emergency communications

Priority of emergency communication is vital. Network operators should ensure that such calls always take priority over all other traffic, either by the use of permanently reserved bandwidth or "on-the-fly" reservation using the QoS mechanisms where these are available in the network infrastructures. In cases of serious network congestion, non-emergency traffic should be disconnected where necessary.

8.7 Quality of Service (QoS)

Emergency communication should not normally be worse than that of basic communication services, according to SR 002 180 [1], but in the extreme, poor communication should be regarded as better than none at all.

Call set-up time and speech quality are the parameters most likely to be commented upon by the casual user. Long call set-up times will encourage the caller to attempt to clear his initial call and try again, leading only to further confusion. Poor speech quality (volume, clarity, regional accents) will result in unnecessary repetition and possible confusion of verbal information. Time to answer is also important; most users expect some indication (ring tone, for example) that their call has been accepted but then expect to be answered quickly.

Accuracy of any data that is automatically transmitted with the call is paramount, both as regards its source and transmission and display at the PSAP.

8.8 Localization

Accurate location information is very important in directing emergency teams to the citizen, who may not be able to accurately assess or describe where help is needed. Automatically generated location information also assists in the routing of emergency communication to the most appropriate PSAP and provides an important tool to apprehend malicious callers.

Localization is the process of defining the location of the citizen wanting to initiate an emergency communication. The citizen may be using a fixed TE, he may be mobile, he may have roamed from his home network to another compatible mobile network or he may be nomadic, that is, connected on a semi-permanent basis to a "foreign" network at a fixed location. The identifiers used in communications systems are discussed in clause 4.6 where some risks of insufficient accurate caller localization are identified as well as some initial suggestions to overcome difficulties.

The location of fixed line callers can normally be determined by reference to a central database relating telephone numbers or other identifiers to a physical address. This may not always be correct, especially in private networks; refer to clause 9.1 where this issue is further discussed.

Mobile (PLMN) networks normally return cell location information to the PSAP when offering the emergency call. Mobile users on their home own network or roamed to other networks are treated in the same way. Due to the nature of cellular communications, this can cover a large area and the work is underway to more accurately determine mobile location should be expedited.

Only IP-based terminals can be expected to be nomadic and their location information may not be obtainable in a straightforward way and potential solutions are discussed in clause 6.3.6.

9 Private Networks (PN) and Home Networks (HN)

9.1 Private Networks (PN)

9.1.1 General aspects

Private Networks (PN) are commonly used by companies and other big organizations to support their business operations and historically were mainly voice networks formed by the interconnection of the PBXs at different sites. Such PN may be subject to national regulation which typically ends at the NTP. Hence, the following comments, whilst generally correct, may not all be applicable to all PN and not all the recommendations made will be appropriate in all cases.

More recently, private data networks have become commonplace with the interconnection of the LAN (local area networks) at the various business sites either using dedicated lines or technologies such as Virtual Private Network (VPN). The consequence of these changes is that service providers and network operators are now confronted with their customers having complex and extensive networks, often supporting data and voice services, not just simple terminals, connected to the public network. Therefore the various service requirements and also emergency service requirements may have to be met by the owner or operator of the PN rather than by the public network or service provider, a situation made even more complicated by the fact that the organization using the PN may not own or maintain the network infrastructure. However, for the purpose of the present document, the organization will be referred to as the PN network operator.

PN may include a variety of different technologies and topologies. Despite this diversity there are some common points applying to all PN:

- PN are operated primarily to give service to a closed user group.
- PN may connect different sites in one city, different sites across one country or many different sites worldwide. These sites may include some, which do not have their own connection to a SP which then introduces the nomadicity problem to the PN.
- Except in the case of closed networks used for specialized purposes, PN should have at least one connection to an external public network. In the majority of cases many connections are made to a variety of different network types.

- The operator of a PN has the exclusive knowledge of his network and therefore should be responsible for providing the required information, as for example Localization and Identification. The operator of a PN should ensure that the essential requirements for emergency communication described in clause 6.3 of the present document are fulfilled.

- Availability: It is important that all possible measures are taken to ensure that emergency communications can be completed at all times.

- Routing: Large PNs typically have a number of "break-out" points to the public network; operators should ensure that emergency communications are routed to the most appropriate one.

- Prioritization: It is important to enable emergency communication even in congested networks, adequate mechanisms should be implemented in the PN.

- Quality of Service: A range of QoS issues, including reliability, speech quality and call set-up time, should be fully considered in the design of PN and their interconnection with public networks.

- Identification: It may not be readily possible to identify the user of a particular TE in a PN, other than by accepting information given by the caller, since the majority of TE may be accessible to many persons in the business. Conversely, it is to be hoped that caller identification is less of an issue in PNs than in the public network due to the lower probability of malicious calls.

- Location Information: The operator of the PN is responsible for the localization of the specific TE, either fixed or roaming. The location information should be as accurate and precise as possible. For special cases such as emergency communication from remote sites using a VPN connection, the location information should at least include an indication that the session is from a specific remote site.

9.1.2 PBX in Private Networks (PN)

PBX based PN connected to the PSTN are well established in business and despite the limitations expressed above, local procedures have been developed by most companies and organizations for handling outgoing ("citizen to authority") emergency calls. These may be handled using an internal emergency number, which gives priority connection to an attendant who takes details from the caller of the nature of the emergency and then calls the required emergency service or PASP. This process inevitably introduces delay but does provide some degree of verification of the caller's location and identity. An alternative method, which is not permitted in some countries, allows the PBX extension user to dial the PSTN access prefix digit (usually "0" or "9") followed by the public emergency code (usually "112" in Europe) giving him direct access to the PSAP. The PSAP operator will usually receive a CLI from the caller. However, this may be the actual DDI number for the PBX extension (where such facilities are in use), the published directory number for the enterprise operating the network, a number specifically assigned by the enterprise for receiving call-backs (presentation number) or a PSTN number relating to the PN to PSTN gateway used by the caller.

None of these numbers is capable of identifying the caller. The published directory number will identify the organization but not necessarily its location, whilst the presentation number is of no value. Only the first of these numbers is capable of identifying the calling station; the only way of identifying the caller is by voice and the response may be unreliable. Where the PBX has DDI facilities, it is also possible to offer call back functionality since the terminal is always on. The actual location of the calling extension will only be verifiable by the company operating the PN. The caller may be asked to give his location but this may not be correct, either due to lack of accurate knowledge or due to malicious intent by the caller. These problems are long-standing and the present document will make no attempt to find their solutions.

Under emergency conditions, issues may arise where the PBX has no available internal links or where its connectivity to the PSTN is fully utilized. Call Priority Interruption (SS-CPI) and Call Priority Interruption Protection (SS-CPIP) services are defined in EN 301 655 [28] as supplementary services that can be used in intra-corporate telecommunications networks. SS-CPI can be used to allow a priority call request to override other traffic if the service is invoked by the caller during the call set-up phase. The request can be made either by pressing a special key or feature access code, or when the called number is recognized by the network as an emergency number. Call Priority Interruption Protection (SS-CPIP) can be invoked either by the calling user during call set-up or the called user (PSAP) and its use is recommended during an emergency call so that the continued availability of PBX resources is guaranteed.

In spite of the possibility of their misuse, it is recommended that SS-CPI and SS-CPIP functionality is made more widely available on PBXs. Although this will not overcome the problem of many users not knowing how to invoke the facility in an emergency, it will provide an additional resource for those who do.

Emergency incoming calls ("authority to citizen") will normally be addressed to the listed directory number of the enterprise operating the PN. In some high-risk industries, a special incoming-only number is provided for use by emergency authorities. This number alerts the PBX attendant separately from other incoming lines and therefore can be given priority treatment. In the absence of such a facility, the emergency authority has to compete with "normal" traffic for attention by the PBX attendant; this can obviously introduce delay into the system.

9.1.3 IP services in Private Networks (PN)

Private IP-based networks are also well established in business. As noted above, such networks may be small (with only a few terminals, though not necessarily in one location) or extremely large (many thousands of terminals, located worldwide). Except for some specialized, isolated networks, IP-based PNs will have at least one, and often many, gateways to public IP networks each having firewall isolation.

Private IP networks usually allocate IP addresses to TE from one of the IETF specified private address ranges. Only the public IP addresses allocated to the gateways by the public network operator are visible to the outside world. For non-voice applications there is not usually any equivalent of the PBX attendant facility.

The properties of IP addresses in regard to the identification of the citizen are described in clause 4.6. Further identifiers may be either CLI or application specific. The properties of CLI are discussed in the same clause. The degree of identification using application specific identifiers may differ depending on whether user authentication is required and the TE used.

Voice applications on IP networks are emerging but are presently largely confined to the PN with one or more gateways to the PSTN. From outside the PN, these networks are practically indistinguishable from PBX based voice networks, with one important difference. An IP terminal can be plugged on to its host network at any point, thus neither its IP nor MAC addresses are any indication of its physical location.

In the case of an emergency call, therefore, any location information will be dependent on the user providing the correct details, with no possibility of that information being verified automatically. Even the PN operator will not necessarily be aware of the physical location of the TE, let alone the identity of its user.

In regard to the other requirements for emergency communication the assumptions of clause 9.1.1 are true. For the time being mostly voice services have been considered for the use of emergency communication for PNs. With the increasing distribution of IP services also the use of for example Instant Messaging (IM), or E-Mail will have to be considered for the connection to PSAPs.

9.2 Home Networks (HN)

9.2.1 General aspects

The term Home Network (HN) includes the many different technologies and topologies used for a variety of services in the household environment. This can include, but may not be limited to, the following services:

- IP based services, for example, Email, VoIP, Internet access, multimedia streaming and webcam operation.
- In-home IP-based computer wired and wireless networks, including public network connectivity.
- Management of internal and external voice communications, including connectivity to public networks, for example copper-based access, HFC cable systems, wireless networks, etc.
- Remote control of heating and air conditioning services, shutters, lighting, domestic appliances, etc.
- Control and networking of domestic entertainment services, including connection to and distribution terrestrial, satellite and cable delivered services.
- Control and networking of locally generated domestic entertainment services (for example VCR, DVD and CD players).
- Remote monitoring of home security (intruder and fire alarms, surveillance cameras, door controls, personal safety systems and equipment alarms).
- Automatic Meter Reading (AMR) for power, water, gas and district heating.

- Power quality management for distributed power generating units such as for Fuel Cells and Solar panel.

With the exception of locally generated entertainment services, all of the services require at least one connection to the "outside world" in order that they should work effectively, for example, an intruder alarm with no connection to a monitoring station will not be effective as one with such a connection.

Due to the interrelationships and interactions between the many different in-home services, the definition of a gateway device for the interconnection of all services and networks would seem to be a logical consequence. This gateway would run an application capable of managing the various interactions needed to operate Home Networks.

In case of an emergency communication being initiated or an abnormal situation detected anywhere in the Home Network, the gateway together with its application should ensure that the appropriate connection is established and that all the requirements of an emergency communication are met. Because of the importance of emergency communication PSTN and VoIP services in Home Networks will be examined more closely.

The HN owner has the exclusive knowledge of his network. Although from an external viewpoint, this is likely to be much simpler than even the smallest PN, it may include some very complex internal connectivity. The requirement for localization and identification will usually be less stringent but the responsibility for its provision should fall on the PN owner, who should also ensure that the essential requirements for emergency communication described in clause 8 of the present document are fulfilled.

- Availability: It is the HN owner's responsibility to ensure that all possible measures are taken to ensure that emergency communications can be completed at all times. The most likely problem area is that of power to such network elements that do not have in-built back up, such as DECT telephones.

- Routing: HNs may have more than one voice connection to the public network. The HN owner should ensure that emergency communications are not routed via a network that does not provide PSAP connectivity.

- Prioritization: The HN should have the capability to provide prioritization to emergency communication, even in congested network conditions. Adequate mechanisms should be evaluated or may be taken from other technologies.

- Quality of Service: will not usually be an issue in the home environment but care should be taken to ensure that there are no cabling issues, external interference with wireless systems or gateway connectivity problems which may disrupt emergency communications.

- Localization and Identification will not usually be an issue in the home environment.

9.2.2 Switched voice services in Home Networks (HN)

PSTN services in the home are well established and usually consist only of a few parallel, wired telephones or a small PBX or key-system, usually serving only a single household. Outgoing ("citizen to authority") emergency calls can normally be made from any TE by dialling the public emergency code (usually "112" in Europe) giving direct access to the PSAP (key-systems may require a prefix digit). Problems may arise if the PSTN line (or lines) is in already in use or if a parallel extension has been left "off-hook". An important issue is that of the power requirement of DECT telephones which are used extensively in the home. Perhaps, due to their physical similarity with GSM telephones, users do not readily appreciate this need and therefore do not realize that they cannot be used during power outages (see clause 7.10).

The PSAP operator will usually receive the caller's directory number (whether listed or unlisted) as a CLI and this will identify his street address. The actual location of the caller within the household can only be ascertained by asking him. The response may not be correct, either due to lack of accurate knowledge or possibly due to malicious intent by the caller. These problems are long-standing and the present document will make no attempt to find their solutions.

Emergency incoming calls ("authority to citizen") will normally be addressed to the listed directory number although facilities exist for a second number to provide an alternate ringing cadence or some other alerting mechanism. Emergency authorities do not usually have any pre-emption capability, thus if the line is already in use, they are not able to contact the citizen.

9.2.3 IP services in Home Network (HN)

In regard to the requirements for emergency communication the assumptions of clause 9.2.1 are true. Also in the home environment new services based on IP will need to be analysed for their use in emergency communication as for example Instant Messaging (IM), or E-Mail.

10 Installations and infrastructures

10.1 Physical installations/cabling

Besides the availability and reliability of end-user terminals or network nodes the resilience of the infrastructure against external influences is critical to system performance. Each part of a system should satisfy certain minimum requirements. It is not within the scope of the present document to propose such requirements. The main standardization committees for cabling issues are:

- ISO/IEC;
- CENELEC;
- TIA/EIA;
- ETSI.

In CENELEC, the European Standardization committee, TC 215 has published EN 50174 [50] on IT cabling installation. Part two specifies "Installation planning and practices inside buildings" and part three "Installation planning and practices outside buildings". Future parts of series EN 50173 [53] will specify particular requirements of cabling systems for residential and industrial premises as well as for data centres.

Issues for standardization may include:

- Resistance against torsion, bending, coiling, impact.
- Temperatures ranges.
- Resistance against moisture, hydrostatic pressure.
- Test methods to verify the above.

10.2 Device configuration and provisioning

End-user devices and network nodes should be provisioned with all configuration options and profiles required in order to enable emergency communication. The end-user should not need to interact in any way. This should be the case in particular, when a service provider (SP) delivers also the device to the end-user. If "zero-touch" provisioning cannot be achieved the end-user should first be given notice that emergency communication is not possible at that moment and second the information required to enable emergency communication himself, if possible.

11 Information to the citizens

Effective emergency communication is crucial during incidents. Therefore, it is most important that the citizen:

- Is informed about what he has to do in case of an incident so that he reacts in an appropriate way.
- Understands information delivered to him during an incident.

Instructing a citizen how to react in case of an emergency requires that there is information that prepares the citizen to do so. This information should be spread as widely as possible so that as many people as possible know exactly what to do, for example on emergency call posts (ECP). People also need to be informed about the kind of information they are expected to give to the PSAP. This should include:

- Identity of the citizen.
- Location of the citizen.
- Type of incident.
- Impact of the incident; for example how many people are injured and how severely.

For information that is known to the TE or the network (identity, location information), it should be provided to the PSAP (for example GPS capabilities). Clause 4.4 discusses TE capabilities in this regard.

For information that is delivered to people in an emergency situation it is vital that such information is very well structured and easy to understand (as simple as possible).

11.1 From the authorities and public institutions

Possible placements of information regarding emergency issues are advertisements in local media such as newspaper, radio, and television. Advertising for different emergency services besides the well-known emergency number 112 could also be done in distributing brochures in hospitals, at medical doctors and in public spots such as sport arenas. These advertisements should contain contact information how to contact a PSAP in case of an emergency. If there are location specific emergency services provided, such as special health care, this information should also be included in the advertisements, especially if there are different service numbers to use. If emergency services are provided on a call back basis this information should also be included.

11.1.1 Telecommunications authority

Authorities should publish general information regarding availability of emergency services in the country. This information could be published in form of brochures. It is important that those brochures contain all necessary information such as contact numbers, special emergency numbers and a description how to initiate emergency communication. Such brochures could be placed at public call posts or at hotspots.

11.1.2 Civil protection

In case of disasters that have impact on a large number of people all established civil protection plans and methods such as audible warnings (sirens) are used. Furthermore civil protection should inform the public in regular steps via media campaigns how to react when siren alarms are used. Broadcasting of emergency warnings could be done via newsflashes in television or radio.

11.2 From telecommunications operators or broadcasters

Information about available emergency communication services may be crucial to users of a service. In particular if roaming/visiting users or new users are concerned. Therefore, service providers (SPs) should provide information to all service users about existing emergency communication means.

There are different ways to inform people. They also depend on the kind of TE that is used. They include:

- Push Services; for example Broadcast services.
- Pull Services; for example information web site.
- Off-line; for example via information handed out on service subscription with the contract.

SP may also offer information about emergency systems and communication services for example via Hyperlink to a web site dealing with such issues. The scenario may look as the following: when a citizen accesses the SP's service he may be redirected to the home page of the SP.

An information page should offer:

- Multi-lingual support.
- Helpdesk numbers.
- Information regarding availability of emergency services.
- Emergency service manual.
- Current status of the emergency system.

Such a service should be open for all citizens and not bound to any service subscription or any other type that requires payment.

A service subscriber may also at the time of subscription be given emergency service related information. This may either be through for example an information sheet that he gets in addition to the contract.

11.3 From manufacturers

There are some key factors that should be provided from the manufacturer of telecommunications equipment. This information should be made available to the customer in the delivered manual. The manual should also contain descriptions of applications that are designed for emergency services and available when using the hardware. Step by step guides explaining in detail how to use the equipment in case of emergency should also be provided from the manufacturer. All kind of restrictions especially warnings and unavailable functionalities should be included in the delivered documentation. A listing of operator dependent and operator independent emergency services should also be added.

11.4 From special organizations

Profit and non-profit organizations such as private medical rescue services or private security services might also be locally available. These organizations may advertise their emergency services in local newspapers, flyers, radio and television programs. The advertisement should describe exactly how the individual emergency service is to be used, if there are any charges and which emergency services are offered.

12 Commonly identified concerns

12.1 Power dependence

With the development of new technologies such as solar or wind energy in parallel with the strengthening of existing power distribution, power dependence may be in the future solved by an increased locally generated energy.

12.2 Protection of the installations and infrastructures

Public protection of emergency systems, infrastructure and universal service require large investments. Thus, the required reliability and cost are linked reciprocally. For protection issues and availability of emergency services it is recommended that redundant cabling be used. To protect installations and infrastructure against and under special environmental conditions a special coating is useful. This cabling method is also a valuable aspect in ensuring high signal quality and connectivity. By using shielded coaxial cables electromagnetic influences can also be minimized.

One further aspect is the protection against misuse and criminal use. The owner of facility where emergency equipment is located or owner of the equipment itself should be responsible to take measures against vandalism and misuse, for example a telephone in a supermarket.

12.3 User perception

With new systems enhancing user facilities with an increasing number of features, there is an increased risk of impairments in the base services ensuring emergency communications. The cause may be related to physical aspects, as for example inappropriate cabling practice or undue actions in the existing installation. Also modifications of configuration settings made by end users in order to introduce new facilities may result in emergency service interruptions. It is therefore recommended to design telecommunication systems in a manner that user actions cannot interfere with the installations and provisions that ensure emergency communications.

12.4 Trust in user identity and location

The CLI information delivered from most fixed line telephones, when related to the subscriber's address as recorded in the SP's database, has customarily been taken as conclusive evidence of the location of the emergency caller. It has usually not been necessary to ask the caller for his location (except as a cross-check). A number of developments have made CLI less trustworthy as a means of location. Remote breakout from private networks (where traffic is carried over a private network to a point near it destination, to take advantage of lower tariffs) and the more recent advent of IP-based, "portable" services are but two examples.

More reliance therefore has to be placed on the caller's responses when questioned as to his location and identity. This imposes an additional workload on the PSAP call-taker, who now has to make a judgement as to the validity of the call if the information given does not fit the expected profile. It may be seen as ironic that whilst a great deal of work is underway in various for a to improve the accuracy of mobile caller location, location of supposedly fixed lines is becoming increasingly difficult.

12.5 Data protection override

Article 10 of the EC Data Protection Directive (EC 2002/58/EC [59]) already provides (*inter alia*) for emergency authorities to override temporary or permanent suppression of caller's CLI information, as it relates to voice calls made to emergency services numbers. Existing regulations may be ambiguous or impose restrictions on the data available. These need to be clarified to ensure that when an emergency call is made, all relevant information about the telephone line, its subscriber and the caller can be lawfully obtained from any available source. Research may need to be undertaken to ascertain the range of likely holders of relevant information, who may include such bodies as tax and social security offices, medical authorities and local councils. Secure systems need to be put into place to ensure the timely delivery of this information and to ensure its security from improper disclosure following the emergency.

13 Conclusions

13.1 General

The rapid evolution of ICT technologies and the greatly reduced level of regulatory measures in general, have brought to the market a number of solutions. On one hand these solutions are welcome and bring new opportunities in but if standards and, in some cases regulatory measures, are not clear, there might be little benefit for the population in general.

Emergency communications can easily benefit from standardized solutions, in particular those which ensure:

- Assignment of a clear priority to emergency communications (see clause 8.6).
- Reduction of all impediments and costs to the citizen in the emergency situation (see clause 4.1).
- Positive identification of the citizen, his location and his calling line (see clause 4.6).
- The clear identification of special emergency keys or features and specification of their functionality (see clause 4.4).

The analysis in the present document shows that there is no single and straightforward solution for emergency communication. For POTS and ISDN, the situation is reasonably defined. The situation for telecommunication services using IP based transport mechanisms is more complex. There are many different technologies that interact with each other in order to provide a telecommunications service. These technologies have different properties and influence each other also in regard to the requirements for emergency communication. Any one technology may have different properties or shortcomings depending on the technologies it interacts with in a given situation. Moreover, the usual Internet business model allows more than one SP to be involved in the fulfilment of a service without the requirement of a business relationship between them. This leads to complex distribution of areas of responsibility, for example which provider is responsible for delivery of caller location information.

The issues that may be covered by the terminals are:

- Availability of the terminal equipment, for example protection against power outage by provision of battery packs (however this does not solve the power issues in the access and/or core network).
- Emergency communication facilities such as dedicated buttons, automatic alarms and emergency calls through special buttons programmed to signal emergency calls.
- Use of special applications available on the TE to obtain information, for example sensors for certain environmental conditions, etc.
- Request different priorities of a service for emergency communication.
- Means to identify the user of the terminal, for example the keypad to let users enter a code.

The issues that concern the access network are:

- Availability of the network infrastructure, for example in case of a power outage or some other serious disruption.
- Specified minimum levels of QoS.
- Means to deliver accurate location information.
- Means to deliver identification of the TE used.

The issues that concern service providers are:

- Routing to the most appropriate PSAP.
- Routing to an alternative PSAP in case of network overload or system outage.
- Identification of the end-user service account.
- To guarantee emergency communication connection without delay.
- To provide very good media quality and ensure accuracy of all available additional information.

This latter point is a matter that concerns almost every element in the telecommunications network and is therefore also the subject of interest to many different standardization bodies and other interest groups including service providers, network operators, manufacturers and regulators.

13.2 Issues arising from analysis

Arising of this technical report there are some issues that may result in further standardization efforts in order to improve emergency communication capabilities:

13.2.1 Additional SMS profile for emergency communication

Currently SMS messages are always routed to the SMS-SC in the network normally serving the user (home). When SMS is used for emergency communications messages should be routed directly to the nearest SMS-SC, even when originated from a roaming mobile device. Therefore, the use of an SMS for emergency communication requires the capability to store more than one profile for SMS.

13.2.2 The introduction of location information in DECT

The use of DECT telephones is not always restricted to one room or building. Because of the range of a DECT handset it may be possible for it to be used a substantial distance from its base station, or unknown to its user, it may even register with another base station. In this event, localization based on CLI would not correspond with details given by the caller. If DECT systems are to allow such roaming then handsets should automatically signal to the PSAP that they are not connected to their "home" base station and, where possible, deliver accurate location information in addition to the roamed CLI.

13.2.3 Minimum requirements for QoS for emergency communication

In order to deliver the best possible emergency service minimum requirements in regard to QoS, particularly in regard to call set-up time, should be defined. Since this is mainly addressing network issues, this is matter of TISPAN for NGN and 3GPP for UMTS.

13.2.4 Standardization on emergency communication requirements for PN

The architectures of PN are different from company to company. Guidelines for PN in regard to emergency communication and requirements that need to be fulfilled would certainly increase the probability of a working emergency communication service, especially in regard to emergency communication applications based on IP.

NOTE 1: In some countries emergency calls in the PSTN are held under the control of the PSAP even if the calling party attempts premature release of the call. Long call set-up and answer times should be avoided as this may result in the calling party hanging up and not being able to make another call attempt due to the first attempt still being held by the PSAP (which could still eventually answer it).

NOTE 2: VoIP calls cannot usually be held after the first party hangs up. This makes the calls less easy to trace and therefore could lead to more malicious calls, which may have regulatory implications in some countries.

13.3 Future Outlook

Up to now the majority of emergency communications have been PSTN voice calls. With the increasing availability of IP connectivity and the increasing diversity of communications systems means that many additional applications and services will need to be considered. Besides the conventional voice call, a variety of other means of communication may be used. Examples of the types of communications from the citizen to the authority include:

- E-mail.
- Instant Messaging.
- Short Message Service (including variants).
- Multimedia Messages.

Public broadcast services can also provide emergency communication from the authority to the citizen. These should play a considerable role in warning and informing citizens in case of disaster, by means that may include:

- Short Message Service.
- Instant Messaging.
- E-mail.
- Teletext messages on television sets.
- Multimedia Messages.

There is continuing evolution of all kinds of telecommunication services, including the convergence of formerly separated networks, strict differentiation between network, access and TE is no longer possible. For example, a service combining the function of the PLMN with access (xDSL) and ad-hoc networking technologies is being developed. Before the introduction of any new service, the issue of emergency communication needs to be raised and carefully considered.

Annex A:
Further information

The following websites contain further information, mostly of a general nature, relating to the subject of the present document. No responsibility can be accepted for the content of these sites, their accuracy or continued maintenance. Some of the information is not relevant to systems or procedures applying in all countries.

www.nena.org	The National Emergency Number Association (USA), set up to promote standards for "911" operation, especially prioritization of emergency traffic and call handling at PSAPs. Of particular interest is http://www.nena.org/VoIP_IP/index.htm
www.sos112.info	This Swedish sponsored site is focussed on the introduction of the "112" emergency number (per Directive 98/10/EC [60]) in Europe and promoting its wider use. This site has many useful links to other organizations having interests in the use and provisioning of emergency telecoms services and includes information on emergency numbers used in nearly 50 countries.
www.112.be www.eena.org	The European Emergency Number Association (EENA) is a not-for-profit organization established in Belgium. Its main objective is to promote the knowledge and efficient use of the 112, the single European bringing together the organizations (emergency services, enterprises and individuals) involved with the development and implementation of the 112 service.
www.reliefweb.int/telecoms/	United Nations OHCA sponsored site which contains a number of links containing useful information on emergency telecoms whilst its home page links with various other humanitarian aid sites.
http://www.europa.eu.int	European Union main website, see page http://www.europa.eu.int/comm/environment/civil/prote/112/112_en.htm for the latest updates on the 112 European Emergency Number implementation.
www.enisa.eu.int	European Network and Information Security Agency (Enisa) This is an agency of the EU and has been created to ensure a high and effective level of network and information security within the Community and will contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations thus contributing to the smooth functioning
http://www.gstforum.org	Global System for Telematics is an EU-funded Integrated Project that is creating an open and standardized end-to-end architecture for automotive telematics services. Their work includes an interesting project on automatic locations of vehicle emergencies; more details at http://www.gstforum.org/en/subprojects/rescue/about_gst_rescue/introduction/e-merge.htm/en/project_description
http://www.ietf.org	The Internet Engineering Technical Forum undertakes a variety of work of interest in the context of this report. In particular, the reader is referred to http://www.ietf.org/html.charters/ieprep-charter.htm for more details. The work of their WG ECRIT (http://www.ietf.org/html.charters/ecrit-charter.htm) and GEOPRIVE (http://www.ietf.org/html.charters/geopriv-charter.html) are of specific interest, covering Emergency Context Resolution with Internet Technologies and Geographic Location and Privacy matters, respectively.

Annex B:
SMS and CBS concepts in mobile networks

Originally, SMS was defined as 2 services:

- SMS - Point to Point, now referred to as SMS.
- SMS - Cell Broadcast, now referred to as CBS (Cell Broadcast Service).

SMS has been deployed on virtually every GSM network whereas CBS has been deployed on very few GSM networks. The reason for CBS not being deployed is largely due to the difficulty in business case justification (revenue), MMI difficulties and high battery drain in the receiving mobile phone.

3GPP TSG-T feels that it is important to distinguish between two fundamental usages cases for emergency text messages.

Case 1: Mobile originated Emergency text messages to 112 and other national emergency service numbers (e.g. Police, Fire , Ambulance services).

Case 2: Network originated broadcast text messages (in the case of national or local area emergencies).

The further analysis below is presented as a set of first thoughts on this matter from TSG-T and was not fully researched all the detailed issues involved in these two cases. Further work would be needed to establish a comprehensive list of issues.

B.1 Case 1 - Mobile originated text messages

For case 1 it is possible that SMS could satisfy this requirement provided that the receiving entity was within the fixed network and not another mobile phone. The reason for this is that the majority of users perception of SMS poor performance is based on 2 way text messaging mobile to mobile where the main reason for non delivery on the first attempt from the SMS-SC is the non availability of the receiving mobile (i.e. poor radio coverage or turned off). Typically, 38 % of messages are NOT delivered to a destination that is a mobile phone on the first delivery attempt primarily for that reason.

However, once a message has been received by the SMS-SC then there is a very high probability that the message will be delivered within typically a few seconds to a fixed network destination which does not suffer from the same problems as a mobile phone. In fact some network operators have given figures of about 98 % delivery success within 5 seconds of all messages on the first delivery attempt sent to a fixed network.

The sender of a mobile originated SMS message can request delivery confirmation at the time of sending. That delivery confirmation confirms the delivery of the SMS message to its destination. Some mobile networks do not support this feature and unfortunately many user mistake the indication "Message Sent" on many mobile phones as meaning delivery confirmation whereas it only means that the message has reached the SMS-SC.

Despite all this, the capabilities of SMS need more analysis against a clear set of requirements to determine whether SMS is appropriate as an emergency mechanism.

SMS in itself provides no location information. Such information would have to be obtained by secondary means such as agreement with the network operator for cell location.

There is no capability for SMS to be sent without both a smart card and a valid subscription.

In order for case 1 to be considered for emergency messages then 3GPP TSG-T makes the following recommendations:

- It should be possible for the mobile user to set the SMS message Destination Address to 112 or any other national emergency number and for the network operators SMS-SCs to route the message to the 112 emergency service.
- It should be possible for the MMI on mobile phones to have an easy menu selection for sending emergency SMS messages. This could include a predefined text string and automated delivery confirmation request.

- The use of a reply SMS message needs to be treated with caution because of the risk of message delay or even non-receipt due to the recipient mobile being in poor coverage.
- National legislation may be necessary to ensure that network operators receive appropriate funding to provide support for SMS emergency messages.
- Pre-pay phones must be capable of sending an emergency message irrespective of their credit availability.
- Provision should be made for mobile networks to trace malicious emergency SMS calls and forward relevant information to the relevant emergency authority or PSAP.

There is currently no standardized mechanism for defining a priority mobile originated Short Message. Were such a mechanism to be defined then special provision in network elements such as the BSC, VLR, HLR and SC would be required to handle priority Short Messages. Also, provision would need to be made to ensure the facility was not abused for non-emergency short messages. The SMS-SC could analyse the emergency short code destination address (e.g. 112) and treat the message as priority for onward delivery but that does not resolve any requirement for treating an Emergency Short Message as high priority in the radio network..

The use of mobile originated Short Messages for emergencies when roaming could give rise to problems in obtaining local assistance because mobile originated Short Messages are sent to the subscribers home network SMS-SC which may be in a different country. Routing that Emergency SMS content to assistance in another country requires functionality and connectivity that would require special development.

B.2 Case 2 - Network originated broadcast text messages

For case 2, it would seem that CBS is a possible candidate for reaching as many mobiles as possible.

The problem with using SMS in such a scenario is that it can only target specific mobile phones which may or may not be in good radio coverage or switched off and so the message my not reach critical recipients for further dissemination.

By using CBS all mobile phones in a particular area can be targeted and even though some of them may be in poor radio coverage, the probability of reaching many recipients is high and the message could be easily disseminated.

There are drawbacks to the use of CBS for emergency matters - the primary concern is related to battery life. If the Cell Broadcast channel is continuously monitored then there will be a considerable battery drain approximately halving the battery life. For this reason, mobile phones are normally shipped with the Cell Broadcast feature switched off. The feasibility of using Cell Broadcast is therefore questioned.

3GPP has the expertise to devise additional 3GPP features which would enable the support of a low battery drain emergency broadcast message, however we would need to discuss the requirements more closely with the organizations envisioning mass market emergency broadcast capabilities.

Whatever the eventual mechanism used for broadcast, TSG-T makes the following recommendations:

- The MMI on mobile phones needs to be considerably improved so that there is immediate recognition and display of such broadcast emergency messages.
- National legislation may be necessary to ensure that network operators receive appropriate funding to provide support for such a service.
- It will be necessary to prevent malicious emergency messages being broadcast or to authenticate their source.

History

Document history		
V1.2.1	November 2005	Publication