ETSI/AT(04)10_026

European Telecommunications Standards Institute
AT#10 Plenary Meeting
15-19 November 2004, Sophia-Antipolis

LIAISON STATEMENT

Title:	**AT Activity on emergency communications aspects on access and terminals**
From:	
Organisation:	**AT-NGN@Home**
Approval Date:	2005/01/19
Technical Contact:	Ted Laverack
Reply to:	atsupport@etsi.org, ted.laverack@etsi.org
Reply by (if required):	2005/02/18
To:	
Organisation:	**3GPP terminals, DECT, HF, UG, ECMA TC32, EMTEL**
Contact Person:	
e-mail:	

For:

Action:	X
Information:	
Attachment	X

Action/Decision Requested: 2005/02/18

Note: The present suggestion was initiated during a recent STF 274-Steering Group meeting

From the collaboration AT with EMTEL, AT NGN @ Home initiated the Work Item

- DTR/AT-040006, Study of Emergency Telecommunications aspects related to access to non-mobile networks

The work progress was initially slow and the scope wide. STF 274 introduced recently significant progress and at present AT plans to finish the work by middle of 2005.

One of the conclusions of recent discussions was that even if mobile access and terminals are out of the scope of the present AT document, the facilities seen from the user should be similar, particularly those needed in case of emergency. Also, in the case of end-to-end protocols suggested to complement and confirm information available to the Emergency call centre, there should be some (at least) comparable functions to the centre, so that he decides the most appropriate measures to be taken within the shortest time.

We therefore wish to inform you about the latest version available in the folder:

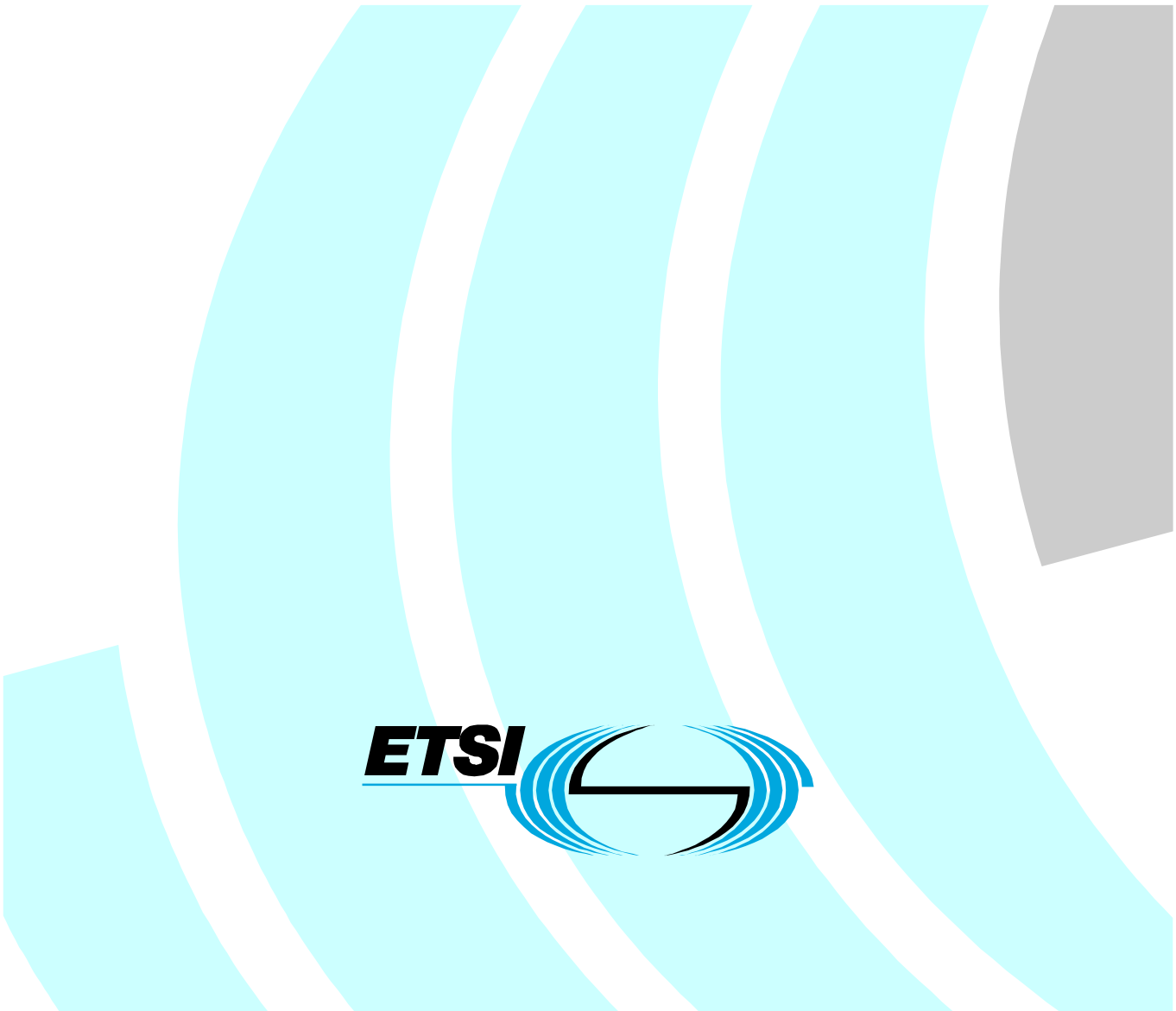
http://portal.etsi.org/docbox/at/ATNGNathome/07-drafts/NGN@Home006/
(Version 1.3.5 is also attached to this LS)

and invite you to comment on it and provide STF 274 and AT in general with relevant information to progress our task.

Draft ETSI TR EmFxAT V1.3.5

Technical Report

Access and Terminals;
Study on Emergency Telecommunications;
Aspects related to fixed line terminals



Reference
DTR/AT-040006

Keywords
access, terminals, 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, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Tasks assignment:

me Milan Erbes ef Edward Fitzgerald td Ted Laverack sc Scott Cadzow rf Ray Forbes

wm Wally Mellors jt Johann Thalhammer ie Ingmar Egger jcp Jean-Charles Point dr Dominique Roche

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, SR 002 181, SR 002 182, SR 002 410, SR 002 299) 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 like installations, terminals, home networks and the related access aspects. Aspects like 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 SR 002 181: "Requirements for communication between authorities/organizations during emergencies".

[3] ETSI SR 002 182: "Requirements for communications from authorities/organizations to the citizens during emergencies".

[4] ETSI SR 002 410: "Requirements for communications between affected citizens during emergencies".

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

[6] ETSI TBR 021 (1998): "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 38 "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 3: "Integrated Services Digital Network (ISDN); Attachment requirements for terminal equipment to connect to an ISDN using ISDN basic access".

[11] ETSI TBR 4: "Integrated Services Digital Network (ISDN);Attachment requirements for terminal equipment to connect to an ISDN using ISDN primary rate access".

[12] ETSI TBR 8: "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 EN300 401: "Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers".

[19] ETSI TR 101 806: "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: “Access to ICT by young people: issues and guidelines”

[25] IEEE 802.3af: “Power over Ethernet”

[26] ETSI I-ETS 300 634 “Title: Transmission and Multiplexing (TM);Single-mode optical fibre cables to be used as underwater cables for lakes and river crossings etc.”

[27] ETSI TR 056: “Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) System Description Document”

[28] ETSI EN 300 175-x: „Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI);“ series

[29] ETSI EN 300 176-1: “Digital Enhanced Cordless Telecommunications (DECT); Test Specification; Part 1: Radio”

[30] ETSI EN 300 001: „Attachment to Public Switch Telephone Network (PSTN); General technical requirements for equipment connected to an analogue subscriber interface in the PSTN”

[31] ECMA 263: „Private Integrated Services Network (PISN) – Specification, Functional Model and Information Flows – Call Priority Interruption and Call Priority Interruption Protection Supplementary Services”

[32] ECMA 264: „Private Integrated Services Network (PISN) – Inter-Exchange Signalling Protocol - Call Priority Interruption and Call Priority Interruption Protection Supplementary Services”

[33] 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”

[34] ETSI TS 101 909 10: „Access and Terminals; 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”

[35] 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”

[36] 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)”

[37] 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”

[38] ETSI TS 23.003: “3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification”

[39] ETSI TS 22.016 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; International Mobile station Equipment Identity (IMEI)”[40] ETSI EG 202 067 “Universal Communication Identifier; System Framwork”

[41] ETSI EN 300 468: „Digital Video Broadcasting (DVB); Specification of Service Information (SI) in DVB systems”

text field!!! To Delete[42] ETSI EN 300 401: „Radio Broadcasting Systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers”

3 Definitions and abbreviations

3.1 Definitions

See: http://webapp.etsi.org/Teddi/

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

Emergency Call Post 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 (see Commission Recommendation C(2003)2657))

3.2 Abbreviations

See: http://webapp.etsi.org/Teddi/

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

ADSL	Asymmetrical DSL
DSL	Digital Subscriber Line
ECC	Emergency Control Centre
ESD	Electro Static Discharge
EMC	Electro Magnetic Compatibility
IMEI	International Mobile station Equipment Identity (check)
IMS	Internet protocol based Multimedia core network Subsystem
IMSI	International Mobile Station Identity
ISIM	IMS SIM
IVR	Interactive Voice Response
PLMN	Public Land Mobile Network
POTS	Plain Old Telephone Service
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
SIM	Service Identity Module
SIP	Session Initiation Protocol
SP	Service Provider
TE	Terminal Equipment
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/ocgemtel/status.asp

SR 002 180 [1] (communication from the user to the authorities) gives substantial guidance on the present chapter. When completed SR 002 182 [3] (communication from authorities to the user) and SR 002 410 [4] (communication among the users) will also provide important information impacting the scope of the present document. SR 002 181 [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 call addressed to 112 or other emergency call number intended to bring the ECC and the person suffering from emergency situation or his representative in bi-directional and direct contact;
- The alarming and other communications used to supply complementary or supplementary data in order to trust or enhance the description of the emergency situation.

Note: The second type includes communications to a number of surveillance systems that might be connected to specialized organizations in charge of producing the first type of calls to ECCs. It also may include additional information directly associated with type one (e.g. 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 moment, free of charge, using any of the most popular Telecommunications telephony terminals when it is 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 also when:

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

Note: For mobile devices the principles are similar, i.e. access networks, except in well-justified cases, are expected to be operational for emergency calls 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: These features are not equally required in all countries.

Most popular technologies are PSTN analogue and digital connected terminals and PLMN terminals. Voice services related to emergency numbers, e.g. 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 in the European regulation (SR 002 299)

Directive 2002/22/EC requires that in addition to any other national emergency call number specified by the national authorities all end users of publicly available telephone services have the possibility 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 means not necessarily directly related to the “112” voice emergency call (normally not in the regulatory domain) are 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 communication user - authority, according European regulation and SR 002 180 [1], is nevertheless the voice services addressed to 112 and to the nationally identified other emergency numbers, associated with the caller location information.

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

Data or video transmission systems may be extremely useful and facilitate a remote control on the environment where humans may no longer be able to appropriately behaviour.

Presentation methods on the terminal available to the operator in PSAP should make available the maximum possible set of trusted information in appropriate manner.

Information provided to the ECC 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 rules and may correspond to lower levels of trust. Nevertheless this second type of information is expected to be of very high importance as a complement. It may filter different types of emergency, detect false alarms and detail available data e.g. localisation or medical data.

Note: ITU-T recommendation E.106, 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 an indirect impact (if any) in the present document

4.4 Features and functions in Terminal Equipment

4.4.1 General aspects

Voice communication terminal equipment should be designed in such a way that emergency calls are always possible even if the terminal is PIN-coded or power supply (mains or other) dependent. 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 call to be well succeeded. This could be made e.g. by reducing the set of features of the terminals, Home systems and private networks to the minimum necessary to always allow a voice call to the emergency numbers. No terminal equipment feature should prevent an emergency call from being made.

Some public terminals are under special risks, e.g. automatic bank machines. The keys (help and/ or survey and/or others) suggested in this clause could easily, where apropriate in future developments, be integrated in many of them and be e.g. 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. Users would hardly understand significantly different implementations. Where standards are not available, they should be produced prior to a large scale deployment.

4.4.1.1 Emergency call terminals and specific posts

A special feature is suggested in SR 002 180 [1] where:

Emergency call facilities with voice application when connected directly to a public network or to a PSAP are expected to make emergency calls free of charge and without the need for the user to know the emergency call numbers. Emergency call facilities are expected to be easy to use and not require specific language knowledge.

The connection to the PSAP/specialized emergency center may be initiated e.g. by lifting the receiver or opening a cover. In addition, the same functionality (direct connection to the PSAP) may also be provided by a certain key as described in the following sub clause.

Terminals dedicated to specific emergency services, particularly those addressing highly centralized services, e.g. E.112, and not used for other purposes may also be recommended in some circumstances. Ways of testing their functionalities regularly without producing false alarms should be foreseen (this requirement is listed in clause 0).

It is easy to imagine a wider coverage and general support of emergency communications to the citizens if e.g. the HELP and other SURVEY keys become popular by some manufacturers or distribution channels.

4.4.1.2 “HELP” key for 112 service on terminals with voice application

This could be implemented if e.g. telephone sets or other terminals would introduce a “Help” key, which, when activated would initiate an automatic call for 112, sending the geographical localisation 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 ETSI HF EG 202 132 [13].

It is recommended that emergency call terminals can be used to the common service, so that in case of failure it will very unlikely be detected during an emergency situation. The terminal can therefore be tested in its basic functions every time it will be used.

The “red HELP” key is suggested to be red and should be put in a “easy to reach”, evident place and have a size superior when compared with other keys. The size, the marking and the overall specification should facilitate the clear identification of the key for all kind of users, including children, elderly people or users with any kind of impairment.

To prevent false alarm situations, it is suggested in particular for 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.

Above and other performances and behaviour(s) associated to 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 to programmable memories with numbers related to other specific emergency services. Different type of text, data or voice messages to be sent in case of emergence might also be kept in memory.

These other keys should easily be understood by the user 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 to.

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 closed to the emergency local, seized by special skilled personal and not necessarily to 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 user wishes to communicate with the ECC via voice. In cases were a user may wish to alert some organization of an emergency without generating noticeable signals on 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 delivering monitored data and the number to the appropriate surveillance centre.

On occurrence, such a "silent alert" may be connected directly to an ECC or be routed to an emergency response organization different from the ECC that verifies the urgency and accuracy of the alert including associated data (e.g. localization information) and contacts if applicable an ECC.

Note: This key, depending on the parameters to be observed and the functionality requested, may be related with the use of microphones (more commonly), video cameras (frequently) or other transducers (fire, chemical, others).

4.4.2 Categories of telephones and other terminals

Telephones may be classified in different ways:

- Accessibility
  - Public
  - Private (with restricted access e.g. family members)
- Charge
  - Pay
  - Free of Charge
- Connectivity
  - Directly connected to a public network
  - In a private network (e.g. PBX)
- Other restrictions (Telephones restricted e.g. by passwords or PIN-codes)

No matter what type of phone, 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 **Error! Reference source not found.**.

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

4.4.2.1 Public pay telephones

Directive 2002/22/EC requires that it be possible to make emergency calls from public pay telephones using the single European emergency call number '112' and other national emergency numbers, all free of charge and without having to use any means of payment. The user 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 without the assistance of an operator to be made free of charge and without having to use any means of payment.

Note: Most private phones are not pay phones (e.g. in homes) still e112 call should be possible.

4.4.2.3 Telephones in private networks

If access to the Public Emergency Services is allowed or nationally required from Telephones with a Private or residential network, then the CLI presented to the PSAP/ECC is normally the CLI of the Attendant of the Private network. Provision of the Two Number CLI service at the Primary rate access to the Public Network allows the Provision of a User Provided CLI that may be useful or required by the Emergency Services.

In Such cases the Private Network Owner is responsible for any Fraud or misuse when calls are placed to the Emergency Services. For this reason Emergency Calls placed via Private network Access are often via an attendant or are monitored by the Private network.

Life Line services such as lift alarm systems are considered part of the Private network and are monitored, managed and maintained locally and are not part of the Emergency Services but may result in requests for assistance from the Emergency services.

Private Networks should also be able of correctly support emergency calls at an acceptable quality level even in the case of power failure, high traffic or intensive use of the system. This could be made e.g. by reducing the set of features of the system to the minimum necessary to always allow a voice call to the emergency numbers. No 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 any other kind of special identity recognition. In all the cases, privately or publicly available, they should be able to allow emergency calls to be made free of charge and without having to use any means of payment.

Note 1: Caller Identity is a mandatory requirement in many countries. Therefore, anonymous e112 may not be allowed. That is why SIM-less emergency calls are outlawed in some countries. This is a result of trying to stop hoax e112 calls and prosecute hoaxers.

4.4.3 SMS in Emergency situations

Generally, SMS may be applied for two different types of communication scenarios:

- Communication from authorities to users;
- Communication from users to authorities.

The first type of communications would typically be a SMS broadcast to a certain area to warn or inform citizens about an incident. The second type may be useful when no emergency call is possible.

Some difficulties related to SMS are:

- store-and forward mechanism; therefore no real-time and bi-directional connection
- no guaranteed delivery;
- the location information is not always trusted.

Nevertheless:

- SMS may be used when calls are not possible
- SMS can be used in both ways
- SMS can be in point-to-point or broadcast modi
- SMS can be used base support to transmit additional information.
- A Short Message (SM) is shorter to transmit and requires smaller bandwidth than an equivalent vocal call. This makes SM suitable to reach a wider number of subscribers to be contacted.

Note: To facilitate the writing of SMSs and for a more efficient handling in ECCs, standard texts may be defined. In this regard similar solutions should be standardized for fixed and mobile networks.

Special routing profiles might be required for emergency SMSs. The contribution of SMS to E112 services may be possible but needs much further studies.

In some mobile systems this facility is used to alert subscribers within the coverage of a certain geographical area (a pre-selected number of base stations can be activated to “broadcast an emergency message”). A similar situation can now be foreseen with the extension of the SMS services to the fixed network (ES 201 912).

In the case the called subscriber would ignore for some reason the urgent aspect of this SM for a while, it would be interesting to be able to trigger in the terminal a special behaviour, e.g. special ringing or other to stimulate the user to understand the emergency situation and follow the guidance in the message.

Also for customers not having a SMS enabled terminal or not registered as SMS users or for SMS enabled terminals not supporting emergency indication, it could alternatively be foreseen an alarm message by means of a text to speech service provided by the Short Message Service Centre (SMSC).

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

It is to note that the advantage of Telecommunications voice terminals in relation to Broadcasting receivers is that they can be alerted (ringing function) at any moment in the idle status. For complex messages, a co-ordinated information system could well make use of the Telecommunications SMS service and invite the user for further information in a certain identified broadcasting channel (TV, radio, or web page).

SMS Emergency Texting; is not considered a priority service by 3GPP and most PLMNs. No country mandates a requirement for its use or behaviour. The Time to deliver latency of text messages is unreliable and not guaranteed. Users use such a feature at their own risk.

4.4.4 Text telephones and fax devices (*contact STF264-/HF-Scott Cadzow*)

Guidance on text telephones can be found in ETSI TR 101 806, Guidelines for Telecommunication Relay Services for Text Telephones [19] including some concerns regarding emergency services.

Fax services associated to emergency and alarm centres need normally a number different from the vocal service. Nevertheless it would be recommendable for voice call assigned incoming lines to detect fax communication and re-route them for 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 initiated devices used in emergency calls should comply with ES 202 076, Human Factors (HF); User Interfaces; Generic spoken command vocabulary for ICT devices and services [16].

Speech recognition standards have been produced by ETSI (STQ) and their use is recommended.

4.4.6 Special terminals

Special terminals for elderly and people with special needs in general, e.g. radio devices are connected to specialised centres in charge of the surveillance and eventually of starting an emergency call. In this context see clause 4.5.

4.4.7 Multipurpose facilities

For multipurpose call facilities (e.g. customer assistance for vehicles and accidents) functionality should, as far as possible, separate the operation modes in order to avoid unjustified calls to public emergency services.

Editors Note: this needs checking and expanding with the eCall documents (EU – eCall project).

4.4.8 Services that could be deployed by emergency authorities

Some applications may foresee the programming of a fix telephone number (ITU-T recommendation E.164) or a fix internet address to special centres in charge of some type of services which could be used in case of emergency, e.g. some special medical services or police services allowing a remote surveillance of the local. These are not considered as first priority services in the context of the present document, but devices supporting such services should beneficiate at least from some parts of this document.

4.5 Usage by disabled, elderly and young users

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

ETSI HF Guide EG 202 116 (“Design for All”) [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.

STF 266 is contributing to DEG/HF-00058, “Guidelines for the design and use of ICT by children”. The work is based on ETSI TR 102 133, “Access to ICT by young people: issues and guidelines” [24]. It will take an approach similar to CEN/CENELEC Guide 6, “Guidelines for standards developers to address the needs of older persons and persons with disabilities” but applied to children.

ETSI HF TR 103 073, “Universal Communications Identifier (UCI); Improving communications for disabled, young and elderly people” [23] gives some information for young people contacting emergency services. It points out some issues that arise when the person calling may be in a state of distress or shock and be incoherent.

4.6 Types of identification in communications systems

4.6.1 General

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

The public communications systems use a number of identification parameters. They facilitate the accomplishment of some legitimate requirements from their users. Emergency communications call centres require in this context three types of identifications:

- The user line (mobile or fixed) identification to allow to call back the user in danger from call centre
- The user identification (discussed in chapter 6.3.5 of the present document) to allow
    - the person doing the call to be responsible for the call and track hoaxers or other inappropriate use
    - an alternative calling method to the user
- The identification of the exact geographical position of the user (discussed in chapter 6.3.6 of the present document) to allow
    - the call routing to the appropriate (normally the closest) call centre
    - to facilitate the most correct ECC decision.

In the future, if proposals like 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 to this key some form of identification in order to identify the user and his localisation. Technologies to enhance the identification functionality may be implemented for example via an end-to-end protocol. Technologies to obtain localisation information may include GPS/Galileo or RFID. It may also be possible that further enhanced functions establishe a data channel within the voice communication connection and transmits several of the parameters described below and eventually more useful data.

In all the cases, the identification of the calling line is important and the designers of new features, devices or home systems are encouraged to create easy means for the ECC to trace the caller in emergency situation.

4.6.2 Identification in the PSTN - CLI

In fixed networks the CLI became a parameter to the caller from the calling line and therefore, in normal cases, with some precision the localisation of the caller and the identification of the used line. With an increasing number of features and technology developments the CLI meaning became less clear.

In most ADSL Technologies the CLI is that of the ADSL termination (DSL or associated PSTN E.164). So it is the line the user is using.

The IP address may indicate the Service provider that they subscribe to. According to TS 101 909-23, Inter-working between the IP cable domain and the ISDN, the CLI is that of the port or Pseudo port added by the ISDN. If the MTA is moved within the IP cable CSTA domain this will still represent the same CLI of the initial Subscriber. This may have legal implications for Emergency Localisation and for tracing malicious calls.

In the case of broadband access, the CLI can be the one associated to the conventional PSTN line, but it should be noted that business and private networks in general might have different real locations (the user may be abroad and use VoIP or even more general Voice over Internet to 'call from home'). In this case it is very convenient to associate the CLI with the user identification and other addresses and information allowing a more appropriate identification of all necessary parameters.

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.

Conclusion:

- CLI identifies the Calling Line.
- CLI can be a 1st tentative identification of the Caller localisation.
- CLI can be a 1st tentative identification of the Caller himself by identifying the subscriber.

4.6.3 Identifiers in the PLMN

With the appearing of Public Land Mobile Network (PLMN) new identifiers have been introduced. As described in [38] they are:

- Mobile Subscriber ISDN Subscriber Number (MSISDN),
- International Mobile Station Identity (IMSI),
- International Mobile Station Equipment Identifier (IMEI);

Regarding the identifiers the following applies:

- The MSISDN identifies the E.164 number that is associated to a certain 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 does only identify the equipment, the mobile phone itself independent of the (U)SIM;

Since the user of the telephony service must 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 may be used to retrieve the identity of a service user. Exceptions include a mobile phone lent to another person or a switched-on and stolen mobile device.

It can be concluded that the MSISDN or CLI now as before indicates the subscriber to the number and SIM card services. However, this is no physical calling line as in the fixed network and no final conclusions about the localization may be drawn.

Note: Some SP enter dummy CLI of base station (BS) to calls in order to support rough localisation 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 identification information about the subscriber or user may be obtained. Since the device is mobile also no localization information may be obtained. It is mainly used in order to detect stolen mobile phones. Therefore it is of limited use for emergency telephony. In case of SIM-less emergency calls it would be the only identifier available, as stated in [3]. It also specifies that emergency services shall also be available for mobile phones listed on the so-called “black-lists”.

4.6.4 IP address identification

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

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

- Network Address Translation (NAT)
- Mobile IP
- VPNs

Reasons to introduce these technologies have been the relatively small IP address space, security reasons or mobility. The problem with the IP address space does only concern IPv4. IPv6 has got considerably larger address space that theoretically would diminish the IP address space problem.

In regard to identification, it can be said, that the use of IP addresses alone is of reduced value. However, the combination of the triple IP address, MAC address and time of allocation identifies a specific terminal at a certain time.

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

SPs have the possibility to record, for a certain time interval, the assignment of IP addresses to the registering equipment and may be able to reveal this information.

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 to a bigger amount of people; except of applications with some kind of authentication mechanism. Mobile terminals are rather used by a smaller group of people. Here also, mobile equipment with integrated authentication modules let conclude the identity of the user. However, such a type of authentication is made independent of any IP address knowledge, although, it may be associated with it, e.g. by the SP.

Location information for fixed line terminals may be known, e.g. in a household. In companies it may not be as easy to derive. The location of mobile equipment can be traced up-to the region that a kind of access node is able to cover with its signal, which may be quite a large area.

Editors Note: The following references may be included: RFC 1631 – NAT, RFC 1918 – Address Allocation, RFC 1166 – Addressing Format, RFC 2132 – DHCP, RFC 1884 – IPv6 Addressing Architecture

4.6.5 MAC (Media Access Control) identifications

The MAC address identifies a network adapter, this is to say, a hardware device on a network. It is unique. Furthermore, the MAC address on its own does neither identify a certain person, nor a certain location. It may identify a person in a scenario as mentioned in the paragraph before where a device is associated with a person (e.g. through the means of authentication and access control, where only a certain person is allowed to use a device) and the IP is associated with the MAC address of the device. The same is valid for the location information. Only if a device is bound to a location the information the MAC address may be used as location information.

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 [38],
- H.323 addresses,
- Telephone number, in systems using NCS or MGCP like 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 user can be known to the communications system if the user is required to authenticate to the application. Otherwise, the application identifier needs to be configured in the application. This corresponds to identity of the calling line in the PSTN. If access is limited to the device to the user identification is also possible.

4.6.7 Universal Communication Identifier (UCI)

According to EG 202 067 [40], UCI is the concept of a single, unique identifier for a user. All communication should be controlled by a single personal user agent (PUA). Since the users must register at their PUAs in order to get access to the service their identity is, if delivered to the second party, granted in each individual communication session. Compared 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, other mechanisms must be used.

4.6.8 Biotechnologies to identify users

One possibility to authenticate towards an application is a kind of code, e.g. a PIN code. Another solution is the use of biometrics, the identification of an individual according to his physiological or behavioural characteristics. ETSI guide EG 202 116 [22] lists the following biometric technologies:

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

Devices 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 only implemented in highly security sensitive areas. Their use for the identification of emergency communications service users is therefore not likely. Concerns and arguments against the implementation of biometrics reach from cost effectiveness to privacy concerns of the users. In regard to localisation it must be said that biometrics do not provide any information.

4.6.9 End-to-end protocols for user identification and localisation

End-to-end protocols can be used for user identification and localisation but corresponding information should be carried under standardized forms to be effective and facilitate the ECC action.

Editors Note: e.g. RFC SIP P-Access-Network-info header is not validated information in 3GPP IMS Terminals this header may be partially trusted due to the terminal radio type approval. [TS 124 229]

4.7 Unclear situations and contradictions

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

The emergency situations can easily beneficiate from standardised solutions in particular to clarify the items listed in this clause:

- Assigning clear priority to emergency calls and reduce all impairments and costs to the user in the emergency situation (see §4.1)
- Identification of the user, his localization and his calling line (see § 4.6)

In case of special emergency keys or features, their clear identification and specification of their functionality (see §4.4)

5 General market aspects sc/ef review

5.1 Multiplicity of solutions on the market

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

For the widest coverage of the population is nevertheless recommended to implement standardised solutions, and in the case of basic services, e.g. E112 voice service it is strongly recommended.

5.2 Population needs coverage by existing solutions

As the first priority is to ensure the wider population 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 beneficiate of the recommendations in the present document.

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

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

5.3 Relationship between mobile and fix equipment

A customer of a communication service expects the same behaviour of a service no matter which type of network or technology he uses. Therefore, it is of very high importance that mobile and fixed network offer the same type of basic services with similar, well accepted, user interfaces. For emergency services, this is particularly important for the user facing an emergency situation to be able to act quickly and correctly.

Editors Note: Input from HF, cooperation with 3GPP in regard to terminals is necessary

For civil alerts and communication from to cast 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 user should be consistent in mobile and fix networks.

Standardised user profiles should be used. STF 265 is producing work in this area, especially related to the draft EG 202 325 [15].

5.4 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

Many details of access networks aspects related to emergency situations are depending from the access technologies specific characteristics and are discussed in clause 6.

Analogue or digital PSTN (POTS or ISDN) TE connected over cable, xDSL or fixed radio links technologies are increasingly being used in the access networks and in general, policy makers support such initiatives in the sense of optimising the usage of the existing wire and radio infrastructures. This means that the same technology “seen by the user” may present different performances, e.g. related with “life line” or CLI functionalities, which are of central importance in emergency situations. These aspects may be solved by National Regulatory Authorities. Nevertheless it is strongly recommended to use harmonised solutions for the interfaces and as far as reasonable ensure basic functionalities even if the power supply is interrupted for a reasonable time (the value suggested is 1hour interruption, but this needs to be studied in connection to power distribution network performance).

6.2 General aspects of terminals and home installations

This is intended to be a general overview for matter treated in detail in the clause 6 for each technology.

6.2.1 Cabling and installations aspects

xxxxx

6.2.2 Simple devices

To ensure a maximum of efficient in emergency situations it is recommended that simple devices are power supply independent.

6.2.3 Featured devices

To ensure a maximum of efficient in emergency situations it is recommended that featured devices offering support to (among other services) emergency services, in case of emergency and in the case of power failure, suspend all non-emergency related functions and ensure for the maximum possible time the operation of the emergency related features.

6.2.4 Data and video devices

The principle recommended in clause 0 is valid.

The surveillance key feature is one of the solutions recommended in clause 4.4.2. It may have application in many cases, e.g. in case of video surveillance cameras a special surveillance key may call 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 Requirements

In general, technical requirements are valid for both TE and network. In most of the cases they cannot be separated and depend on each other. This document covers only TE, home equipment and access aspects. Since there is no clear universal separation, all the technical requirements need to be looked at from the point of view of the TE. From the formal point of view, in the case of public offered interfaces, the Network Termination Point [NTP], in principle the Point where the network operator offers a connection to the consumer, connects TE to the network, i.e. is the point where the equipment is no longer TE and starts belonging to the public network. As different offers may refer to different NTP, this point may have different technical characteristics. Also the TE may incorporate (private) network equipment.

Network aspects are mainly studied in ETSI TC TISPAN (services and protocols aspects) and in TM (transmission, physical layer aspects).

For ISDN, existing standards still apply and cover reasonably emergency services aspects.

This clause highlights important technical properties of emergency services. They include the following:

- Performance
- High reliability and availability;
- Priority of 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 mentioned in ETSI SR 002 180 [1]. The following sub clauses describe them in more detail and also give corresponding references.

6.3.1 Equipment performance

Additionally to base standards, used to design the terminal that should be fulfilled as far as reasonable, close to nominal values, care should be taken with other parameters like performance, i.e. product life, failure rate and others. Also aspects related to resistibility and immunity, e.g. ESD, mechanical, thermal, EMC, etc, should carefully be considered.

Terminals intended for emergency services support, should at least as far as it concerns these emergency services, be able to operate appropriately (eventually reducing other non-emergency functions) without the need of external power supply.

6.3.2 High reliability and availability

Reliability and availability issues are very important for emergency services. Fast and immediate delivery of emergency services is only possible if "always-on" means of communication do exist. However, not all technologies and equipment do support such capabilities by default, sometimes because they have not been incorporated in the systems development from the beginning. ETSI SR 002 180 [1] also stresses the importance through stating that network terminating points (of public or private networks) should supply TE with a minimum power supply in case of local power failures. Also ETSI TS 102 302-1 [20] highlights the vital role of robustness.

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. Relieves may be:

- Battery-Reversal-Packs for terminal equipment (TE);
- Universal 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** specifies the requirements for line powering of IP Terminals connected to 802.3 interfaces.

A further issue is the reliability of the connection of TE to the communication infrastructure. This especially includes cabling and plugs. These issues are dealt with in [Reference].

6.3.4 Priority of emergency services

Besides availability and reliability the priority of emergency services as described in ETSI SR 002 180 [1] is vital. According to it all network operators should accord emergency calls priority over all other calls.

Examples for how priority may be ensured are:

- The use of separate communication infrastructure for emergency services (prioritised routing);
- An a priori reservation of channels or bandwidth;
- "On-the-fly" prioritisation.

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

6.3.5 Identity of emergency service user

The identity of the user of an emergency service is another important property of an emergency communication service. However, its determination is very difficult. “Real identification” is not very likely without biometrics and these technologies are not yet widely used at the consumer level.

The identifiers used in communications systems are discussed in clause 4.6. Generally, the identity of the caller may be used to:

- Hold the caller responsible in case of emergency communications misuse,
- Find alternative communication methods in case of emergency communications break-down;

In the case of misuse of the emergency communications service, the ECC may have on-line access to identification information. If SP’s do save call information (e.g. if there are regulatory requirements) it may also be obtained off-line. However, whether such mechanisms deliver accurate identity information depends on the technology used. For example, obtaining the identity of the user of an emergency service is not as straightforward as it seems to be. In the PSTN, the only identification mechanism is the CLI, which identifies the calling line of the service subscriber and not the emergency communications service user. Since telephones are bound to locations located in the homes of the subscriber, the identity of the caller in most of the cases the service subscriber is the service user or a family member. However, a general identification without additional methods, for example authentication codes, is not possible.

Another important requirement for emergency communication is the possibility for the ECC to initiate a communication to the emergency service user in case of communication break-down. If the initial communication media is still available the identification of the calling line is sufficient. In order to seek alternative methods the identity of the user is required. According to ETSI SR 002 180 [1] clause 4.2.1.1, it is strongly recommended that that the ECC should be able to return a call to the calling party.

For telephony emergency services, E.164 numbers are used. This number is further on delivered to the ECC. However, there are technologies that use communication identifiers different from E.164 numbers. In that case it may be required to support means for the configuration of identity information.

The Emergency Control Center (ECC) should be able identify a session initiating party. It should also be able to initiate a communication session with the user if the initial connection breaks down. Furthermore, the identification may be used to obtain location information.

IP based TE should be capable to support all communication system related functionality to support these requirements. Their specification for example for NGN is scope of TC TISPAN.

The identifiers used in communications systems are discussed in clause 4.6 where some risks of inaccurate caller identification are cited as well as some initial suggestions to overcome difficulties.

6.3.6 Location Information

Another very important item in order to direct emergency teams to the user is location information. Besides providing the ECC with important information to guide emergency relief teams as fast as possible to the place of emergency the location information may also allow the ECC to detect fraudulent calls. Geographic numbers and location 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, e.g. children and also for automatically initiated emergency communication sessions as it is the case with special emergency key functionality as described in clause **Error! Reference source not found.**.

A further property of the emergency system in connection with the location information is the routing of incoming emergency communication to the ECC located nearest to the user of the emergency service. This is a network matter and therefore falls under the responsibility of ETSI TC TISPAN project EMTEL.

The identifiers used in communications systems are discussed in clause 4.6 where some risks of insufficient accurate caller localisation are identified as well as some initial suggestions to overcome difficulties.

6.3.6.1 Caller localization issues for nomadic TE

For nomadic IP terminals the location information may not be obtainable in a straight forward way.

Possible solutions depend on a system's architecture and offered services and may even involve user interaction. Examples for solutions are:

- User informs ECC personally in case of an emergency
- TE detect dislocation
- Restricted nomadity
- GPS

It should be noted that TS 102 164 will be revised to handle Geodetic co-ordinates for Geographic position, Postal co-ordinates, IP addressing and GPS.

One possibility to overcome the lack of localisation information might be for featured terminals to detect when their connection got interrupted and therefore their localization might have changed. Here, the user may be prompted to enter changed localisation information or confirm that the position stayed the same.

Also the nomadity of a terminal may be restricted to a small and certain area. or global positioning system (GPS) data may be used to gain localisation information.

An emergency communication application requires the knowledge of the TE's feature along with the permission of the user to use and transmit the obtained information.

Editors Note: Private Networks, PBX with direct- dial-in, can send CLI, localisation info not accurate.

6.3.7 Services to protect the emergency communication

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

In order to prevent emergency communication from misuse, security services such as authenticity and integrity for communication need to be provided. This has to be done via appropriate means. For example, the PSTN is relatively secure by its nature. The access network delivers from the PSTN Port Identity a Network CLI. This may be used by the ECC for Ring-back or for tracing malicious calls. IP as transport mechanism offers a broader range 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 communication service. This should be done in a way that does not occupy any resources of the ECC 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 (e.g. Interactive Voice Response (IVR)).

After describing the individual features of emergency services the following clauses explore capabilities and restrictions of several technologies in regard to emergency services. Each clause mentions general emergency service related information, TE relevant facts, access and installation issues. They also list corresponding standards and eventually suggest improvements.

7 Network Connectivity

Editor's note: EMTEL & … to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.1 POTS, the analogue legacy interface of the PSTN me

7.1.1 General aspects

In the present clause only the analogue legacy interface of the PSTN is discussed, not the same type of interface offered over other kind of technologies ("cable", xDSL, fibre, WLL, etc). Gateways from alternative technologies offering analogue PSTN interfaces, should nevertheless, as far as reasonable fulfil the guidance and the standards applicable to this popular, widespread technology to limit the risk of incompatibilities.

The analogue legacy interface of the PSTN is one of the best fix Telecommunications terminal supports to emergency situations. It probably corresponds in Europe and world wide to the widest park of terminals.

Voice services related to 112 dialling, including CLI features, are easily supported and a wide range of data functionalities are available. The network normally offers the functionality "life line".

Featured terminals may have (or not) capabilities of receiving or starting a call in the case of power supply failure. Simple terminals normally do not need mains power supply.

Data or video transmission systems associated to this interface may be extremely useful and facilitate a remote control on the environment where humans may no longer be able to appropriately behaviour.

7.1.2 TE

TBR 21 and the full series of TS 103 021 are no longer mandatory documents under EU regulation, but they represent the large majority of POTS/ PSTN terminals in Europe and there are other countries deriving their market access conditions from these documents. Furthermore, these standards are widely recognised 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 handset the reference standard should be TBR 38, which is also not of regulatory value at present, but has a wide acceptance on the market and matches the international harmonised transmission plan specified in ES 202 020 [17].

See also the importance of the indication of the loading factor in the clause "6.1.4 installations".

7.1.3 Access

ES 201 970 [7] is recommended by CEC in the list of standards under the Framework and the Universal Service Directives. This recommendation may, according these Directives, become an obligation if CEC or the national authorities will find appropriate. Since this standard specifies a harmonised solution, is the most used standard and was designed to support not only terminals according harmonised standards (TBR 21/ TS 103 021 series and TBR 38), the

interfaces offered to terminals should follow ES 201 970. Doing so, any new facility designed for emergency telecommunications could have then a maximum of impact in a short time for a low cost.

Additionally it is recommended the interface to supply power also in the case of failure of the mains power supply.

7.1.4 Installations

TBR 21, now updated in the TS 103 021 series, created a concept of loading factor explained in EG 201 120. This concept was later applied to ES 201 970 where the operator has to indicate the loading capability of the interface offered to terminals.

Devices fulfilling TBR 21 and TS 103 021 are supposed to offer lower loading factors than 100 LU. Interfaces respecting ES 201 970, offer capabilities for more than 100 LU.

The installation should normally not have a relevant impact in the effectiveness of an possible emergency call but, with the increasing number of Telecommunications applications on the terminals and the decreasing level of prices, the user 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.

Also an inappropriate installation at “do-it-yourself” level, may introduce additional risks in the level of quality and availability of the Telecommunications service.

CENELEC xxx, clause xxx, standardises cabling and installation aspects. TR xxxx discusses different aspects of Telecommunications installations.

7.2 ISDN, the digital interface of the PSTN me/tl

Editor’s note: EMTEL & AT-D… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

Editors Note: Prioritization of Emergency Communication: E.106 International Emergency Telephony preference service
EN 300 356-22 ISDN SS7 ISUPv4 IEPS service (Q.761-764) This allows Priority to be given to any e112 call across the Access network and alleviation from call gapping on route to the PSAP/ECC.

7.2.1 General aspects

7.2.2 TE

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

For ISDN voice terminals with handset the reference standard should be TBR 008 which is also not of regulatory value at present but has a wide acceptance on the market and matches the international harmonised transmission plan specified in ES 202 020 [17].

7.2.3 Access

7.2.4 Installations

7.3 Ethernet

7.3.1 General aspects

7.3.2 TE

7.3.3 Access

7.3.4 Installation

7.4 xDSL technologies ef/ne revisit

7.4.1 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. In all these cases it is normally not foreseen the function “life line” unless special uninterrupted power supply [UPS] feature is foreseen by the xDSL modem installed at the user facilities.

Data or video transmission systems may be extremely useful and facilitate a remote control on the environment where humans may no longer be able to appropriately behaviour.

In the context of the present report, to simplify the discussion of the subject and independent of the regulatory definition of the NTP, the xDSL technologies are seen as access network technologies and the terminal is the voice band PSTN (analogue or digital) voice terminal.

7.4.2 xDSL technologies associated with splitters

xDSL technologies associated with splitters share the physical infrastructure and therefore the power feeding circuits of other technologies like PSTN analogue or digital access. XDSL splitters should not significantly disturb the power feeding of analogue and digital access to PSTN. The series “TS 101 952-x specify the relevant technical requirements for splitters and DSL filters.

There is some interest on the market to develop users’ xDSL splitters fed by the Telecommunications 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.

Editor’s note: EMTEL & AT-A, TM6… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.4.3 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 as far as the cable used between central exchange and users’ facilities allows.

Editor’s note: EMTEL & AT-A, TM6… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.4.4 TE

7.4.5 Access

7.4.6 Installations

7.5 Telecommunications over “cable”, CATV infrastructures JCP

Editor’s note: EMTEL & AT-D, JTC Broadcast… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.5.1 General aspects

Voice over “cable” technologies systems often use VoIP techniques. In this case the telephone interface usually is analogue (POTS), legacy digital (ISDN) or IP based. In all these cases it is normally not foreseen the function “life line” unless special uninterrupted power supply [UPS] feature is foreseen by the MTA installed at the user facilities.

Data or video transmission systems may be extremely useful and facilitate a remote control on the environment where humans may no longer be able to appropriately behaviour. 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.

7.5.2 TE

CATV systems are based on a cable modem located at the customer premises. The customer premises equipment (CPE) is connected to the cable modem. Therefore the localisation of the caller 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.

Since the cable modem offers IP connectivity it is necessary to use an additional adapter (MTA) to connect analogue (POTS) or legacy digital (ISDN) phones to the cable network. Otherwise it is possible to use an IP phone that is connected directly to the cable modem using the IP interface. The architecture used in CATV based Telecommunications networks is called IP Cablecom and specified in ETSI TS 101-909 series.

In ETSI TS 101 909 2 [33] clause 4.4 several services offered within the IP Cablecom network like Calling Identity, Recall are specified. In principle the used MTA or IP phone have to support these services.

As stated above, VoIP techniques are used in cable networks. Therefore it is important to consider the Quality of Service (QoS) aspects. IP Cablecom supports priority mechanisms of emergency services as described in ETSI TS 101 909 2 [33] clause 4.4.2.

There are two scenarios in requesting QoS discussed

- Scenario 1: During call set up the terminal issues a bandwidth reservation request to the call management server (CMS) and the CMS sends a special message element and grants the request.
- Scenario 2: The CMS analyses the dialled number and decides to reserve bandwidth in case of an emergency.

IP Cablecom defines a possibility to change QoS parameters during a call. This possibility 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 of normal calls in favour of emergency calls.

IP Cablecom must support a list of element messages including emergency services as depicted in ETSI TS 101 909 10 [34] clause 7.1.

In most cases an emergency call is an On-Net to Off-Net call. This means that the customer is located at the cable network and the Emergency Call Centre is located in the PSTN. In this case the emergency call is routed via PSTN gateways to the Emergency Call Centre. ETSI TS 101 909 10 [34] clause 9.2.1 defines that special trunks are used for emergency calls and explains how this feature is used by the CMS.

From the point of emergency the availability of the emergency service is also a very important aspect to look at. ETSI TS 101 909 17 [37] clause 8.1.7 describes a pre-emption technique where the access network is able to issue a pre-emption priority element to free pre-reserved resources in favour of emergency calls. It should be noted that only the access network and not the MTA is able to provide pre-emption priority elements.

Note: Pre-emption is normally prohibited in public networks. Thus, this feature should be revisited in IPCablecom.

7.5.3 Access

A possible solution in offering emergency services to the customer besides dialling an emergency number is to implement a “red button” or “panic button” on the used device. This might be done implementing a new button in new manufactured analogue (POTS) or legacy digital (ISDN) phones or to use an already existing button and to assign an emergency number to it. If the customer presses this button a collection of digits representing an emergency number is sent to the CMS and the CMS provides the necessary services like pre-reservation of bandwidth and routing to special emergency trunks.

7.5.4 Installations

In general the cable modem that is located at the customer premises is not operational in case of power loss. Normally the cable modems do not have a backup battery included. This aspect is very critical in regard to emergency calls. As discussed earlier it is possible to use analogue (PSTN) or legacy digital (ISDN) phones in connection with a MTA to use telephony services in cable networks. In ETSI TS 101 909 24 [36] clause 7 and ETSI TS 101 909 18 [35] clause 5.2 the implementation of backup batteries and minimum requirements for availability are recommended.

The customer can use an IP phone that is connected directly to the cable modem without MTA. In this case it is recommended that to implement a backup battery or to power the cable modem from the cable network.

7.6 CATV infrastructures without Telecommunications offers jcp

Editor’s note: EMTEL & AT-D, JTC Broadcast… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.6.1 General aspects

The traditional Broadcasting function for Radio and TV is a central support to the communication between authorities and citizens.

In EN 300 401, Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers, Section 8.2.3 deals with Emergency Warning Systems (EWS).

In EN 300 468, Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems, Section 6.2.2 gives details of the Announcement Support Descriptor.

7.6.2 TE

Regarding Emergency a cable TV system without telecommunication offers can be used for broadcasting warnings and emergency related information. This possibility of issuing emergency warnings should be included in national or local civil protection plans. The architecture of such CATV systems offers only the possibility to carry information to the users via downstream but there is no interaction with the users possible because of missing upstream capabilities.

As explained in ETSI EN 300 468 [41] clause 3.1 there are a few possibilities to downstream information in CATV systems like via satellite or cable or terrestrial. The user has only to provide a receiver with or without a conditional access module. The DVB receiver must comply the specifications provided in ETSI EN 300 401 [42] and ETSI EN 300 468 [41].

In ETSI EN 300 468 [41] clause 6.2.10 a country availability descriptor is explained and it might be useful for service operators on behalf of authorities to use this descriptor to make emergency warnings or information available only to a defined region.

Since DVB and DAB is a broadcasting service no location and no identification information of the user is available in case of an emergency. The user has to use alternative ways to communicate with Emergency centres.

As mentioned before it is possible to use DVB and/or DAB receivers with or without a conditional access module it is recommended not to scramble in case of an emergency so that every DVB / DAB receiver can receive the broadcasted emergency information.

ETSI EN 300 468 [41] section 6.2.3 defines an announcement descriptor that ca be used for emergency warnings and this clause gives also the possibility to specify the transporting method. Using these features can be valuable to support and reach impaired 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.

7.6.3 Access

Receivers are used for receiving broadcasted information. The user needs to connect additional equipment to watch the broadcasted information. This equipment might be television or audio equipment. There is no guarantee to reach all intended people in case of an emergency since the used equipment and also the receiver can be switched off.

7.6.4 Installations

To provide an always-on functionality it is recommended to implement a backup battery in receivers so that broadcasting can be received every time.

7.7 Fibre to the home jcp

Editor's note: EMTEL & TM1, AT-D, JTC Broadcast… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.7.1 General aspects

7.7.2 TE

7.7.3 Access

7.7.4 Installations

7.8 PLT sc

Editor's note: EMTEL & PLT… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.8.1 General aspects

7.8.2 TE

7.8.3 Access

7.8.4 Installations

7.9 Fixed radio access jcp/ ne

Editor's note: EMTEL & TM4… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

7.9.1 General aspects

7.9.2 TE

7.9.3 Access

7.9.4 Installations

7.10 DECT jcp/sc

7.10.1 General aspects

DECT is a well know and the most popular cordless technology in Europe at present. The best well known applications are associated with cordless telephones, the wireless local loop and PBXs.

DECT technology is used in

- Public Access Service (PAS)
- Business Cordless Telecommunications (BCT)
- Residential Use (RU)

It is important that the devices supporting emergency features respect strictly all appropriate requirements.

However, there are some restrictions to the emergency telephony service as provided by the DECT standard series EN 300 175.

- no connection between residential networks therefore no hand over, no roaming between public ones or residential and public networks

- emergency calling is defined in ETSI EN 300 175-5 but not implemented because of security issues (open base stations)- therefore it is performed like a normal call (a normal call is only possible when the terminal is authenticated)
- user authentication is mandatory for terminals but not for base stations (residential)
- in business cases : special services like vpn can be offered by DECT PBX and the use of it might be restricted by user authentication
- no reliability because if all speech channels of a base station are used it is not possible to make a call
- no priority available for emergency calls (more than one call at a base station – first come first serve)
- no identity of the user – only the cell information is available or better only the radio used by the terminal is known -> user information is not transmitted over the air

Using DECT hand set for an emergency call, the location information refers to the line where the base station is connected to and not to the hand set. The distance between the base station and the hand set may reach upto several hundred meters. Enhanced location information (location of the hand set) similar to GSM could be useful.

7.10.2 Simple TE

For DECT terminals, and in additional to the interface and basic voice standards referred to above, the reference standards should be the ETSI DECT Harmonised Standard EN 301 406????XXXXXXXXX TBR 010, TBR 006 and xxxx special feature for emergency recently developed.

It is recommended that DECT terminals fulfil the requirements for speech performance as depicted in ETSI EN 300 175-8 clause 7. DECT terminals should also support hand over procedures when the user in case of an emergency situation changes from one FP to another. Each base station has a manufacturer built-in identity. This identity is broadcasted from the base station. During the call set-up phase the portable checks the broadcasted identity and validates it if a locking in is possible. Since the DECT base stations are not connected to each other no roaming is possible also hand over functionality is only supported within one base station. In principle there are two forms of hand over procedures supported within a base station (bearer hand over and internal hand over). Bearer hand over procedure is done when the DECT portable switches from one radio to another to gain better quality. This is done in the MAC Layer see ETSI EN 300 175-3 for more information. Internal hand over is done when a base station has more than one fixed radio parts and the portable switches from one to the other fixed radio part. This hand over is called internal hand over and discussed in more detail in ETSI EN 300 175-4 Data Link Control Layer.

Generally availability and reliability of DECT systems are restricted by DECT coverage. It is possible that more than one FP is available for one area. Each base station offers a number of speech channels. At present there is no mechanism developed to ensure a free speech channel in case of an emergency. It is recommended to implement an algorithm in base stations so that a decision can be made which call to drop to gain a free speech channel for an emergency call

To gain a greater availability a technology called dynamic channel selection (DCS) is used. This technique tries to share the available channels as effectively as possible to achieve a high and reliable traffic. Even though DECT terminals made the traffic channel selection, the base stations must also support DCS. See also ETR 310 clause 5.2 for more details regarding this technique.

At present DECT base stations in residential environment are not connected via a network. This means that it is not possible to have roaming functionality which might be useful when an emergency situation occurs. Because of security issues each DECT portable must authenticate itself at the base station. More information regarding the authentication can be found in ETSI EN 300 175- 5 clause 13.3.2

In ETSI EN 300 175-5 clause 9.8 requirements for an emergency call are defined. Through the Inter Working Functionality a special message element indicating an emergency call is implemented. It is necessary that the base station is able to handle this special element so that no authentication is needed to make the call. This implies that DECT base stations should not request authentication and each DECT portable can start an emergency call without logging in. That means no validation of the broadcasted base station identifier by the DECT portable.

In residential environments user authentication is mandatory for DECT portables. In ETSI EN 300 175-5 clause 13 a few portable user identity types are defined. It is suggested to use portable user identity type N for emergency calls. It is optional for DECT base stations to have user authentication implemented.

In ETSI EN 300 175-5 clause 13.4 procedures handling the location information are defined. Both parts in a DECT system the fixed and the portable part must have these location procedures implemented. Therefore the base station knows the location of the portable part and if the portable part is ready to receive calls. However the user identity is not transmitted over the air and the base station knows only the terminal identity. In case of an emergency call the user must provide some information to specify his location.

In Residential DECT systems all authenticated portables are ringing simultaneously in case of an incoming call. If the customer has a ISDN access and a DECT system with two portables each portable has its own number. Therefore in case of an incoming call only one portable will ring. In case of an emergency with call back functionality the right portable can be reached.

Some Emergency Call Centers offer call-back functionality. If a customer, who has PSTN access and a DECT system with more than one portable, uses one portable to make an emergency call offered call back functionality cannot be used. When the Emergency Center operator calls back all portables will ring simultaneously. As a consequence a call forward functionality from one portable to another must be implemented. A possible solution might be that the base station records all calls and decides where to route the incoming call. Alternatively the PSTN network supplies an additional digit which is mapped from the base station to a portable.

7.10.3 PBX and complex TE

In business environments DECT PBX systems are used. In such a scenario more than one DECT base station are connected together and the network provides routing and roaming / hand over functionality using CENTREX functionality. All DECT portables in such business DECT systems are pre-authenticated by the manufacturer. Therefore it is not possible to use un-authenticated terminals. All DECT base stations broadcast two identities and all pre-authenticated portables know these. In business or public DECT solutions where multiple base stations are available in different locations hand over from one base station to another (external hand over) is possible.

In business environments a special emergency service is possible but it is not generally defined (manufacturer dependent).

In DECT PBX systems no priorities for special calls are defined, but it might be possible that a manufacturer implements special message elements in the base stations used in such a system as proposed in ETSI EN 300 175-5 clause 9.8. These message elements can be used to classify a call as an emergency call and the base station can provide a free speech channel by dropping a call in case that all speech channels are used. In regard to this special message element no validation of the broadcasted base station identity is done by the DECT portable.

For special services like VPN user authentication must be implemented on both sides PBX and terminals. For DECT terminals it is mandatory to have user authentication implemented. For base stations of PBX DECT systems the implementation of user authentication is optional.

In DECT PBX systems there is no location information that identifies the user available. Only the radio that is used by the DECT portable is known. In case of an emergency call the user must specify his location. Alternatively an additional message element containing the base station identity could be defined an transmitted to the PSAP.

In business solutions security is an aspect that must be concerned. As defined in ETSI EN 300 175-5 clause 13.8 a DECT portable can initiate a ciphering procedure that is handled by the MAC Layer (see ETSI EN 300 175-3 for more details) and used to encrypt the communication between portable part and fixed part. In case of an emergency this encryption might also be requested to protect sensitive user data.

In business environments DECT PBX systems have a mapping and routing functionality (Direct Dial In) implemented so that in case of an incoming call the right portable is ringing. Therefore the use of call back functionality, if offered by an Emergency Call Centre, is possible.

7.10.4 Access

In ETSI EN 300 176 limit values of environmental conditions like temperature and power supply issues are discussed. Also in ETSI EN 300 175-2 clause 5.2.3 requirements for minimum power under extreme conditions for transmission of physical packets are defined. As discussed above DECT portables use a technique called dynamic channel selection to achieve best traffic parameters like field strength and bit error rate depend if the portable is equipped with an antenna. In case of an emergency this can restrict the use of emergency service (the signal strength is too weak for call setup or the call is disconnected).

7.10.5 Installations

In ETSI ETR 056 Annex A clause 3.4 various scenarios of DECT systems are explained in more detail.

7.11 Other less deployed terminal access technologies

The emergency features as described in chapter 4.4.2 can be deployed in terminals with different access technologies, including radio, optics, cable, power line and others. It is nevertheless recommended to deploy these features primarily in terminals with harmonised wide spread interfaces like those referred to in chapter 6, clauses 6.1, 6.2 and 6.12. This will facilitate an earlier deployment and a wider coverage, therefore better service for a wider population.

Note that normally technologies like Wireless Local Loop and cable-TV based have their gateways to the conventional technologies in particular to the analogue PSTN interface terminals. These gateways should strictly respect the needs reflected in the standards describing the interfaces offered to such popular terminals.

8 Service Connectivity

8.1 General

This clause analyses the impacts of the requirements developed in clause 0 in regard to TEs and their means of connecting to a certain service. However, for the time being only IP based terminals are considered.

The technical functional requirements for terminals as described in the beginning of clause 0 also apply for IP based terminals. The different technologies used on different layers introduce a wide range of possible implementations for those features. Systems designer may choose between different ways of realization. Thus, the implications of the functional requirements to the used technologies must be evaluated on a per case basis.

Aspects related to user identification and localization are discussed in chapter 6.3.5 und 6.3.6.

8.2 Availability

Availability is important for all types of terminals. The mechanisms to ensure that terminals are also operable in situations of disaster are the same than for terminals. Some possible measures are listed in clause 0. Especially, the In-line power supply for IP terminals, Power over Ethernet (PoE), is important to be noted. The Institute of Electrical and Electronical Engineers (IEEE) standardizes PoE in 802.3af [25].

8.3 QoS in Emergency Communication

Under normal conditions emergency communication should not be worse than that of basic communication services. [SR 002180] states this for the case of an emergency call.

Note: To Put in NENA requirement that says call setup times need to have a maximum value!

In order to comply with this requirement IP based terminals shall implement all client-technologies required to support QoS models developed for the IP layer. Two QoS models are standardized at the Internet Engineering Task Force (IETF); the Integrated Services (IntServ) framework and the Differentiated Services (DiffServ) model. At ETSI, TC TISPAN WG5 is dealing with QoS issues.

8.3.1 Others

QoS mechanisms are not restricted to the IP layer. For example DOCSIS [ref DOCSIS] uses MAC layer service flows to provide QoS. To determine the policy of bandwidth allocation many systems use the IETF protocol Common Open Policy Service (COPS) as standardized in IETF RFC 2748 [ref RFC 2748].

9 Private Networks and Communication Systems

Editor's Note: Ref to 002 180 for location info- should be made available if possible (4.1.1.6, 4.2.1.2.3). 002 180 4.5.1 Emergency calls should be given priority.

9.1 Ethernet, IP terminals ie

Editor's note: EMTEL & TM1, AT-D, JTC Broadcast… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

See also clause 6.13 recently drafted

9.1.1 General aspects

The implementation of emergency services on fixed-line Ethernet terminals requires to consider the following:

- Line and Terminal Identity (check with 4.6, 6.3.4/5)

  The identity of fixed line Ethernet terminals is given by the assigned IP address. All Ethernet terminals support the DHCP Protocol and receive their IP addresses from the Mainframe. Regarding the DHCP functionality a planning of the IP assignments to Ethernet terminals is needed. Since the handling of emergency communication is done on application level IP address information is available and can be transmitted to the ECC.

  Note: The IP address information may be used to perform a mapping to the physical location of the Ethernet terminal in small restricted areas. Delivering of this information across firewalls presents difficulties. A global database may be unlikely.

- Power over Ethernet

  The Standard IEEE 802.3af specifies PoE issues for PoE enabled terminals. Ethernet Terminals that are "always on" should support the PoE Standard otherwise back-up battery functionality is needed. Power supply must be guaranteed on permanent basis to ensure the availability of Emergency services.

- Quality of Service

  Fixed Line Ethernet Terminals have "always on" functionality and are connected to a Mainframe on a permanent basis. It might be possible that a special keystroke combination or even a special key issues a command or set of commands that can be interpreted by the operator of the Mainframe. In this case these keyboard actions "override" all other applications and commands. The operator of the Mainframe takes the necessary actions to supply Emergency Services e.g. contacts a PSAP.

- Routing / Priority

  Fixed Line Ethernet Terminals need a connection to a Mainframe for operation. In case of an Emergency it might be possible that an application running on the Mainframe or the operator broadcasts a special emergency message. In this case the TE displays this message or possibly produce audible alarms so that the user is aware of the Emergency case. Otherwise it should be possible that a user starts a voice conversation or at least issues a voice message with the operator at the Mainframe in case of Emergency.

- Localisation

Note: fill

- User Identity

  Fixed Line Ethernet Terminals can be used by multiple users. The location of the fixed line Ethernet terminal is well known. Therefore in addition to the transmitted IP address it could be also necessary to transmit the user credentials in case of Emergency. This mechanism ensures that the ECC is able to identify the user.

- Security

Note: fill

In addition to the required support for the protocols there are a few functional requirements needed for fixed line Ethernet Terminals.

- Keyboard Support for keyboards with 122 keys
- Local Language Support
- Display Support for LCD, TFT, touch screen
- Windows-enabled
- Implementation of a local web browser for the use of Web-Applications
- Implementation of a Mail-Client
- Audio Support for Audio-Out
- Microphone Support for Voice Chat
- Reception of Broadcast Emergency Messages
- Displaying of Alarms (audio – or video signals)

9.1.2 TE

In general there are two different types of Ethernet terminals available.

- Text based Terminals
- Window based Terminals

The Emergency Services listed below can be used with both terminal types:

- broadcast messages (only in direction authority to customer)
- special keystroke combinations (in both directions authority to customer and vice versa)
- special commands (in both directions authority to customer and vice versa)

Text based terminals with audio support can also use the following Emergency handling mechanisms:

- audio messages (in both directions authority to customer and vice versa)
- audio conversation (in both directions authority to customer and vice versa)

Window based terminals can also use the following Emergency handling mechanisms:

- if the terminal has audio support
  - audio messages (in both directions authority to customer and vice versa)
  - audio conversation (in both directions authority to customer and vice versa)
- video messages (in both directions authority to customer and vice versa)

- video conversation (in both directions authority to customer and vice versa)

Furthermore there is a difference regarding the connection type used:

- Fixed Line Ethernet Terminals are referred to as Thin Clients
- Wireless Ethernet Terminals are called Tablet PCs

9.1.3 Access

- Fixed Line Access is implemented in most of the currently available Ethernet Terminals through standard IEEE 802.3 [25]. Supported cabling mechanisms are twisted pair or coaxial.
- WLAN Access is used by Wireless Ethernet Terminals like Tablet PCs. In this case the implemented standard is IEEE 802.11.

Note: The WI-FI Alliance promotes WIFI and offers certification programs for vendors.

9.1.4 Installations

The following aspects of Ethernet Terminals are to be taken into account during installation:

- Dimension;
- Weight;
- Power Consumption;
- Isolation;
- Environmental Conditions (ETSI EN 300 019-1-3 V2.1.1 and ETSI EN 300 019-1-4 V2.1.1).
  - Temperature Range
  - Humidity
  - Physical Handling (Shock, Vibrations)

For Fixed Line Ethernet Terminals cabling should be done in a reliable and safe way. This is necessary to ensure that the quality of the connection fulfils the requirements in case of Emergency.

9.2 PBXs and Collective centres (SR 002 180)

9.2.1 General aspects

Emergency calls from private networks may be routed via an attendant or collective centre and from there be switched over to the public network.

Depending on the nature of the emergency (internal/external), an attendant service may be required according to local legislation to determine the nature of the request, either internal or external. When external assistance is required a collective centre is expected to immediately forward an emergency call to the PSAP or the corresponding emergency control centre.

This includes phones in public places where users expect to make emergency calls, free of charge and without having to use any means of payment.

Location information within the geographical region managed by a collective centre should be made available when possible and shall comply with the requirements of the corresponding emergency authorities in the area.

9.2.2 Simple legacy TE

There are a few requirements and recommendations available concerning and supporting emergency calling.

In ECMA 263 two supplementary services called Call Priority Interruption (CPI) and Call Priority Interruption Protection (CPIP) are defined.

Call Priority Interruption (SS-CPI) as defined in ECMA 263 is a supplementary service that allows a call request for a priority call to proceed successfully in case that there is no user information channel available. The supplementary service maybe invoked by the calling user. The invocation of SS-CPI is done during the call set-up phase. It can be issued either by pressing a special key if implemented on the terminal side or when the dialled number can be classified as an emergency number.

Call Priority Interruption Protection (SS-CPIP) as defined in ECMA 263 can be invoked either by the calling user during call set-up (clause 7.2.2) or the called user (PSAP). The use of SS-CPIP is recommended in case of an emergency call so that the availability of PBX resources is guaranteed.

In ECMA 263 clause 4.10 the possibility of assigning priority levels to calls is defined. It is defined that a priority call has a priority level greater than zero. When SS-CPI is requested to assign a priority level greater than zero to a call the availability of a free channel is guaranteed. As described in ECMA 263 clause 6 in case that the route is not available a forced release of non-priority calls including in-band warning to users of an established call is done.

If the PSAP is connected via a PBX it is recommended that the SS-CPI(P) services should be implemented in this PBX and the terminal of the PSAP operator. The signalling and inter-exchange handling is explained in more detail in ECMA 264.

Location information is well known since the terminals are wired to the PBX. The User Identity is normally unknown because user authentication is not mandatory and therefore the PSAP operator must ask the caller. Since the location information of the terminal is well known it is possible to transmit this information in-band the emergency call to the PSAP operator. It is also possible to offer Call Back Functionality since the terminal is always on. It is required that the PBX has the Supplementary Service DDI (direct dial in) implemented.

Multiparty Calls are implemented as supplementary service on PBX and terminal side and can be invoked by the PSAP operator and used in case of an emergency.

9.2.3 System specific and intelligent TE

One possible solution to made emergency calls easy available is the introduction of a “Red key”. As mentioned in clause 4.4.2.1 a special key on the terminal can be assigned to issue an emergency call. This call can be given a priority greater than zero during call set-up when using the supplementary service CPI. The supplementary service CPI must have been implemented by the manufacturer of the PBX and of the terminal.

Furthermore it might be possible that upon dialling an emergency number the terminal requests the SS CPI to assign priority to the call. This request can be issued during the call set-up phase.

9.2.4 Access

The terminals are wired to the PBX. Terminals should have in-line power supply (called loop powered) implemented if that is provided from the PBX. This is recommended to guarantee highest availability even in system power outages.

9.2.5 Installations

Installations in private environment, in particular when there is no professional usage, are often subjected to changes like inappropriate cable extensions or unprofessional connection methods or changes to the settings of the equipment and the installations not necessarily following the state of the art and the guidance of the manufacturers, installers, operators and service providers. This is a fact that can hardly be changed due to the necessary respect of the private property. Nevertheless appropriate measures at a level of user information may limit the negative impact of the actions mentioned above.

The design of all the equipment to be installed in the private domain and associated installations methods should always follow the standards. Standards in this domain (see clause 10) should take in consideration the basic needs in a

emergency situation and try to limit the possibility of inappropriate actions impairing the functionality of communications systems in such situations.

9.3 Home networks, LANs and private networks sc

Editor's note: EMTEL & AT-D, CENELEC… to co-operate,

some clauses may be limited to a simple reference to the most relevant document developed by another TB.

9.3.1 General aspects

9.3.2 Simple legacy TE

9.3.3 NGN and intelligent TE

panic button from alarm systems

9.3.4 Access

9.3.5 Installations

10 Installations and infrastructures dr(cenelec215)/jt *(importance questioned)*

10.1 Physical installations/ cabling

Editors Note: TC 215 has published EN 50173-1:2002 on Generic Cabling Systems (which is almost identical to the international cabling standard ISO/IEC 11801:2002 - produced by ISO/IEC JTC 1/SC 25 - and which replaces EN 50173:1995 and its Amendment A1:2000), series EN 50098 on dedicated ISDN cabling, three standards in the series EN 50174 on IT cabling installation, EN 50310 on the application of equipotential bonding and earthing requirements in buildings with ICT equipment and EN 50346 on testing of installed IT cabling.

Editors Note: Future parts of series EN 50173 will specify particular requirements of cabling systems for residental and ***industrial*** premises as well as for data centers. The series EN 50174 concerning installation practices inside and outside of buildings is being revised to cover new needs typical for the residential/industrial/data center environment. New developments related to the testing of optical fibre cabling will be introduced with the revision of EN 50346.

Editor's note: EN 50174-2, Information technology – Cabling installation – Part 2: Installation planning and practices inside Buildings

To withstand disasters cabling shall conform (if existing) to appropriate standards like e.g

- ETSI I-ETS 300 634 "Title: Transmission and Multiplexing (TM);Single-mode optical fibre cables to be used as underwater cables for lakes and river crossings etc." [26]

10.2 Device configuration and provisioning (jt to improve title)

Terminal equipment should be pre-configured, pre-provisioned in order to ease (self-)installation (goal: Plug&Play). Configuration should be minimized, e.g. through prepared configuration files and settings.

Editors Note: ETSI EG 201 212: "Electrical safety; Classification of interfaces for equipment to be connected to telecommunication networks".
ISO/IEC 11801: "Information Technology; Generic Cabling for Customer Premises"

11 Information to the users jt/rf/wm

Effective emergency communications is crucial during incidents.

Therefore, it is most important that the user:

- is informed about what he has to do in case of an incident (generally) so that he reacts in an appropriate way;
- understands information delivered to him during an incident.

Instructing a user how to react in case of an emergency requires that there is information that prepares the user to do so. This information should be spread as broad as possible so that as many people as possible know exactly what to do, for example on emergency call posts. People also need to be informed about the kind of information he is supposed to give to the emergency centre. This should include:

- Identity of the person;
- Location of the person;
- Type of incident;
- Impact of the incident; e.g. how many people are injured and how severe;

For information that is known to the TE or the network (identity, location information), it should be provided to the ECC (e.g. GPS capabilities). Clause xxx discusses TE capabailities 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 like 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 like sport arenas. These advertisements should contain contact information how to get in touch with PSAP in case of an emergency. If there are location specific emergency services provided, like 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 like contact numbers, special emergency numbers, if there are others available besides the 112, and a description how to issue an emergency call. 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 amount of people all established civil protection plans and methods like issuing audible warnings via 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; e.g. Broadcast services
- Pull Services; e.g. information web page
- Off-line; e.g. via information handed out on service subscription with the contract

Such a broadcast emergency service may be realised for example via SMS. In case of an emergency or disaster, the SP issues a short message to a certain group of users, for example in a particular area. A further possible broadcast emergency service is the sending of newsflashes or updates about the state concerning the SP's emergency system, or system outages to users.

Service Providers may also offer information about emergency system's and communication services for example via Hyperlink to a web page dealing with such issues. The scenario may look as the following: when a user accesses the SP's service the user 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 shall be open for users and not bound to service subscription or any other type that requires payment.

A subscriber may also at the time of service subscription be given emergency service related information. This may either be through e.g. an information sheet that he gets in addition to the contract. A remark describing the offered and guaranteed emergency services may even be included in 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 must be included in the delivered documentation. A listing of operator dependent and operator independent emergency services should also be added.

11.4 From special organisations

Profit and non-profit organisations like a private medical rescue service or a private security service might also be locally available. These organisations have to advertise their emergency services in local newspapers, flyers, radio and television programs. The advertisement must 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 jt/all

12.1 Power dependence

With the development of new technologies like solar or wind energy in parallel with the strengthening of existing power distribution, power dependence may be in the future solved by an increased developed locally generated energy. An important issue is also to spread the implementation and use of power over Ethernet techniques in terminals and access networks.

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 coax cables elector magnetic influences can also be minimized.

One further aspect is the protection against misuse and criminal misuse. 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, e.g a telephone in a supermarket.

Editors Note: move text to 6.3.1 and enter cross references at both sides

13 Special needs on standardisation identified jt/all

13.1 Communication from citizens to authorities

This type of communication includes the most typical emergency situation when a customer issues an emergency call using his or her own equipment or using a public available equipment like a public call post. Another possibility is mentioned in the project MESA (www.projectmesa.org) and deals with transmitting of monitoring data to an authority.

The possibility of surveilling certain situations or parameters, e.g personal charactistics, might be used in immediate medical support for elderly people to pre-recognize and alert the appropriate specialized center 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 like banks, so that an employee in an emergency case has the possibility to issue an emergency call based on earlier, trusted information obtained form a number of consistent alerts. In this case the data transmission functionality may be connected directly or indirectly to the ECC. In the indirect case the alarm is dealt with by an intermediary organization e.g. a specialized security service. "Silent alert" is an example for this type of service.

Generally, ETSI SR 002 180 [1] specifies the requirements for communication from citizens to authorities in case of distress.

13.2 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 are well trained in

contrast to a citizen making an emergency call. Furthermore, terminals should support also the transmission of this collected information to another ECC or PSAP.

ETSI SR 002 181 [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.

13.3 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. ETSI SR 002 182 [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 ETSI SR 002 182 [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 text service on terminals is necessary.

13.4 Communication amongst affected citizens

ETSI SR 002 410 [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 and MMS. 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 CPE as mentioned also in this document in clause 0.

14 Conclusions

14.1 General

14.2 Need of changing or completing present standardisation

Editor's Note:

- SMS profile for emergency communication (since SMS always routed to SMSC in home network)
- Localisation Info in DECT

There is a (evident, not evident, no) need to…. Because…

How, where to apply, implement, how to survey…

Need	Evidence	Justification	Remarks

	Importance		

14.3 Other aspects

.

Annex A:
Information to be kept during work, to be deleted before publication

A.1GSC 8 & 9 resolutions


"GSC-8-1-Emergency Communications.doc"


GSC9-02_JOINT_Emergency_Communicat

Abbildung 1

A.2xxx

History

Document history		
V0.0.0	April 2003	1st proposal ToC and base structure
V0.0.0c	November 2003	draft reviewed structure and initial inputs for AT#8 review
V0.0.0f	Jan 2004	draft reviewed after AT#8, to collect inputs for inputs for AT#9
V0.0.1	June 2004	Revision after AT#9, to collect inputs for the work start of the STF OU
V.0.0.2a	040908	Kick-off meeting STF 274 notes
V1.1.3	October 2004	Draft with advanced generality text in sections 8 to 10 and sections 6.1, 6.9, 6.13
V1.2.0	October 2004	Draft with advanced generality text and incorporated comments of SG Meeting
V1.3.0	November 2004	Draft with further incorporated comments of SG Members and TC TISPAN Project EMTEL
V1.3.1	November 2004	Working draft; Incorporated comments of SG Meeting #2
V1.3.1rev	November 2004	Further update following comments
V1.3.3	November 2004	Update including comments received at AT#10
V1.3.4	December 2004	Working Draft
V1.3.5	January 2005	Working Draft after EMTEL-Rapporteurs Meeting starting Phase 2