

Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies



Reference

RTS/EMTEL-00009

Keywords

emergency

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2008.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	9
4 Description of the type of relations between authorities	10
4.1 Relation between PSAP and Emergency Control Centres.....	10
4.2 Relation between PSAPs	11
4.3 Relation between Emergency Control Centres.....	11
4.4 Relation between Emergency Control Centres and Mobile Rescue Teams/Agents	11
4.5 Relation between Mobile Rescue Teams/Agents	12
4.6 Relation between Special Task Force/Command Centres and Permanent Entities in special conditions	13
4.7 Relation between Military Authorities and Civil Authorities.....	13
5 Emergency services Communication Requirements	13
5.1 Methodology to determine the communication requirements	13
5.2 Actions that require Communications	14
5.3 Description of the required communications services	14
5.3.1 Speech services	14
5.3.1.1 Point To Point Speech Services	15
5.3.1.2 Group Speech Services	15
5.3.1.3 Push To Talk (PoC)/Command and Control (C&C) features.....	16
5.3.2 Video Teleconferencing.....	16
5.4 Data services	16
5.4.1 Paging Services.....	17
5.4.2 Status Monitoring and Location Services	17
5.5 Interoperability of Communication Services.....	17
5.6 Example application	17
6 Scalability.....	18
6.1 Priority schemes and traffic management	19
6.1.1 Traffic Management	19
6.1.2 Emergency Preference schemes.....	19
6.1.2.1 Interaction with the Emergency Call service e112.....	23
7 Requirements applicable to the Network(s) and user services, (services to support) and the network features and capabilities	24
7.1 Recognition and treatment of emergency services from the view of the service.....	24
7.1.1 Transmission quality.....	24
7.1.2 Ensuring conveyance of communications.....	25
7.1.3 Assignment of inter-authority calls to the appropriate authority	25
7.1.4 Preventing effects of discrepancies in coverage	25
7.1.4.1 PSAP routing in mobile networks	25
7.1.4.2 International cooperation	25
7.1.4.3 Cordless technologies.....	25
7.1.4.4 Interworking of Technologies	26
7.2 Recognition and treatment of emergency services by the originating network	26
7.2.1 Call-related information.....	26
7.2.1.1 Indication of the (emergency) caller's location	26

7.2.1.2	Identification of the mobile terminal equipment/subscription	26
7.2.1.3	Interworking of Technologies	26
7.2.2	Network identification	26
7.2.3	Minimum power supply for authority representative user accesses.....	26
7.3	Requirements on call handling between networks	27
7.3.1	Handling of inter-Authority calls between networks	27
7.3.2	Interworking with carrier selection/carrier preselection codes	27
7.3.3	Inter-Authority communications from other countries	27
7.4	Providing termination of Inter-Authority calls for the relevant authorities	27
7.5	Network Management support functions for delivery of Inter-authority calls	28
7.5.1	Priority of inter-authority emergency communication.....	28
7.5.2	Monitoring of the lines and availability of the Authority	28
7.5.3	Diversion of Inter-Authority calls.....	28
7.5.4	High or Resilient availability	28
7.5.5	Security provisions at the access to authorities.....	28
8	Security.....	28
8.1	Role of National Communication Security Authorities.....	28
8.2	General Security Issues	29
8.3	Interconnection of secure communication systems	29
Annex A (normative):	Basic Architecture.....	30
Annex B (informative):	Organizational related issues for Authorities to Solve	31
B.1	Handling of foreign languages	31
B.2	Mitigating consequences of radio coverage discrepancies.....	31
B.3	Definition of priorities (list of beneficiaries, levels, conditions of effective implementation)	31
B.4	Contingency planning.....	31
B.5	Organization of authorities in case of catastrophic event.....	32
B.6	Communication between civil authorities and non-governmental organizations.....	33
B.7	Communication between civil authorities and press organizations.....	33
Annex C (informative):	Security mechanisms	34
C.1	Symmetric encryption schemes.....	34
C.2	Asymmetric encryption schemes.....	34
C.3	Hybrid encryption schemes	34
C.4	Digital signatures.....	35
C.5	Authentication methods.....	35
C.6	Authorization schemes	35
C.7	Logging	35
C.8	Virtual Private Networks.....	35
Annex D (informative):	United Kingdom Interoperability Agreement between Chief Fire Officers Association, Ambulance Services Association, and The Assistant Chief Police Officers Association	36
Annex E (informative):	Bibliography.....	39
History		40

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 Specification (TS) has been produced by ETSI Special Committee Emergency Communications (EMTEL).

The present document is one of several deliverables covering the communication needs of citizens and authorities in emergency situations, as identified below:

TR 102 180 [7]: "Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)";

TS 102 181: "Requirements for communication between authorities/organizations during emergencies";

TS 102 182 [12]: "Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies";

TR 102 410 [13]: "Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress".

Introduction

The present document outlines the requirements for communications between emergency authorities, and the need for standardization in this area to support these requirements. Clause 4 describes the relations between authorities in general terms defining each authority. Clause 5 categorizes the emergency services communications requirements. Clause 6 discusses the scalability and priority issues, including the dynamic need to employ resources. Clause 7 outlines the requirements applicable to the network(s) and user services, describing the services and the network features and capabilities. Clause 8 raises a number of security considerations. The annexes describe some more operational considerations, which may be useful, background but do not constitute part of the communication requirements.

1 Scope

The present document addresses the requirements for communications between the authorized representatives who can be involved in the responses and actions when handling an emergency.

Clearly, the type and number of these authorized representatives in a given situation will directly depend upon the nature of the emergency. In the most frequent cases, only people on duty will have to intervene according to a day-to-day routine, but in some cases crisis teams or temporary headquarters will be called. In accordance with a plan, the additional resources will organize a mass action gathering and, if needed, include the resources of several centres, or even including in the rescue plan additional levels of administrative authority, private operators and associations. These new authorized representatives will follow instructions or orders from the administrative crisis authority; for example utilities companies (water supply, transport, energy, etc.) may have to stop the provision of service or install priority of service schemes or execute a coordinated schedule for the restoration of the infrastructure and the service, as applicable.

It is recognized that the public authorities keep the responsibility of overall management of actions during the duration of the crisis, establishment of pre-planned scenarios and, in specific locations, e.g. tunnels, underground transports, plants with high level of risk, organization of field exercises involving all these authorized representatives.

The present document describes the functional requirements for communications between the authorized representatives involved in the responses and actions when handling an emergency. The level of precision has been chosen to avoid interaction with the specific local, regional or national organizations and diagrams of relations between authorized representatives. It follows from this that adaptations will have to be done when implementing the present document at a local level.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
 - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
 - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

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

- [1] C(2003)2657 Commission Recommendation of 25th July 2003 on the processing of caller location information in electronic communications networks for the purpose of location-enhanced emergency call services, published on O.J.E.U. L 189/49 the 29.7.2003.
- [2] ITU-T Recommendation E.409 (2004): "Incident organization and security incident handling: Guidelines for telecommunication organizations".
- [3] ITU-T Recommendation G.114: "One-way transmission time".
- [4] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".
- [5] ETSI EN 301 419-3 (V5.0.2): "Digital cellular telecommunications system (Phase 2+); Attachment requirements for Global System for Mobilecommunications (GSM); Advanced Speech Call Items (ASCI); Mobile Stations; Access (GSM 13.68 version 5.0.2 Release 1996)".
- [6] ITU-T Recommendation E.106: "International Emergency Preference Scheme (IEPS) for disaster relief operations".

2.2 Informative references

- [7] ETSI TR 102 180: "Basis of requirements for communication of individuals with authorities/organizations in case of distress (Emergency call handling)".
- [8] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".
- [9] ETSI EN 300 403 (all parts): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control".
- [10] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".
- [11] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).
- [12] ETSI TS 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies".
- [13] ETSI TR 102 410: "Emergency Communications (EMTEL); Basis of requirements for communications between individuals and between individuals and authorities whilst emergencies are in progress".

3 Definitions and abbreviations

3.1 Definitions

(TR 102 180 [7] is considered the master document in terms of definitions, by the end of this revision the definitions are to be taken from TR 102 180 [7] and included here to ensure that we have the same definitions.)

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

access network: portion of the telecommunications network that provides access to the switching function and terminates the user access signalling, in a PLMN this is a radio access via a base station

NOTE: See ITU-T Recommendation Q.931 [8], EN 300 403 [9], TS 124 008 [10].

authority: organization within the public services fully or partly responsible for emergency preparedness and handling of incidents

authorized representative: individual officer or institution authorized by public service (fire, police or health) to play a key role in handling of an emergency case

emergency control centre: facilities used by emergency organizations to handle rescue actions in answer to an emergency call

NOTE: A PSAP forwards emergency calls to the emergency control centres.

emergency number: special short code(s) or number(s) which is used to contact the PSAP to provide emergency services

NOTE: The emergency number, is used by the emergency caller to request assistance from the emergency services. There exist two different types of emergency numbers in Europe:

- 1) **European emergency number, 112:** unique emergency number for pan-European and GSM emergency services and used, for example, in EU member-states, Switzerland and other European countries.
- 2) **National emergency numbers:** each country may also have a specific set of emergency numbers.

emergency response organization: e.g. the police, fire service and emergency medical services

emergency service: service, recognized as such by the member state, that provides immediate and rapid assistance in situations where there is a direct risk to life or limb, individual or public health or safety, to private or public property, or the environment but not necessarily limited to these situations (see Commission Recommendation C(2003)2657 [1])

fleetmap: parameter information programmed into the system infrastructure and into the subscriber radios to control how the radios will behave on the system

incident area: area where the incident occurred, and/or the area which needs communication coverage to manage the response implemented

location information: data processed in a public mobile network indicating the geographic position of a user's mobile terminal, and data in a public fixed network indicating the physical address of the termination point (see Commission Recommendation C(2003)2657 [1])

originating network: access network from which the emergency call was originated

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 [1]) New definition in 102 476 (23/1 2007, not available at the moment)

3.2 Abbreviations

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

C&C	Command and Control
CBRN	Chemical, Biological, Radiological or Nuclear
CQI	Call Quality Index
DGNA	Dynamic Group Number Assignment
DMO	Direct Mode Operation
EC	European Commission
ECC	Emergency Control Centre
FIFO	First In, First Out
GoS	Grade of Service
GSM	Global System for Mobile telecommunications
ICT	Information and Communication Technologies
IEPS	International Emergency Preference Scheme
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
LCS	LoCation Services
NCSA	National Certification Security Agency
NGO	Non-Governmental Organization
PLMN	Public Land Mobile Network
PMR	Professional Mobile Radio
PoC	Push To Talk
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
TCP/IP	Transport Control Protocol /Internet Protocol
TETRA	TErrestrial Trunk Radio Access
VPN	Virtual Private Network
VTC	Video TeleConferencing

4 Description of the type of relations between authorities

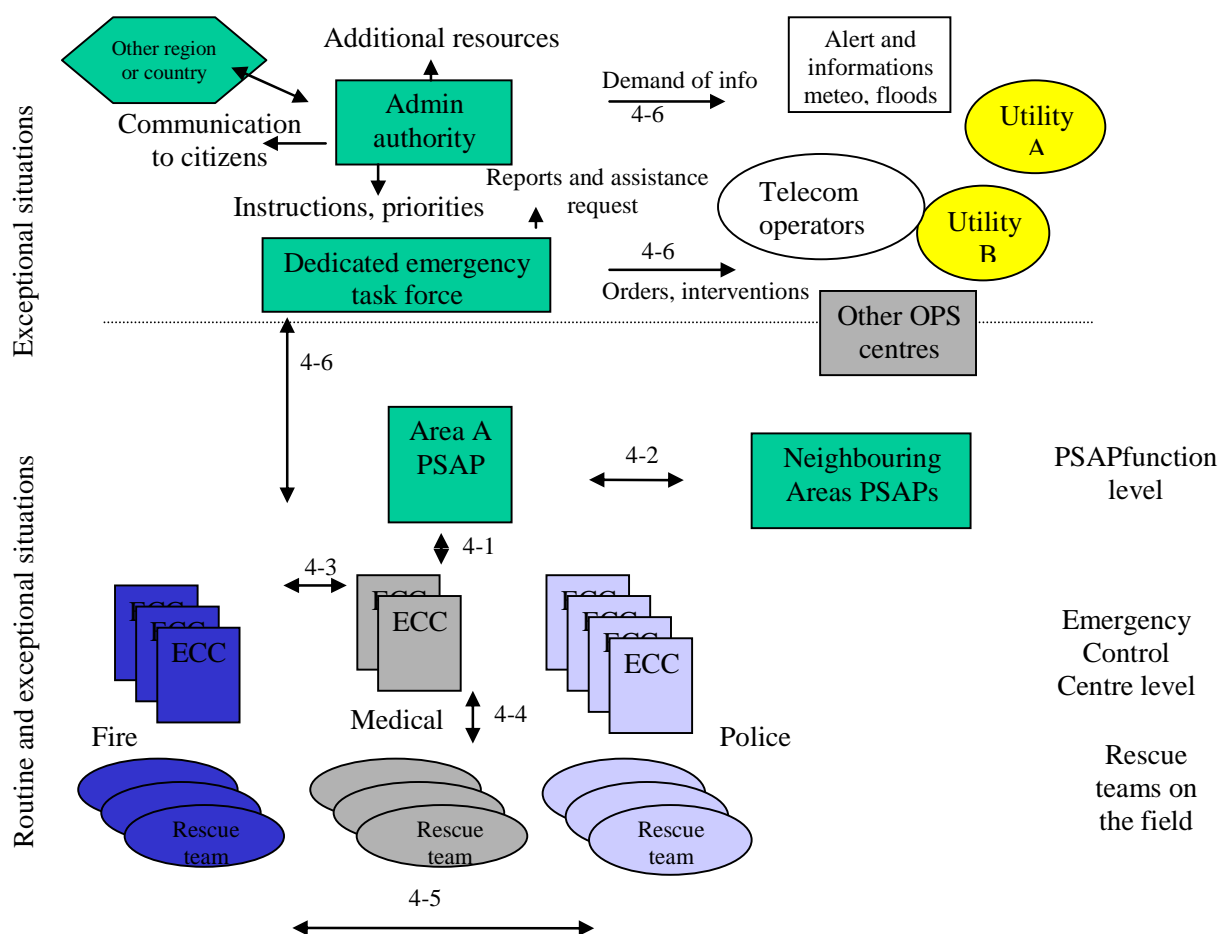


Figure 1: Reference points between functional entities

National bodies should enter into formal agreements to ensure interoperability between services at all levels of incident management. An example is shown in annex D.

The description of the type of relations relies on the model illustrated in figure 1. PSAPs/emergency control centres and rescue services in the field may be organized differently in different countries, e.g. in Sweden the PSAP and control centres for medical services and fire are combined, whereas police have their own control centres (to which calls are transferred from the common PSAP).

NOTE: The Military Agencies (**relation 4.7**) are not shown in figure 1.

The Temporary task force for coordination may be a pre-defined group which is activated according to set criteria, e.g. kind of emergency (landslide, earthquake, etc.), number of casualties, need for resources, etc.

The requirements in the present document cover both public and private networks. However, the implementation of all the requirements may not be possible in both types of networks.

4.1 Relation between PSAP and Emergency Control Centres

PSAP and emergency control centres are two different functionalities that may or may not be integrated.

The PSAP will, after reception of an emergency call, without delay communicate with the competent emergency control centre and transmit the location and nature of the emergency of the calling party along with any other relevant information that may be available associated with the call.

4.2 Relation between PSAPs

PSAPs normally work independently from each other, and their interrelation is not subject to special needs.

In cases where calls arrive at another PSAP than the one responsible for the area where the call is originated (e.g. mobile phones in the bordering area between different PSAPs), there may be a need to transfer the call together with additional information (e.g. location data).

The need will depend upon operation rules which have been established for these types of situation:

- the call is handled by the receiving PSAP;
- the call is immediately transferred to the PSAP appropriate for the incident area; in such a scenario the location data must be made available to the PSAP handling the incident, as for any received call;
- depending on local procedures, the receiving PSAP may transfer the call directly to the relevant ECC, possibly together with information to the correct PSAP that the call has been transferred.

It is the responsibility of the PSAPs or their organization to pre-define these rules of procedures.

4.3 Relation between Emergency Control Centres

ECCs need to have the facilities to collaborate with other ECCs either within the same service or across services (e.g. fire and health).

Examples of cases where this is needed:

- Calls are forwarded to an inappropriate ECC:
 - The call needs to be transferred to the correct ECC together with additional information (e.g. location data).
- Cases involving more than one ECC (e.g. fires with risks for human lives; typically involve fire, health and police, CBRN incidents (or suspected incidents), terrorism).
- The communications facilities exist to integrate the resources from two or more emergency control centres, in case of a larger emergency situation.(see figure 1, "Exceptional situations").

Communication requirements between ECCs must:

- Establish communication links to support a number of services, including speech and data.
- Support conference calls including external resources may need to be set up and kept over a substantial amount of time. In contingencies, calls to external resources may be required.

4.4 Relation between Emergency Control Centres and Mobile Rescue Teams/Agents

Access to permanent bidirectional links between emergency control centres and their mobile teams is crucial in the handling of emergencies and need to be available for the duration of the emergency/disaster.

The main communication needs of the mobile rescue teams, representing the emergency services can be briefly categorized as follows:

- specialized functionality in group communications and dispatching, with instant connection and including appropriate security, dynamic management of talkgroups, emergency calls, prioritization of communications, etc.;
- call establishment times, typical requirements for voice call set-up time in the range 0,3 s to 1 s.

- seamless radio coverage throughout the area affected by the incident itself and the areas of operational activities associated to the incident (rescue facilities, hospitals, etc.). - including means to maintain communication during network outage;
- incident capacity; the need for radio capacity is increasing during major incidents and accidents. Efforts have to be made to ensure as far as possible that sufficient communication facilities are available;
- a voice quality sufficient not to impair the understanding of the message;
- access to the network controlled by using functionalities such as assigning priority to potential users, thereby restricting some parties from access to the network under certain circumstances.

These communication links will facilitate the following aims:

- managing the teams and operational coordination;
- communicating between involved parties (mobile team members, control centre staff, receiving and assisting units/institutions);
- reassessing on a continuous basis the overall situation and the priority of the missions;
- enabling the reporting from the teams;
- enabling the teams to call for additional support and resources.

The above requirements are fundamental factors for the efficiency, the safety and survival of the victims of the incident as well as for the rescue agents themselves.

These actions remain the responsibility of a variety of public authorities, but it should be mandatory that technical systems provide solutions for all the above requirements. Technology provides tools to improve the effectiveness and efficiency when handling the tasks and procedures. It can never replace the responsibility of the authorities and the correct application of their agreed procedures in the event of an incident.

The need for radio coverage, instant access (network capacity), reliability and specialized communications facilities such as all informed net (group call) and fast call set-up, is normally considered best served by the use of a solution consisting of a private radio and fixed communications system, shared by several independent authorities. Risk assessments, together with moves towards cross-services and international collaboration, have led to an emphasis on interoperability between various services. For this collaboration to be efficient, the communication systems in use have to be interoperable.

4.5 Relation between Mobile Rescue Teams/Agents

For mobile rescue teams to work efficiently when handling a larger incident, they need facilities for communication with other mobile rescue teams involved in the same incident. The need is for communication across the services involved, as well as within each service. These links will facilitate the following aims:

- managing the teams and operational coordination;
- communicating between team members;
- reassessing on a continuous basis the overall situation and the priority of the missions;
- enabling the reporting within the teams;
- enabling the teams to call for additional support and other resources;
- exchanging information for guidance of the staff involved in the incident and assessment of the injuries and preparation of fixed rescue facilities before arrival of casualties.

Interoperability between the communication systems in use is a pre-requisite for the efficient handling of the emergency.

Fallback communication service needs to be available to the mobile rescue teams in cases where network service is either unavailable or disturbed due to the nature of the emergency/disaster.

4.6 Relation between Special Task Force/Command Centres and Permanent Entities in special conditions

For their efficient work in handling emergencies, special task force or command centres and emergency control centres are depending on access to permanent bidirectional links with the mobile rescue teams and other operational entities.

This access needs to be available for the duration of the incident/disaster.

There is a basic need for configurable communications to fulfil the needs for handling of potential incidents that are identified. This includes escalations from local to regional/national disasters.

4.7 Relation between Military Authorities and Civil Authorities

Military forces are routinely used to support emergency services and such involvement may take place in three types of scenario:

- a) during major national emergencies where military authorities provide manpower and equipment to supplement public safety resources. These incidents are frequently in response to natural forces e.g. flooding, earthquakes;
- b) for pre-planned support to public safety organizations for planned major event e.g. Olympic games;
- c) in response to man made emergencies e.g. terrorist incidents where specialist military skills or equipment are necessary and may form an integral part of the emergency response.

5 Emergency services Communication Requirements

While the nature of an emergency may vary greatly, the communications services which may be required by authorities is more definable, although there may still exist disparity in geographical area, scale and the number of authorities involved in any particular emergency. This clause is intended to describe mandatory communications services, together with other services which may be necessary or beneficial to users in some scenarios.

5.1 Methodology to determine the communication requirements

The great variety of emergency situations and events combined with the possible ways of their organizational and technical handling results in an extraordinary large number of different scenarios for which baseline requirements are laid down in the present document. However, the associated criticality and probability of occurrence of these scenarios may be very different. Therefore it is strongly recommended to carry out a risk analysis in each scenario and define the priority of handling for these scenarios. The procedures and actions required to be taken for handling the scenario shall be measured in dependence with the associated criticality, risk and probability of the scenario, taking into account the costs and resources required for the realization. When the probability of occurrence of a scenario is marginal, and its criticality is not high, the prescription of mandatory requirements may not be justified.

To present the requirements in the scope of the present document, a methodology has been chosen based on the following steps:

- identification of types of actions to be performed during the handling of the emergency case;
- if applicable, identification of the relations involved for these actions;
- identification of generic telecommunication or information exchange services which can help to perform these actions;
- identification of typical telecommunications services and overlying applications likely to be used in performing these actions;
- tentative combination of the above lists to illustrate a practical application.

It must be noted that the above methodology is not the unique way to handle the subject. It did, however appear appropriate to prepare a document enabling to approach the variety of situations encountered in reality. It is clear that no unique document can fix the detailed requirements of a given team or entity working in a unique social, geographic, administrative and economic environment.

An alternate methodology would be to examine the historic communication requirements from previous emergencies. While this method is being undertaken to provide a guide of services used, it recognizes that communications between authorities during emergencies in the past was sub-optimal. Similarly, a historic evaluation cannot in itself identify all future requirements.

5.2 Actions that require Communications

Communication requirements for emergency services shall be concerned with ensuring that the required information is available to the correct person or organization at the appropriate time.

In essence communications must be timely, relevant and accurate for all actions that maybe undertaken.

Examples of situations requiring such systems are provided below:

- Mobilization of resources.
- Pre-informing related authorities of the services required from them e.g. informing hospital services of arriving casualties and their needs.
- Relay of command and control information to the incident area.
- Request and receipt of information from specialist sources where abnormal hazards are involved e.g. hazardous materials, biological agents, etc.
- Transmission of images (still pictures and video) from an incident to a central command point.
- Transmission of updated information on the state of the incident and status of actions to the ECC and to other forces at the site of the incident.
- Transmission of control information from ECC to the emergency location. This may involve point to point, point to multi-point or broadcast communication services.

5.3 Description of the required communications services

The efficiency of the emergency operation is dependent upon the ability of the communications network to deliver a timely exchange of information between several authorized emergency personnel. This can occur at various levels in the emergency situation: e.g. between mobile rescue teams, between ECCs and the mobile, and between a temporary task force/command centre and a permanent PSAP/ECC.

The efficient exchange of information may be facilitated by a number of communication services, described below.

5.3.1 Speech services

Speech services are currently the most instinctive and most used communication services in emergencies, and this is likely to remain the case for years to come. This clause does not imply that a particular technology or switching mechanism be employed in the provision of speech services.

For speech services there exist several universal requirements, characterized by:

Speech intelligibility: that received speech is capable of being understood reliably, this is required even in the presence of high levels of background noise and/or when personnel are under stress or exertion.

Call setup-time: short call set-up times enable rapid communication of relevant information. Communication mechanisms which require unacceptably long call set-up times may endanger life, or users may resort to setting up a connection before it is necessary and keeping it connected when not required in order to avoid an unacceptable delay when communication is required.

End to end delay: in addition to the delays noted for call set-up times, it is recognized that where a duplex voice communication system imposes an end to end delay of over 500 ms there is a degradation in the communicability of the users. (International telephone connections and circuits - General Recommendations on the transmission quality for an entire international telephone connection One-way transmission time, ITU-T Recommendation G.114 [3] Telecommunication standardization sector of ITU (05/2003).)

Speech quality: although the prime attribute for a speech service in most emergencies will be intelligibility, there are cases where high speech quality is desirable. These cases may be when liaising with authorities or organizations unused to public safety communications e.g. external specialists; or where a level of trust is required to be established, e.g. NGOs, community groups.

Within speech services there may exist a requirement for prioritization and pre-emption of calls. The implementation of such features will be dependent on the technology employed, and the use of such features will be determined by procedure and organizational systems.

Underlying networks should have the capability to handle prioritized calls correctly, including the capability of pre-emption of unprioritized calls. Transit networks should convey priority related signalling in order to support end-to-end priority.

5.3.1.1 Point To Point Speech Services

Point to point duplex voice communications are required for many instances to provide communications, particularly between different authorities e.g. between commanders of different emergency services, between emergency service staff and external specialists.

5.3.1.2 Group Speech Services

The use of group speech services of various types is well established in all fields of public safety, although these services are frequently only provided with one service and/or users from one geographic area.

During emergencies the same communication services will be required, but the personnel utilizing them may differ. There will be a requirement in some cases to form groups containing members from multiple services and/or multiple geographic units.

Sufficient interoperability should be provided by systems to support group services across multiple networks. Interfaces between networks should support enhanced speech services such as *Advanced Speech Call Items* see EN 301 419-3 [5] between networks as well as within them. Group members may be drawn from different services and be issued with different communication terminals. Mechanisms to support dynamic creation of multi-service teams are desirable.

Group services may for example consist of several mobile rescue teams for an unlimited period of time and are required to be in a permanent relationship. Or it may consist of several mobile rescue teams for a limited period of time and require a simple procedure to form a relationship, for as long as it is required.

Each individual may belong to one or more teams. It should be possible for the individual user to identify which group(s) is/are active at any given time. To facilitate this one or more of the following example services may be utilized:

Talk group: Point-to -multipoint group addressed communication established within a selectable predefined area. The coverage is associated to the group number and may be different of the total coverage. Resources are allocated all the time. Any concerned user may enter or leave the talk group at any time.

Emergency services call (authority to authority): On a user action a status shall be sent by the terminal. Two options shall then be possible (as an operator option):

- Automatic call set-up of a pre-emptive open channel.
- Using a pre-emptive priority, a predefined user (e.g. ECC) shall establish a call chosen on an operational basis.

EXAMPLE: Open channel, ambience listening, individual call.

Ambient listening: This functionality shall enable a dispatch position to switch an individual piece of equipment into transmitting mode without any indications being noticeable at the piece of equipment itself. This functionality is only to be available in PMRs.

Intrusion: This service shall allow an authorized user to intervene in an ongoing authority-to-authority call.

Priority call: This service shall allow a call to proceed before any other call with lower priority. The priority level can be assigned according to various criteria.

Dynamic group number assignment: This service shall allow a served user or an authorized user to create, modify and delete a group (dynamic regrouping/group merging).

5.3.1.3 Push To Talk (PoC)/Command and Control (C&C) features

Especially in emergency situations it is necessary to avoid network congestion. Even in case of high traffic on the network communication between individual users (point-to-point) or existing or ad-hoc user groups (point-to-multipoint) PoC has to be enabled. It shall be possible to add and remove users from the communication group dynamically during the session.

Communication should require as little bandwidth as possible. Preferably it should not occupy lines permanently (as most of the group communication services mentioned above do) but data or voice should only be transmitted if information is actually exchanged. This holds especially for emergency communications characterized by many short speech items transmitted between talkgroup members over a certain period of time (e.g. giving and receiving instructions in C&C communication).

To facilitate this simplex communication services like push to talk can be used. PoC helps to avoid network congestion by transmitting voice over a data channel (GPRS, UMTS) and thus can be used even in times of high traffic on the communication network. Furthermore PoC provides flexible management of user groups.

5.3.2 Video Teleconferencing

VTC may be required to enable effective coordination between services at a command level or below. VTC services may be utilized to provide reconnaissance information from the incident back to control rooms.

5.4 Data services

Data services are used to provide a large number of applications which can have widely differing requirements in terms of capacity, timeliness and robustness of the data service.

Sufficient data bandwidth, in both fixed and wireless networks, shall be provided to support a wide variety of data applications required for emergency telecommunication purposes.

Ideally, the data transmission rate shall support the required data throughput and minimize end to end delay, especially for applications such as real time video. Noting the extreme circumstances which may be in force during an emergency, it may be desirable for networks to degrade gracefully when user requirements exceed the agreed levels of service.

Table 1 shows the diverse needs of data applications. Where data applications share the use of a data transmission capability, provision of sufficient capacity and effective management must be provided to ensure application data is communicated appropriately.

Table 1: Requirements on data applications

Service	Throughput	Timeliness	Need for preservation of data integrity
Email	Medium	Low	Low
Imaging	High	Low	Variable
Digital mapping/ Geographical information services	High	Variable	Variable
Location services	Low	High	High
Video (real time)	High	High	Low
Video (slow scan)	Medium	Low	Low
Data base access (remote)	Variable	Variable	High
Data base replication	High	Low	High
Personnel monitoring	Low	High	High

Throughput: data volume in a given time.

Timeliness: importance of the information arriving within an agreed timeframe.

Preservation of data integrity: how (reliable) free from biterrors the information transmission needs to be. E.g. a bitmap image with some errors is still useable, a jpg image with some bit errors may be unreadable.

Some applications may be used with dedicated communication assets which will be tuned to the particular needs of that application, although interfaces may be necessary to exchange data from such dedicated systems with other applications e.g. screen capture one frame from dedicated video transmission equipment and email the resulting still image. Where appropriate such applications should be based on appropriate standards to facilitate information exchange.

Specific applications are listed in the following clauses.

5.4.1 Paging Services

Paging services are used by a variety of authorities in order to contact their personnel, and paging services are available from a variety of networks and technologies. The network needs to be able to identify the requested authorized emergency agent(s), and then deploy the appropriate technology to contact them. This requirement may encompass different communication network technologies, services and applications such as paging, presence, texting, etc.

5.4.2 Status Monitoring and Location Services

Status monitoring includes a wide variety of parameters, e.g. breathing air tank levels, accountability monitoring, distress buttons and vital signs monitoring. Location services provide real-time information regarding the position of personnel or vehicles to a command point. This information may also include status information regarding the person or vehicle. The service may require frequent transmissions to update position; the amount of data transmitted is likely to be small when location is based on satellite-based solutions, but can be quite extensive when location is to be calculated inside buildings as other technologies may have to be used. Location reporting services may be one-way with no acknowledgement, necessitating a robust communication mechanism. Position information may be considered sensitive in some emergencies and may require security mechanisms to protect the data.

5.5 Interoperability of Communication Services

Voice communication services are generally possible across heterogeneous networks, although there may be loss of functionality where special services are available (see clause 5.4.1.2). Where different techniques are used for voice encoding there may be additional loss of intelligibility and quality due to the need to decode and re-encode the voice signals.

Data (used by applications in emergency scenarios may need to flow to multiple sources) needed in emergency situations may be used by multiple applications. Applications must therefore be able to communicate with one another and present data in a format which is useable by other applications.

EXAMPLE: Situational awareness applications may benefit from inputs from other systems e.g. aircraft movement, automatic vehicle location, maritime distress systems, etc.

A high level of interoperability between different systems and applications allows information to be communicated rapidly, widely and effectively to all relevant parties.

5.6 Example application

The application selected as an example application is the management of several field teams in an emergency situation requiring different expertises.

The needs are supposed to be limited to one specific area.

They can imply the following relations (see references in point 4):

- 4-1 (PSAP to ECC);
- 4-3 (coordination between different ECCs);

- 4-4 (ECCs with rescue teams); and
- 4-5 (between different rescue teams).

It may be necessary to have relations of 4-2 type (coordination with other PSAPs) pending on the size or the location of the event.

The type of actions required cover mainly:

- Mobilization of resources.
- Transmission of updated information on the status of the action.
- Pre-informing hospital services etc. of arriving casualties and their needs.
- Transmission of images from an incident to the emergency control centre.
- Real time combination of actions between the different teams.

The relations-actions matrix can be developed in order to explain what kind of services are to be provided through the communications system. Whereas 4-1, 4-2 and 4-3 type of relations may be handled through fixed lines, 4-4 and 4-5 services must be mobile and on a radio carrier system.

An example of the full analysis is given hereunder; the resulting matrix can be used in a procurement process as the basis for preparing the terms of reference of the required system. One important point is to provide interoperability between different teams. The obvious solution to have a unique platform will not always be available; teams are then under different systems. The connection will then go through switching and connecting arrangements between different systems; which in general reduces or forbids the VPN between all actors, losing advantages of an easy interconnection.

Table 2: Relations-Actions matrix (Illustrative)

Actions Relations	Mobilization of resources	Transmission of updated information - status	Pre-informing hospital services, etc.	Transmission of images to the ECC	Real time actions between different teams
Section 4-1	Yes	Yes	N/A	Yes	N/A
Section 4-2	Yes	Yes	N/A	N/A	N/A
Section 4-3	Yes	Yes	Yes	Yes	Yes
Section 4-4	Yes	Yes	N/A	Yes	Yes
Section 4-5	Yes	Yes	Yes	N/A	Yes

6 Scalability

Scalability is an important consideration especially when the communications system (networks in combination) handle the escalation from a case involving e.g. one ambulance and one ECC up to national authorities (regional control centres, ministries, municipal authorities as well as local services).

To fulfil this objective some descriptions may be useful:

- Contingency planning, see annex B.
- Organization of authorities in case of catastrophic event, see annex B.
- Emergency Preference schemes and traffic management.

6.1 Priority schemes and traffic management

The objective of rescuing injured or endangered people calls for arbitration of the emergency authority's representatives access and use of shared, scarce (scarce or privileged) resources. Such schemes can be permanently assigned or activated when the need arises in connection with the escalation of the disaster and a pre-organized contingency plan.

Additionally, in cases where the crisis event impacts a significant portion of the population, panic attributes that the demand for information may raise the traffic demand on the communication networks to a level where the integrity of the network itself is put at risk. See ITU-T Recommendation E.409 [2] for information on the nature and scales of network resilience security threats and events to be planned against.

Priorities for certain types of calls and access to data services should be described in a comprehensive scheme, that enable priority or essential traffic to be maintained at the risk of allowing other types of traffic to be degraded. Such schemes require contingencies to be described considering a break down for regional or localized eventualities. These plans also require the protection of all essential stakeholders in the planned contingency, including the involvement of public and political authorities, representatives or emergency services, operators and secondary support organizations.

The model of an emergency preference scheme should serve as guidelines for the purpose of the foreseen risk and may lead to the imposition of traffic management techniques by the network operators to ensure spare capacity is maintained to cater for the expected needs that may be foreseen for the continued support of essential and emergency services.

Professional radio communication networks are dedicated to emergency services and as such traffic is guaranteed to the users during the emergency.

6.1.1 Traffic Management

In general, an emergency situation will not directly affect the infrastructure and the performance of communications networks.

Nevertheless, situations may arise where either public networks, private networks, or both, are affected as part of the emergency.

In both cases, the additional bulk of traffic, caused by the crisis, can lead to congestions in the network. It then becomes a vital requirement that the network operator take measures to mitigate against the possible failure of their network. To obviate these consequences and to maintain the access to the network resources required by authorized representatives, in the exceptional time, the operators should be prepared to activate traffic management measures.

In general such measures, taken for the sake of the interest of emergency communications, will require the decision of the administrative authority, to mitigate the concerns of users who lose access rights, and to nominate those whose traffic involved in the emergency situation is subject to protection.

However, measures to protect the integrity of the network may under normal times of exceptional load be employed by the operators on a purely statistical basis. On such occasions, handling of Emergency Services Calls may be protected against loss.

By definition a private radio communication network designed for use in emergencies shall be dimensioned to handle the emergency team's high traffic particularly in a small area. It shall be possible to dynamically configure the traffic management for the emergency location.

6.1.2 Emergency Preference schemes

A public Safety user always wants to be able to establish communications instantly and at all times. Because of limited physical resources (number of trunks, lines, radio channels, etc.) communication networks can become overloaded in emergency situations. The reason why most communications networks have limited physical resources is because the additional cost to increase the size of communications networks to adequately handle abnormal traffic loads in emergencies cannot be justified. As a consequence, compromise solutions are needed.

EXAMPLE: Adaptive traffic management and emergency preference schemes.

Some examples of these user driven solutions for fixed and mobile, public and private, communication networks are:

NOTE: This may be used for private network/systems.

PSTN/Cellular solutions

An example of a network access based call preference scheme has two levels of control:

- 1) a basic national end-to-end call set-up protection of priority network accesses from restrictive transport and termination controls; and a further
- 2) more severe regional protection of priority network accesses from restrictive originating network controls.

The basic functional requirement is for a preference scheme available, but not invoked, on all fixed network accesses to provide an enhanced probability of achieving successful completion of the call attempt to the termination across all networks, for nominated network accesses of essential users. Normal call unsuccessful conditions permitting (busy, No answer, etc.) the requirement is for the protection of the call set-up and call delivery to the point of termination. This capability is required to be available nationally, across all networks on a licensed equitable basis.

The state of network access based call preference scheme is always available, but under normal conditions not activated. Once activated, the registered network accesses of nominated essential users will automatically invoke the enhanced network access based call preference scheme whenever a call is placed. Network management controls are required for activating and deactivating the service and registering the network accesses of nominated essential users.

The more severe form of control protection of priority network accesses from restrictive originating network controls would be introduced only within parts of the network that are severely affected. This geographic form of control would be applied as a network protection and severe form of a network traffic management measure. However the case of network failure/disaster cannot be foreseen and clearly may not affect other networks. See ITU-T Recommendation E.409 [2] for information on the nature and scales of network resilience security threats and events to be planned against.

The escalation from an activation of the basic enhanced network access based call preference scheme to the more severe localized level of the service will also require network management controls. A procedure will be required for local escalation and de-escalation of the network traffic management measure.

NOTE: The network access based call preference scheme provides priority service to the essential users nominated network access(es), it is not provided personally to the user themselves, as this adds immediate complexities.

Additionally, a user based call preference scheme has two features:

- 1) a protected priority access code; and
- 2) a user based validation platform.

The protected priority access code employs similar features to the protection priority of e112 access (Directive 2002/22/EC [11] on universal service and user's rights relating to electronic communications networks and services) and the network access base call preference scheme. Subsequent user request being validated and authenticated the terminating leg of the call set up may also employ the protection afforded to the network access base call preference scheme.

See International Emergency Preference Scheme ITU-T Recommendation E.106 [6] and interworking with national schemes.

Professional radio communication systems which are dedicated to emergency services shall be dimensioned to handle the peak of traffic exclusively for them. Yet priority call shall be available to allow authorized users to intervene when needed.

Professional Mobile Radio (PMR) Networks

To balance the needs(ed) between acceptable cost, available traffic capacity and an acceptable grade of service (GoS) in emergencies, a number of services and facilities have evolved on PMR networks designed specifically for public safety applications. Although these services and facilities are in effect the solutions used to optimize a network's performance in emergencies, the names for these solutions have been adopted by the industry and often specified as user requirements.

- call queuing when busy;
- dynamic traffic management algorithms;

- group call (commonly called "all in formed net" and "talk group call");
- pre-emptive priority call (Emergency Services Call);
- call retention;
- priority call;
- Direct Mode Operation (DMO);
- Dynamic Group Number Assignment (DGNA);
- ambience listening;
- call authorized by dispatcher;
- area selection;
- late entry;
- voice encryption.

Call queuing when busy

To prevent unnecessary user frustration when a network is busy, call queuing is provided in "First In First Out" (FIFO) and/or access priority order. This means that users trying to gain access to the network are informed that the network is busy, and then they are automatically called back when they get to the top of the queue and their called party connection is being initiated.

Dynamic traffic management algorithms

To optimize GoS and capacity during busy periods a dynamic means of managing different types of calls are required. For example, the use of dynamic call duration timers with "time out timer" warnings on "one to one" calls, preferred site operation for group calls, restricting wide area group calls to base station sites where the majority of group members are registered and/or allowing wide area group calls to proceed only on sites at which preferred users in the group are registered.

Group call

- Use simple "push to talk" operation to provide fast call set-up group communications.
- Be operated and managed in particular ways to optimize network loading, some examples being:
 - Simplex operation.
 - Preferred site operation.
 - Area selection.
- Have a very reliable call-set up signalling protocol to ensure all users in a group are connected together when a call is first initiated (call acknowledgment signalling is impractical for group calls).
- Have priority mechanisms to ensure that specified users in a wide area group call (spanning multiple base station sites) are connected together when a network is busy.

Pre-emptive priority call

This call service, commonly known as Emergency Services Call, provides the highest uplink priority and highest priority access to network resources. If a network is busy, the lowest priority communication is dropped to handle the Emergency Services Call. Unlike 911, 112 or 999 initiated public network emergency calls, a PMR Emergency Services Call can be initiated by using a dedicated switch located on the terminal. Activating the Emergency Services Call automatically alerts the affiliated control room dispatcher and other terminal users in that persons talk group.

Call retention

This service protects selected radio terminal users from being forced off the network as a result of pre-emptive calls (Emergency Services Calls) during busy periods. When Emergency Services Calls are supported in a network, it is essential that only a small amount of radio terminal users are provided with this facility as the objective of retaining important calls during busy periods could be lost.

Priority call

During network busy periods, that service allows access to network resources in order of user terminals call priority status. As there are multiple levels of priority, this service is very useful in providing different Grade of Service (GoS) levels (and tariff structures) during busy periods.

EXAMPLE: Front line officers would be provided with the highest priority levels in a public safety network to maintain the highest level of service access whilst routine users would be provided with lower priority levels.

Direct Mode Operation (DMO)

DMO provides the ability for radio terminals to communicate directly with each independent of the fixed network infrastructure. DMO is not new and has been a facility mandated and used by many traditional PMR user organizations for several decades. The primary requirement for DMO has been brought about by the need to balance the RF Coverage, GoS and reliability of a network with that of the network's overall cost.

Dynamic Group Number Assignment (DGNA)

This service allows the creation of unique groups of users to handle different communication needs and may also be used to group participants in an ongoing call. This service is considered by many public safety organizations to be extremely useful in setting up a common talk group for incident communications.

EXAMPLE: selected users from the police, fire and ambulance could be brought together to manage a major emergency where close co-ordination between the three emergency services is required.

Similarly, DGNA is also considered useful for managing incidents by other user organizations such as utilities and transportation.

Ambience listening

A dispatcher may place a radio terminal into ambience listening mode without any indication being provided to the radio terminal user. This remote controlled action allows the dispatcher to listen to background noises and conversations within range of the radio terminal's microphone. This is an important service to utilize for those persons transporting important, valuable and/or sensitive material that could be "high jack" targets. Similarly, this is a useful service to have implemented in public service vehicles where a driver's health and safety could be at risk.

The number of user applications for the ambience listening service are numerous and in many cases application specific. However, it is important to note that many users feel that this service invades a person's privacy and for this reason only those users who need ambience listening as part of their work duties should be provided with this service.

Call authorized by dispatcher

Dispatcher verifies call requests before calls are allowed to proceed. This is a useful service to utilize when radio user discipline needs to be maintained. This service also reduces the amount of radio traffic on a network as only essential work related calls are permitted. However, the frequent need for all informed net group communications between terminal users and time delay experienced in authorizing calls can make this service unacceptable for some user organizations.

Area selection

Areas can be chosen on a "call by call" basis. This service basically simulates the ability for a dispatcher to select different base stations to make a call as was possible in conventional networks. This service also helps to improve network loading and overall spectrum efficiency by restricting the area of operation for selected all informed net group calls.

Late entry

This service provides continuous call in progress updates on trunked radio network control channels to allow latecomers to join a communication channel. This is not a service but an air interface feature that allows a trunked radio terminal to behave similar to conventional PMR terminals.

EXAMPLE 1: If a user turns on their terminal the control channel will automatically divert the user's terminal to a talk group call, if a call is already in progress.

Similarly, if the user's terminal has been outside radio coverage.

EXAMPLE 2: In a tunnel, the control channel will also divert the user's terminal to a talk group call assuming a call is already in progress.

Voice encryption

To prevent eavesdropping by unauthorized users, PMR technologies used by public safety organizations require high levels of voice encryption with multiple keys and over the air re-keying. Also, these wireless technologies also need to support "end to end" encryption using a variety of encryption algorithms as deemed necessary by national security organizations.

6.1.2.1 Interaction with the Emergency Call service e112

Once the severe category of this enhanced network access based call preference scheme has been activated, all network accesses should still provide access to emergency services e112. The network access based call preference scheme will allow essential and non-essential users the ability to make e112 calls and to access whatever parts of the network are still available.

The nominated network accesses of essential users will not get access to reserved resources, e.g. trunk reservation, as is the case of the emergency services themselves. This implies no additional network management overhead. Therefore, within the network access based call preference scheme network accesses will get a priority service handled similarly to the Emergency Services e112, without access to reserved resources, but with the ability to terminate to any termination.

NOTE: The level of priority could therefore be seen as lower than that of the essential emergency services e112 themselves.

7 Requirements applicable to the Network(s) and user services, (services to support) and the network features and capabilities

7.1 Recognition and treatment of emergency services from the view of the service

7.1.1 Transmission quality

Apart from defining an appropriate minimum bandwidth that is needed to provide a specific emergency service, one of the most crucial problems that have to be solved is assuring a sufficient transmission quality. Depending on which communication channels are used and which services have to be provided, the requirements will vary widely between different systems.

Some of the most important quality parameters for connectivity and their significance for different communication services are discussed in the following.

High availability and reliability are desirable for any kind of connection (but are especially important for applications where the stability of the connection is crucial, such as continuous cardiac monitoring for rescue workers). In any case the restoration time (i.e. the time needed to restore the required QoS after a service disruption) of the connection should be kept as short as possible.

Though a low error rate is always desirable, for transmission of speech or data that is highly redundant or can be interpolated (like video streaming) the acceptable error rate can be considerably higher than for more sensitive data. However for applications like cardiac monitoring a very low error rate must be guaranteed.

The time it takes to get information across a network (latency) is a parameter that is relevant to nearly all applications that use network connections as high latency implies that the user will have to wait for the application to react to his actions. Voice calls may be considered special, as the latency itself is annoying but not necessarily a crucial problem. Human actors are fault tolerant and can deal with a certain degree of delay. However the variation of latency for transmitted data packets (jitter) is particularly disruptive for voice calls as well as for other real-time applications like video monitoring as it will disturb the transmission of the data stream.

The dropping of data (packet loss) might cause a temporary failure of the transmission. Compared to data traffic, video streaming and voice traffic are quite robust to loss ratio. However in data-oriented traffic (e.g. network connections using TCP/IP) the fact that some data packets did not reach their destination might cause the protocol to terminate the connection.

For speech transmission in emergency situations there is often a trade-off between connectivity and call quality (that can be measured e.g. through the Call Quality Index (CQI) proposed in ITU-T). Connectivity is often the more important factor as long as a certain minimum (baseline) call quality is provided.

EXAMPLE: Whenever a lot of users are trying to make voice calls in parallel (which is most likely in case of an emergency), it will be more preferable to enable most of them to make calls below the baseline quality normally offered to them than to give high quality connections to a few of them while shutting out the others.

Human actors can deal with low quality speech e.g. by repeating their messages whenever they notice that the connection quality gets to poor.

For critical transmission channels asking for best-effort services is definitely not enough. Especially real-time applications like video-streaming or voice over IP will need a minimum QoS to be fully functional. For every communication service used by the authorities, it will be necessary to define a minimum transmission quality for speech and/or data that has to be available to ensure that the service can be provided properly.

NOTE: This may be used for private network/systems.

7.1.2 Ensuring conveyance of communications

Network operators shall make every reasonable effort to ensure the answering, inter-network forwarding and termination of inter-authority calls, including in exceptional circumstances such as crises, catastrophes, etc. See ITU-T Recommendation E.409 [2] for information on the nature and scales of network resilience security threats and events to be planned against.

Network operators should assign privileges to traffic according to decisions from proper authorities.

Networks should have the capability to handle prioritized calls correctly, including the capability of pre-emption of unprioritized calls. Transit networks should convey priority related signalling in order to support end-to-end priority.

7.1.3 Assignment of inter-authority calls to the appropriate authority

A fleetmap structure makes it possible for different groups of personnel to access department specific and common group structures.

Common groups across different authorities should be available to improve interactions in common operations.

Common groups should be able to include users from different networks, in order to facilitate both cross border operations and country specific operations.

All users shall be able to communicate with their respective ECCs and with each other. The ECCs should communicate with all users regardless of their position within the network by means of:

- Group calls.
- Individual calls.
- All kinds of mode of voice and data communication.
- Simultaneous voice and data.

Users from other departments and authorities should be able to access specific groups based on case-by-case admission authorized by the respective emergency centre. It should be possible to define groups limited to a geographic area.

The authority should be able to create and use dynamic groups, e.g. by "drag and drop" users in to the dynamic group and to distribute this information to selected users.

7.1.4 Preventing effects of discrepancies in coverage

7.1.4.1 PSAP routing in mobile networks

Due to physical uncertainty and variations of radio coverage limits there are border effects where an Emergency Services Call is routed to the wrong PSAP. Attention should be given to all parties involved, and more specifically operators, when designing the network to limit the occurrence of such cases. Where these cases occur, cooperation of PSAPs/ECCs should be applied and organized as appropriate.

7.1.4.2 International cooperation

A situation similar to that described in clause 7.1.4.1 may appear near country borders: Cross-border Emergency Services Call handling requires international cooperation between all involved parties.

7.1.4.3 Cordless technologies

Situation similar to those described in clauses 7.1.4.1 and 7.1.4.2 may be applicable as well to cordless technologies that use fixed-line networks.

7.1.4.4 Interworking of Technologies

Different authorities and organizations may rely on different communication technologies for their field actions (e.g. analogue PMR, TETRA, Tetrapol, GSM-R and VHF Maritime frequencies). Attention should be given to ensure proper communication between such systems not restricting the efficient cooperation between field personnel and the emergency centre in charge.

7.2 Recognition and treatment of emergency services by the originating network

If a virtual net is established for emergency work, with subscribers in different networks, this may be an issue for consideration.

7.2.1 Call-related information

Information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Also, call related information originated by an authority representative shall be transmitted on inter authority communications.

7.2.1.1 Indication of the (emergency) caller's location

Location information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Also, call related location information originated by an authority representative shall be transmitted on inter-authority communications.

7.2.1.2 Identification of the mobile terminal equipment/subscription

Mobile terminal equipment/subscription identity information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Also, call related mobile terminal equipment identity information originated by an authority representative shall be transmitted on inter authority communications.

7.2.1.3 Interworking of Technologies

Call related data originated by any authority representative shall be transmitted on inter authority communications independent of the use of differing technologies, e.g. location information.

7.2.2 Network identification

Network identification information from the Emergency Services Call shall be forwarded along with the Emergency Services Call to any authority representative. Also, network identification information originated by an authority representative shall be transmitted on inter-authority communications.

7.2.3 Minimum power supply for authority representative user accesses

If feasible, fixed network operators should provide a minimum power supply at their network termination points. This minimum power supply should enable telephone terminal equipment connected to the network termination point to be operational in the case of a local power failure.

NOTE: Emergency authorities are expected to have their own policies for guaranteeing electricity supply for terminals, generators battery back-up, etc.

7.3 Requirements on call handling between networks

7.3.1 Handling of inter-Authority calls between networks

Handling of inter-authority calls between networks shall be conveyed with the associated call priority information to alleviate the call from restrictive network management controls, as specified in clause 6.

7.3.2 Interworking with carrier selection/carrier preselection codes

Interworking with carrier selection/carrier preselection codes needs to be considered as authorities may chose to change supplier, but shall work in the normal way.

NOTE: ITU-T Recommendation E.106 [6] Carrier selection may be overridden for international preference schemes.

7.3.3 Inter-Authority communications from other countries

International assistance treaties commonly exist across local borders land/sea, e.g. France/Switzerland in the area around Geneva, UK/France in the Channel, UK/Norway in the North Sea, etc.

Call handling between international networks shall have the following functionalities:

- Integration into foreign talk groups.
- Contact with own dispatching unit (ECC).
- Emergency Services Call handling in foreign networks.
- Data transmitting for status messages and automatic vehicle location.
- Individual call and phone call.

For call handling from other countries the network must provide the following services:

- The display on the handset has to show the active network.
- Selection of the preferential network.
- Identification of group members.
- Use of DMO (direct mode operation).

NOTE: For call handling between Tetra and Tetrapol networks, the Helsinki report (ETSI/GA32(99) 04) provides different solutions.

7.4 Providing termination of Inter-Authority calls for the relevant authorities

Any network to which the points of access to authorities are directly connected should deliver the Emergency Services Call to the authority together with any related data, without undue delay or modification.

If the appropriate authority is not reachable, the call must be forwarded to the alternative nominated authority.

Terminating networks to authorities should, if possible, meet the functional requirements as agreed, to ensure the continuity of the access to the authority, call diversion deflection, load balancing, etc.

The network operator will be expected to protect the integrity and ensure the survivability of their network, according to nationally agreed objectives. This may be achieved by employing no single point of failure within their network equipment. See ITU-T Recommendation E.409 [2] for information on the nature and scales of network resilience security threats and events to be planned against.

It is also required, where possible and agreed in the service level agreement, to guarantee that the access required by nominated authorities can have an enhanced survivability in the case of load or disaster. This may be achieved by employing no single point of failure.

7.5 Network Management support functions for delivery of Inter-authority calls

7.5.1 Priority of inter-authority emergency communication

Inter-authority calls should be afforded preference status as nominated for their use in a call preference scheme in times of disaster. This preference should be accorded across public telecommunications networks.

7.5.2 Monitoring of the lines and availability of the Authority

Transmission lines over which emergency telephone services are connected should be available without restriction. The terminating network permanently monitor the functionality and transmission quality of the transmission lines. Technical modifications and maintenance should not impair emergency telephone lines to the authority. If the quality falls below a minimum threshold the network and authority should deactivate the access and check the availability and quality of the connection. Any such deactivation should not affect any call in progress.

7.5.3 Diversion of Inter-Authority calls

If a network access to an authority is deactivated or out of order the network must be able to divert incoming Emergency Services Calls to back-up/alternate equipment, lines, network access, if required by the authority. The authority shall inform the network operator on requested reconfigurations.

7.5.4 High or Resilient availability

Subject to the nationally agreed service level agreements, network operators should use network management measures to ensure the termination of inter-authority calls.

7.5.5 Security provisions at the access to authorities

The network operator should make reasonable provisions to mitigate against the impact of attack, either deliberate or accidental, to the access and core networks to which authorities are connected.

8 Security

8.1 Role of National Communication Security Authorities

For many governmental organizations including public safety, responsibility for communication security lies with a national communication security authority. Any mechanisms employed in communication systems used by such organizations shall meet the specific requirements laid down by such national authorities. International coordination exists between many NCSAs, embodied in the Common Criteria ISO/IEC 15408 [4] and the ITSEC arrangements which are accepted by most national governments within Europe and the European Commission.

Users, equipment manufacturers and service providers are advised to contact the relevant national authorities in order to establish the relevant security requirements for particular communication services.

8.2 General Security Issues

For all emergency communication, the organizations involved have to make sure that data is protected according to its sensitivity level during transmission, processing and storage and that access to communication channels and critical systems is only granted to authorized persons. In the context of emergency communication several security requirements have to be discussed:

- Confidentiality of data: Whenever confidential data is transmitted it is necessary for each party involved that they can rely on the fact that no eavesdropper gets hold of it. According to the degree of its confidentiality the data must be transmitted via secure channels and protected by encryption during transmission and storage.
- Protection of signalling information, to prevent denial of service attacks or traffic analysis.
- Authentication of persons or devices: All persons (and devices, if necessary) involved in critical communication shall be provided with means to authenticate themselves. It should be possible for them to do so without having to trust or even know each other, especially in scenarios where ad-hoc communication has to be provided to parties that can not communicate via secure channels established in advance.
- Authorization: Access to confidential information and critical systems is restricted to persons with appropriate entitlement.
- Integrity of data: Each of the parties has to be able to control if the data they get is complete and correct and if it was changed during transmission.
- Non-repudiation: None of the parties involved in the communication should be able to subsequently deny that they took part in the information exchange and the commitments they made during the communication.
- Logging: Records of communications should be available to protect users. This information may also assist with subsequent assessment of the emergency.

Many public safety services already possess some degree of security to prevent eavesdropping and denial of service. Some systems will not operate without security mechanisms being in place. However, it is essential that in an emergency appropriate security mechanisms will be supported without detracting from the usability.

8.3 Interconnection of secure communication systems

As communication systems employed by many public safety organizations operate in conformance with security requirements issued by NCSAs there may be significant difficulties in supporting interoperability between systems. Ad-hoc solutions to these problems are generally unsatisfactory and result either in a loss of security as all users fall back to operating in non-secure mode, or in the loss of all but basic services as interconnection is proved only through "red gateways" or "swivel chair interoperability" (where a single user is provided with terminals for multiple systems).

Significant pre-planning and co-ordination of security solutions is necessary in order to support interoperable secure voice and data services between different user communities and across different networks.

These requirements can be fulfilled with a variety of security mechanisms which are described in annex C.

Annex A (normative): Basic Architecture

Figure A.1 represents the basic architecture and the interfaces between authorities where the Rx are the numbered reference points for identification and showing the interfaces.

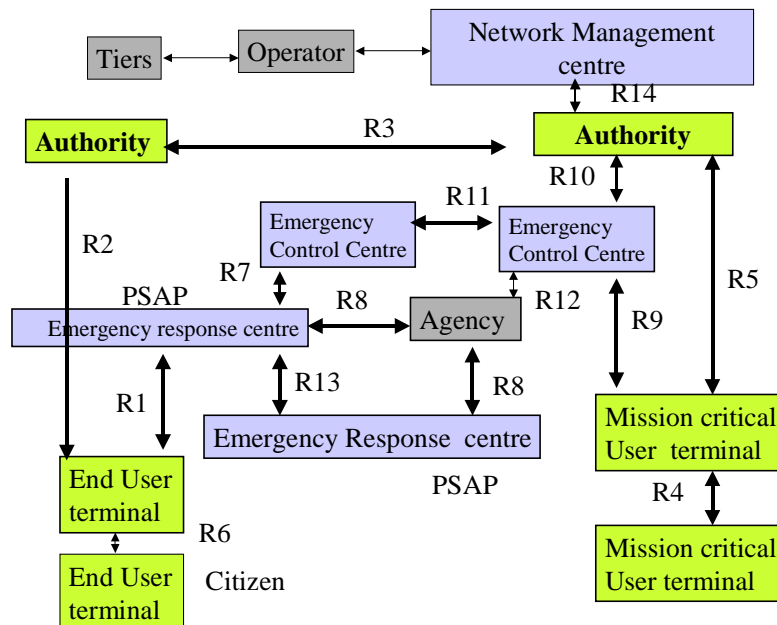


Figure A.1: Basic Architecture (Citizen to be replaced with Individual)

Annex B (informative): Organizational related issues for Authorities to Solve

Telecommunications systems or operator services cannot cover all emergency communication needs. In the present document attention of public authorities are drawn to some situations where a fair level of performance can only be reached if organizational decisions are taken by the authorities themselves.

B.1 Handling of foreign languages

In the case of communications between authorities, and compared to the case of receiving the emergency calls, the problem may be simpler (often between neighbouring countries and a good probability to have on both sides bilingual people). But in general, the solution cannot rely on a statistical hypothesis and requires a minimum training of staff and specific agreed procedures or definition of contacts points for example.

B.2 Mitigating consequences of radio coverage discrepancies

One possible consequence is that some calls may arrive on a wrong destination (presumably in a neighbouring area). Staff in this situation must be informed and know how to act to transfer the call or answer to the caller, without delay.

B.3 Definition of priorities (list of beneficiaries, levels, conditions of effective implementation)

The policy in priorities is clearly a political issue. It can be expressed through lists or plans. For a given area, the preparation of such plans should be made in a collaborative way with the operators and users (rescue services), initiated and coordinated by the concerned administrative authority. An International Emergency Preference Scheme (IEPS) is defined in the ITU-T Recommendation E.106 [6].

B.4 Contingency planning

The entities and relations special task force, temporary headquarters and administrative entities or secondary response organizations will be mobilized in disaster situations as soon as the events have reached a predefined level of importance.

This may not be just a question of the regional coverage or a disaster event or of number of casualties, but the need to call on other organizations to perform secondary tasks (e.g. cut the water or gas supply to avoid a risk in the vicinity of an accident with specific conditions); some of the situations require only a normal means of communicating between the emergency control centres and corresponding technical operation centres.

It is, however, clear that all authority representatives must be ready to face dramatic events, where the normal PSAP/ECC will be overloaded with calls and tasks to prioritize.

The prerequisite for facing this sort of situation relies in the hand of the national or local authorities who have the power and the responsibility for fixing the frame of adequate plans, obtain or impose agreement from all authority representatives and making available some needed contingency resources. Also, they will often take the decision of declaring a crisis status, condition for activating the exceptional plan.

The cases where ECCs need to invoke a contingency plan are dependant on a lot of factors, for example: the need for extra resources, simultaneous actions of various disciplines (fire and medical, road traffic, fire, etc.), general organization, geographical distribution of resources, etc.

As a result relations between authorities, and their need for communications can be based on a regular and daily routine, but may be required to escalate to cater for exceptional cases, and specially faced to dramatic events.

In the case of dramatic events, it is advisable to have plans pre-defined in order to be activated on request of one of the ECCs or on demand on an administrative body (e.g. Le préfet in France). In general the plan will include several actors outside the ECCs themselves (private companies of ambulances, private doctors, technical services of companies operating facility services, etc.).

Such plans may consist of:

- lists of designated contacts and their co-ordinates;
- basic organization scheme;
- priority schemes (categories of priority, list of people authorized according to each category);
- procedures for requesting the activation of priorities towards the telecom operator (s);
- procedures for updating and change of the previous info;
- procedures for cancellation of the exceptional situation, end of the plan and return to normal.

B.5 Organization of authorities in case of catastrophic event

Most countries have a concept of levels of authority and assistance that can be called on in major catastrophes. In normal emergencies the primary authorities and organizations can be relied upon to react to the situation. In more serious emergencies three general effects take place. First mobile ECCs are created. This enables the resources of the primary authorities to be concentrated and managed closer to the disaster. The second effect is the escalation toward greater administrative control. In which case contingency plans exist for the local/regional/central government to provide resources, evacuation, planning of transport, food etc. Thirdly, secondary assistance can be called on where commercial organizations that provide essential services are called on under special legal conditions to restore water, electricity, repair roads, communications, etc.

The definitions of the primary authorities, The emergency responsibilities of political authorities, the legal mandates on secondary organizations in an emergency situation vary between countries. But the general concepts remain true. These differences are not the aim of the present document.

The communications needs for the escalation is paramount to the present document. The provisions of communications to primary authorities need to be considered in the context of the need where an emergency can rapidly escalate and a rescue team and/or ECC is required. In these cases a mobile ECC is a means of concentrating resource hence it may be seen as subsidiary to a fixed ECC. A mobile ECC has greater communication needs than a normal response unit.

EXAMPLE: A mobile hospital may have needs for video relay of consulting to other hospitals for advice on treatment, operations, radiology, etc.

The requirement for guaranteed QoS data services is therefore much greater in this context. Communications for emergency services shall be scalable in terms of numbers of users and bandwidth.

The communication needs for mobile emergency unit and/or control centres are:

- Guaranteed QoS data services.
- Priority access to other peer level and supply organizations.
- Ability to call on recognized experts (doctors, midwives, chemical experts, etc.) and equip them with intuitive communications.

The communication needs for local/regional/central government control and planning during disasters are:

- Priority access to other governmental, primary, secondary and supply organizations.
- International communication for cross-border assistance, e.g. a ship sunk in a common international sea-lane.

The communication needs for secondary assistance organizations that provide essential services are:

- Priority access to governmental, primary, other secondary and supply organizations.
- Access to the emergency communications features of the primary authorities during the repair/crisis.

In addition, the following communication needs may also be present:

- International communication for cross-border assistance.
- Temporary authorization as an authorized emergency organization, electronic authorization.
- Compatible communications equipment and personnel when called on to assist across national borders, e.g. authorized UK electricians assisting the repair of the French electricity network after a hurricane.

B.6 Communication between civil authorities and non-governmental organizations

NGOs are frequently closely involved in the response to emergencies. While this involvement may not take place in the hours immediately after an incident, they may form a vital part of the response to an incident. It is essential to coordinate with NGOs, both for protection of NGO staff and for effective liaison and sharing of information between NGO and authorities.

B.7 Communication between civil authorities and press organizations

Emergencies are news. Although this is not a high priority, communications support to emergencies should plan to support some degree of communications with the press organizations. Procedures should be in place to ensure that the channel used to press organizations involves checks on the releasability of information.

Annex C (informative): Security mechanisms

The following techniques may be utilized in order to provide security features described in clause 8.2.

C.1 Symmetric encryption schemes

Two parties A and B agree on a secret encryption key either during a personal meeting or by communication on a secure channel. A message one of the parties encrypted using this secret key can only be decrypted by the second party. If their secret key is compromised, A and B must agree on a new key. Symmetric encryption schemes run much faster than asymmetric schemes but they do not allow spontaneous interaction between parties who do not know each other. Another restriction that occurs with symmetric encryption is key management, as every pair of participants in the scheme has to find a way to agree on different keys and store all those keys safely.

It is a common characteristic of emergency communications that typical communication channels for standard situations will be known prior to the real emergency case, so secret keys can be exchanged before an emergency occurs. Thus symmetric encryption is the preferable method, especially for real-time communication such as voice calls that would suffer from any decrease in performance.

C.2 Asymmetric encryption schemes

Party A chooses a pair consisting of a private key it keeps secret and a public key it publishes for everyone to know, for example in some public directory on the internet. It is not possible for anyone to compute A's private key from the public key. If Party B wants to encrypt a message to A, it gets the public key and does so. Nobody but A (who knows the private key) can decrypt this message. Every participant in the scheme needs only one pair of keys. The key management, however, has some difficulties and requires some kind of public key infrastructure. To link a key to its identity, Party A has to have the key signed by a certification authority. Anyone who trusts this authority can check the signature by using the authority's public key that is generally known. Problems can occur, if there is no third party that A and B both trust. Asymmetric encryption schemes allow spontaneous secure communication between strangers as everyone, who wants to send a message to A, can get the appropriate public key and use it for encryption. A disadvantage of the publishing of the key occurs when A's private key is lost or compromised and has to be changed. A cannot know for sure who got the old public key and warn these persons, not to use it anymore. All A can do is publish the key on a revocation list and hope that B will look into it before encrypting a message with the compromised key. It will be necessary to use asymmetric encryption if non-standard situations occur during the escalation of an emergency, e.g. if parties from different countries have to exchange information without having had the chance to establish secure communication channels in advance.

C.3 Hybrid encryption schemes

To enjoy both the benefits of symmetric encryption (e.g. better performance) and those of asymmetric encryption (e.g. spontaneous confidential communication between parties that have not had the chance to agree on a shared secret key prior to their communication) a hybrid scheme could be used. This means that the involved parties use asymmetric encryption to agree upon or exchange secret keys in a setup phase of the communication after which they will be able to continue their information exchange using symmetric encryption.

Hybrid schemes will be helpful in situations that require spontaneous information interchange as well as excellent performance and where asymmetric schemes would have to be used otherwise.

C.4 Digital signatures

Party A signs a message by creating a hash value of it, to which it applies an asymmetric encryption algorithm involving its private key afterwards. The result of this process is a digital signature of the message that A can send to B or publish along with the original data. Everyone can use A's public key to verify both that the signature is valid i.e. that the message was really signed by A and that the content of the message has not been altered after the signature has been made. In addition A cannot repudiate the message afterwards, as a valid signature can only be created with A's private key. Thus digital signatures are a means to ensure non-repudiation as well as sender integrity and data integrity.

C.5 Authentication methods

Depending on the criticality and sensitivity of the concerned data and communication, various means of authentication could be used. The simplest method providing a basic security level is having the users identify themselves with a username and password. For stronger authentication one-time passwords or certificates stored in software or on smartcards are the preferable means of authentication. The use of digital certificates issued by trusted organizations also provides the advantage of spontaneous authentication between parties that have not been in contact before.

C.6 Authorization schemes

For all critical systems and resources as well as for all sensitive data there should be strict rules defined as to who is allowed to use, change and delete them. This ensures that only authorized entities can log into the system and only work with the data and use the resources they have been explicitly allowed to access. The most efficient way to handle authorization is to assign access rights to the role a group of persons are playing in the organization rather than to the persons themselves. This makes the management of rights easier and allows a quick replacement of people in case of illness, vacation or termination of the work contract of a role bearer. Every role should only be assigned only the minimum rights that are needed to fulfil its tasks. Accounts should not be shared between several people so it will be possible to identify who exactly is responsible for which actions.

C.7 Logging

Logging mechanisms do not prevent attacks or access to data without permission, but do at least store these events. Thus it is possible to identify attacks or attempts of attacks (and hopefully stop them before too much harm is done) and use this information to prevent further disruption of the system.

C.8 Virtual Private Networks

A VPN can be used to facilitate joint or co-operative actions; this may be deployed on a permanent basis between entities acting within a common area, specially if there are not collocated.

However a VPN may be required for temporary situations where an ad hoc co-ordination levels may have been created, e.g. Between PSAPs, and emergency control centres a permanent VPN can be established to facilitate the relationship. A temporary VPN may be established between emergency control centres and a mobile co-ordination centre of an emergency, this may then be extended to individual emergency service personal.

VPNs provide services such as closed user group, on-net/off-net, on-net authentication, on-net encryption, on-net priority and pre-emption, authorization to intrude/pre-empt, authorization to not be able to intrude/pre-empt, place priority calls on-net/off-net. Secured long tail access, service integrity, secure data services, encrypted data services, high integrity data services, etc.

Annex D (informative): United Kingdom Interoperability Agreement between Chief Fire Officers Association, Ambulance Services Association, and The Assistant Chief Police Officers Association

1 Responding to Catastrophic Incidents

- 1.1 The existing joint policies and practices of the emergency services to major incidents remain the foundation upon which to review our responses to catastrophic incidents and to incidents involving the release of Chemical, Biological, Radiological or Nuclear (CBRN) agents.
- 1.2 The emergency services are still assessing the lessons for the UK from the events in New York on 11 September 2001. However, with regard to communications at such incidents, two lessons are clear:
 - (1) in principle, there is a need for emergency services and their control rooms to be able to inter-communicate irrespective of the organizational boundaries and location within Great Britain;
 - (2) those communications to be resilient.

2 Responding to CBRN Incidents

- 2.1 Planning for CBRN incidents must include mutual aid for all but the smallest.
- 2.2 The current strategy is to disperse equipment, decontamination facilities and the specialist drugs/instruments for use by paramedics throughout the UK to provide for an immediate local response that will be supplemented by mutual aid. It is therefore a key element of this strategy that aid from different parts of the country can arrive exactly where required and can directly communicate their arrival and receive their instructions from the Incident Commander (Silver) of their service.
- 2.3 This will be possible only if each emergency service has an interoperable communications system.

3 Communications between Control Rooms

- 3.1 It is assumed that effective voice (and where appropriate, data) communications already exist between the control rooms of the primary emergency services in an area and between the control rooms of one of the services and the control rooms of that same service that surround it.
- 3.2 These need to be enhanced to ensure that voice communications can be maintained irrespective of a failure of the Public Switched Telephone Network and any associated private circuit.
- 3.3 They also need to be enhanced to ensure that control rooms of an emergency service can communicate by voice with any other control room of that service irrespective of its location in Great Britain, where necessary, independently of the public switched telephone network and any associated private circuit.

4 Command and Control at Major Incidents

- 4.1 Voice communications between the Incident/Silver Commanders of the primary emergency services at a major incident is a long-established principle and represents the basic minimum requirement for interoperability.
- 4.2 The main lessons from 11 September is to ensure that organizational boundaries or differing technical solutions to the provision of wide-area radio systems do not impair operational communications and build resilience into planning.
- 4.3 The importance of *multi-service* interoperability at the incident/silver command level will increase in the event of failure of the systems providing wide-area communications to one or more of the primary emergency services.

5 The Agreed Requirement

5.1 For the purposes of this agreement:

Directly	<p>Means that communication can take place using the wide-area radio system of that service, save where a control room is involved in the communications, without the need to involve any control room. For <i>multi-service</i> interoperability it includes the radio systems of the services involved and any gateways necessary to provide that interoperability.</p> <p>This agreement does not require the primary emergency services to use a common wide-area radio system, but where they do not do so, any interfaces, gateways and links between systems that facilitate <i>multi-service</i> interoperability must be resilient to failures of power supplies, equipment and connecting links between systems.</p> <p>Connexion for both types of interoperability need to be quick and effective (it should ideally be less than the total of the maximum specified connexion times of the wide-area radio systems involved, plus 10 %).</p> <p>Connexion and communication should be transparent to users and should support real-time duplex voice communication as a minimum.</p>
Mobile resource	<p>Means any operational vehicle equipped with a radio capable of accessing the wide-area radio scheme.</p>
Great Britain	<p>Means the landmass of England, Scotland and Wales (including inhabited islands).</p>

5.2 For *same-service* interoperability, the requirement is:

- (1) That the mobile resources of each primary emergency service, wherever located in Great Britain, shall be able to communicate directly with all other mobile resources of that emergency service and every control room of that service irrespective of organizational boundaries.
- (2) That every control room of that service shall be able to communicate directly by voice with any mobile resource of that service, wherever located in Great Britain and with every other control room of that service.

5.3 For *multi-service* interoperability, the requirement is:

- (1) That the incident command (or silver) of each primary emergency service at an incident shall be able to communicate directly by voice with the incident command (or silver control) of the other emergency services attending the incident.
- (2) That every control room (or gold) of each primary emergency service dealing with an incident shall be able to communicate directly by voice the control room (or gold) of the other primary services dealing with that incident.
- (3) Any locally agreed transmission of data between the primary emergency services will take place between control rooms from where it will be cascaded through the command structures of each emergency service, as required.

5.4 For resilience:

- (1) That the *same-service* and the *multi-service* interoperability between mobile resources shall continue to function even when any or all of the headquarters and control rooms of any of the emergency services are non-operational.
- (2) That the *same-service* and *multi-service* communications requirements shall continue to function irrespective of any failure of the public switched telephone network or any associated private circuit.

- (3) In the event of the failure of the wide-area radio system used by one or more of the primary emergency services which prevents the planned *multi-service* interoperability and at incident/silver command level, incident commanders will determine locally how best to provide this level of interoperability. Where the primary emergency services have common equipment that will operate in a mode that does not involve access to a fixed radio system, this may be used for this purpose. Where this is not the case, this agreement provides that the police service at the incident will temporarily provide equipment to the incident/silver commands of the other emergency services for this purpose.

5.5 It is neither intended nor desired that *multi-service* interoperability should apply to the handheld radio sets used to provide fire service at-incident communications.

6 Protocols

- 6.1 Nothing in the above excludes, nor requires as an essential precondition, the control of interoperability by protocols.
- 6.2 However, pan-service operating procedures will be essential to successful same and multi-service interoperability. In particular, safety and command requirements demand that at any incident communication between the fire service and the other emergency services are restricted to the Incident Commander (Silver-Fire). It is expected that all fire appliances except the vehicle designated as "Silver Control" must switch off their radio sets on arrival at an incident.
- 6.3 Nothing in the above in any way diminishes or interferes with the rights and responsibilities of each emergency service to control *same-service* interoperability by its own standard operating procedures.

7 System Management

- 7.1 All communications systems need to be managed on behalf of the user service.
- 7.2 Multi-service interoperability will require management representing the needs of all the services using it and dealing with procedural and technical issues.

8 Data Requirements

Save as provided, the transmission of data is outside the scope of this agreement.

Annex E (informative): Bibliography

- ETSI TR 102 476: "Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities".
- ITU-T Recommendation E. 107: "Emergency Telecommunications Service (ETS) and interconnection framework for national implementation of ETS".
- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).
- ETSI EG 202 116: "Human Factors (HF); Guidelines for ICT products and services; "Design for All"".
- ITU-T Recommendation E.115: "Computerized directory assistance".
- ETSI TS 123 271: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Functional stage 2 description of Location Services (LCS)".
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- ETSI TS 101 109: "Digital cellular telecommunications system (Phase 2+); Universal Geographical Area Description (GAD) (3GPP TS 03.32 Release 1998)".
- ETSI SR 002 299: "Emergency Communications; Collection of European Regulatory principles".
- ETSI TS 102 164: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Emergency Location Protocols".
- ETSI TR 102 299: "Emergency Communications; Collection of European Regulatory principles".

History

Document history		
V1.1.1	December 2005	Publication
V1.2.1	February 2008	Publication