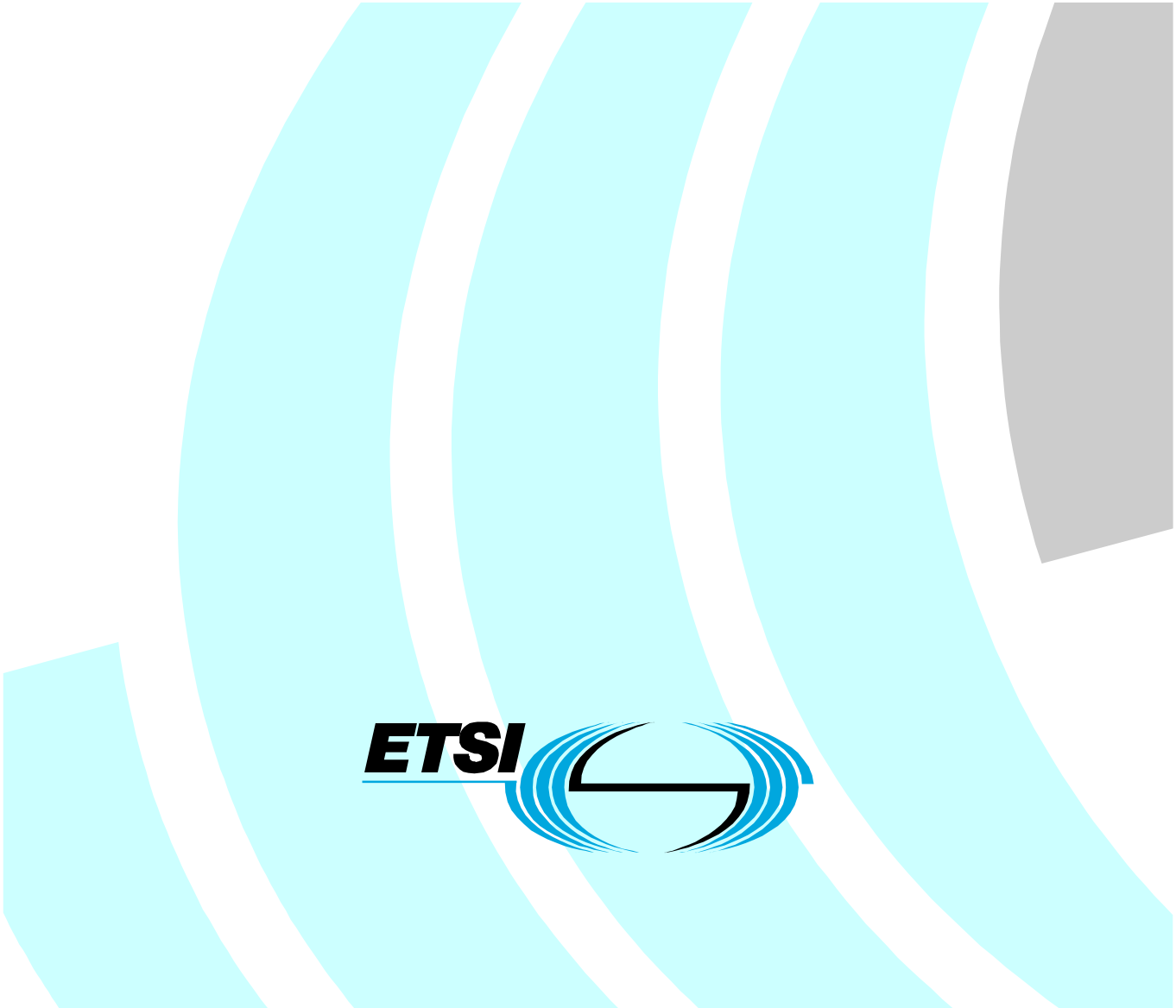
ETSI EG 202 339 V1.1.1 (2004-09)

ETSI Guide

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Definition of requirements on the functional architecture for supporting Emergency and Priority user services



Reference
DEG/TISPAN-02006-EMTEL

Keywords
architecture, emergency, service

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

Contents

Intellectual Property Rights

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

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

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

Emergency Telecommunications (EMTEL) have taken much importance and requirements on the functional architecture for supporting Emergency and Priority user services are needed from the expressed users needs which depend of:

- the **type of user** (User, Government agency, Business, Law enforcement, Emergency);
- the **type of operation** (Day to day, Emergency, Disaster);
- the **phase of the emergency** (Risk assessment, Response, post Disaster);
- the **localization of the user** (On disaster site, outside disaster site);
- the **service characteristics** (Voice call, Data transmission, Conference call).

Typically this concerns:

- communications of Citizens with Authorities;
- communications between Authorities;
- communications from Authorities to Citizens;
- communications of Authorities with the Emergency multi-disciplinary teams;
- communications of Authorities with Agencies to get information from Information Systems.

The objectives and requirements should include priority, interoperability, reliability, security and functionalities depending of the users and communications networks:

- wired or wireless;
- public or private;
- legacy or future.

A common set of services has to be identified.

Typical scenarios, corresponding to the list above, have to be identified, in order to use them as reference scenarios.

New areas of standardization may be found from the requirements.

This could be applicable to Homeland Security.

1 Scope

The present document defines requirements and proposes a functional architecture of an Emergency Telecommunication Service for international cooperation in Europe.

It clarifies definitions of the different actors.

It classifies the concerned users, types of services offered, timing and location of the events requiring Emergency Telecommunications Service.

It refers to the existing models, while protocols adaptations are being developed in ITU T and R, ETSI, IETF and other organisms of standardization and forums.

It defines the requirements for a functional architecture to support Emergency and Priority user services based on the services asked by the users concerned, through:

- The European Commission and Civil Protection (EGERIS) [7];
- ETSI Emergency Telecommunications (EMTEL) [9];
- ITU-R and T Public Protection and Disaster Relief (PPDR), Emergency Telecommunication Service (ETS), Telecommunication Disaster Relief (TDR) [3];
- ETSI TETRA Users Requirements (URS) [6];
- IETF Internet Emergency Prepareness (IEPREP) [8];
- ETSI-TIA MESA Specifications of Requirements (SoR) [1].

It proposes a list of services needed in a phasing to define.

NOTE: The term requirement means a capability which may be part of the ETS service, dependant on national decision and technical feasibility.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

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

[1] ETSI TS 170 001: "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements".

[2] ETSI TR 170 003: "Project MESA; Service Specification Group - Services and Applications; Basic requirements".

[3] ITU-R Report M.2033: "Radiocommunication objectives and requirements for public protection and disaster relief".

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

[5] ITU-D Handbook on disaster communications.

[6] ETSI TR 102 021 (all parts): "Terrestrial Trunked Radio (TETRA); User Requirement Specification TETRA Release 2".

[7] ETSI EG 201 936: "Services and Protocols for Advanced Networks (SPAN); Interworking; IP Federating Network (IPFN) architecture".

[8] IETF IEPREP: "Requirements for Emergency Telecommunication Capabilities in the Internet".

[9] ETSI OCG terms of reference OCG17(02)30: "Proposed Terms of Reference for the OCG ad-hoc group on Emergency Telecommunications (OCG EMTEL)".

[10] ITU-R Report M.2014: "Spectrum efficient digital land mobile systems for dispatch traffic".

3 Definitions and abbreviations

3.1 Definitions

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

Emergency Response Centre: node of a network which receives the emergency calls (e.g. 112) and takes in charge these calls, answering and handling them to the right entity

NOTE: It may interoperate with control centres. It is also referred as Contact centre, PSAP (Public Safety Answering Point).

control centre: node of a network getting information from network connected Data Bases (GIS) for display, computing and which is in contact and monitoring the interdisciplinary emergency teams on site (Voice, Data, Location)

NOTE: It may be connected to other control centres for information exchange, connected to administrations networks. It is also called Command and Control Centre, Operational and Tactical Centre, Monitoring and Information centre, Computer Aided Dispatch, Emergency Operation Centre.

user: any entity that actually establishes communication with an emergency response centre service, Control Centre

NOTE: It includes Civilians also referred as citizens, mission critical users, government agents, relief organizations.

relief organizations can include the following:

- Emergency authorities;
- Public Utilities;
- Government authorities;
- Agents/applications;
- Private Service Providers.

inter-working: ability of equipments to communicate together from different systems and with similar services

NOTE: Those equipments are not roaming from one system to a different one.

interoperability: ability of equipments from different manufacturers (or different systems) to communicate together on the same infrastructure (same system), or on another while roaming

location based services: specific services offered depending of the user geographical location like mapping services, points of interest, routing services

portability: ability of an entity or element to be used in different systems or environments

roaming: process of changing the network access point from one Location Area, Network or Domain to another within one system or between different systems

NOTE: This may include different systems using the same technology.

gateway: interface, between two (or more) systems that have similar functions but dissimilar implementations, enabling users on one network to communicate with users

server: server is an application program that accepts requests in order to service those requests and send back responses to those requests

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in [1] and the following apply:

EC	European Commission
EMTEL	EMergency TELecommunications
ERC	Emergency Response Centre
ETS	Emergency Telecommunications Service
GETS	Group for Emergency Telecommunications Service
GIS	Geographical Information System
GPS	Global Positioning System
IAA	I Am Alive
IEMS	International Emergency Multimedia Scheme
IEPREP	Internet Emergency PREParedness
IEPS	International Emergency Preference Scheme
IETF	Internet Expert Task Force
IPFN	IP Federating Network
PAS	Priority Access Service
PIM	Presence and Immediate Messaging
PSAP	Public Safety Answering Point
QoS	Quality of Service
ROBO	Remote Office Branch Office
SOHO	Small Office Home Office
URS	Users Requirements Specification
V+D	Voice plus Data
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

4 Background information

It is a fact that wireless and wireline technologies are diverse with their specific services adapted to different markets including the Emergency one.

- ETSI has launched EMTEL.
- International Emergency Preference and Multimedia Schemes are being specified by ITU-T, -R, -D [3], [4], [5] and other organizations and projects such as IETF (IEPREP) [6], [7], [8], 3GPP (PAS), GETS (USA), IAA (Japan) in order to set up procedures and processes for handling emergency communications.
- It should be made clear that many of these procedures are mainly applicable in Day to Day operations, when the corresponding telecommunications infrastructures are still up and running.
- They do not apply when the situation corresponds to large emergency or disasters. In such cases fixed and mobile public networks are usually totally congested and/or partly destroyed.
- Sers specifications start being collected [1], [2],[6].
- European specificities should be considered in particular for interoperability.

5 Classifications

5.1 Major user's classes concerned

Figure 1 shows the actors concerned by emergency and priority services, their interconnection through wired and wireless public and private networks.

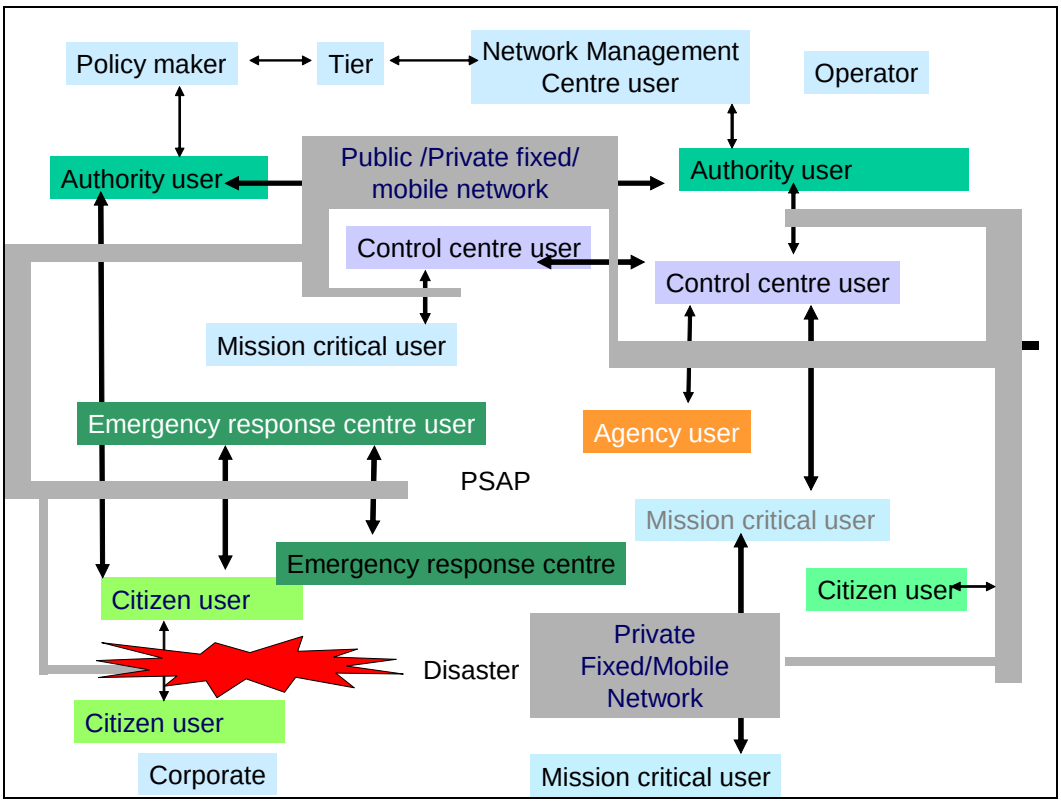


Figure 1: Actors concerned

Two major classes of users are identified as mission critical and non mission critical:

- Mission critical relief organization such as:
  - Fire brigade, Security forces, Ambulances, Civil protection, Military, Medical, Air and Sea rescue, Criminal Justice, Mountain rescue.
- Non mission critical entities such as:
  - **Users** (public) to allow the citizens (residential) to make an emergency call, communicate, be informed.
  - **Administration critical** users (public and private) such as Government authorities, Agencies, Utilities, Diplomatic, Customs, Immigration, Law enforcement, Environment in order to decide, coordinate, inform.
  - **Business critical** users (corporate) such as Companies, ROBO, SOHO, network operators and tiers which have to maintain and restore their work environment.

These users have different communications means public, dedicated or commercial, with different policies, and they need to be able to inter work.

5.2 Emergency communications situations

Communications situations can be classified as defined by ITU in:

- **Day to day** or routine for example on large areas such as urban, country.
- **Emergency** such as a fire, a car accident on a hot spot.
- **Disaster** such as an earth quake, a flood.

They do not require the same communications means.

5.3 Emergency communications types

Different types of communications can be identified such as:

- Mission critical communications:
  - Local: between on site users (Fire, Security, Medical).
  - Remote:
    - Relief organization to Control centres.
    - Local members of the relief organization to the control centres.
    - The control centres to the local members of the relief organization.
- Administration critical communications:
  - **Between Administrations** (local/regional/central, government).
  - **Communications** between Administrations and **Agencies** (meteorological, environmental).
  - **Communications** between Administrations and **Utilities** (electricity, gas).
  - **Communications between Administrations and Network Management centers.**
- Business critical communications (corporate, ROBO, SOHO).
- Users critical communications:
  - Communication from users to Emergency response centres.
  - Broadcast from Authorities to Citizens.

5.3.1 Mission critical communications

Mission critical communications use a separate (operated or not) private, fixed and mobile, voice and data digital network (TETRA, APCO25, TETRAPOL, idEN as defined in ITU report M.2014 [10]).

Special services are offered such as:

- High quality voice and data in noisy environment, end to end secured calls, fast call set up, high traffic support on a small area, redundancy.
- Specific Tele and Supplementary Services like Group call, Emergency call, Ambiance listening.
- Direct Mode Operation (DMO).
- With on site coverage, possibly "ad hoc".

They are composed of different specific sub systems like:

- Highly optimized Radio access, redundant secured Core network.
- Repeaters, Gateways, Control centres, Emergency response centers.

Inter working between different organizations is supported.

5.3.2 Business critical communications

In case of emergency it is necessary to maintain and restore business for Corporate, SOHO, ROBO and to allow geographical dispersion while maintaining services on public and private VPN networks, circuit and packet switched, for Voice and Data.The Networks requirements for Corporate V+D continuity can be:

- Network fast switching, data rerouting, redundancy, variable bandwidth, back up access.
- Mobility of switches.
- VPN connectivity.
- Remote access.

Remote management.

5.3.3 User critical communications

Various infrastructures and services are concerned at the user's Home such as PSTN, ISDN, IP, Cable, GSM, TV, RADIO.

- Users need Voice and Data emergency communications (112), call back, possibility to give location information, broadcast reception.
- The same information can be sent to different types of terminals in their home.
- The PMR core network, if "under loaded", could be used as a backup to the public network.

5.3.4 Administration critical communications

Agencies and Administrations need Communications resources for information, coordination and control (warning, reports). This is mainly data base information, secured voice communications and data exchange.

5.3.5 Mission critical connectivity

Interconnection of public networks and private networks may be needed depending of the situation:

- "Routine" situation:
  - PMR private networks offer services for mission critical users who need fully reliable communications whatever the conditions, the location, even underground.
  - EMTEL will offer a limited set of PMR services on public wired and wireless networks.
  - Possible end to end Public to Private / Public calls may be offered.
- Emergency situation:

  It is necessary to differentiate on site mission critical users connexity and remote users connexity:
  - On site connectivity:

    Inter working of public/private networks is needed to share information.
  - Remote connectivity:

    Points of connection between Private and Public networks are needed through gateways, with guaranteed QoS, Security in order to allow:
    - Some back up/rerouting for Control and Call centres users;
    - Some administration, business, user's priority/emergency calls;
    - Some end to end Public to Private (to public) calls.

6 Operational scenarios

The scenario chosen in priority shall reflect user needs, including a mix of different types of communications such as public, private, corporate. They are corresponding to the EC priorities given at EMTEL in ETSI.

They include Emergency Response Centres, Control centres as sub systems added to a public and private WAN.

The main scenarios and interfaces associated correspond to figure 2, numbers correspond to scenarios and interfaces.

The different scenarios are described in table 1 with the following information:

- from which user;
- to which user;
- by which means;
- for which reason;
- the network problem to avoid;
- the scenario number.

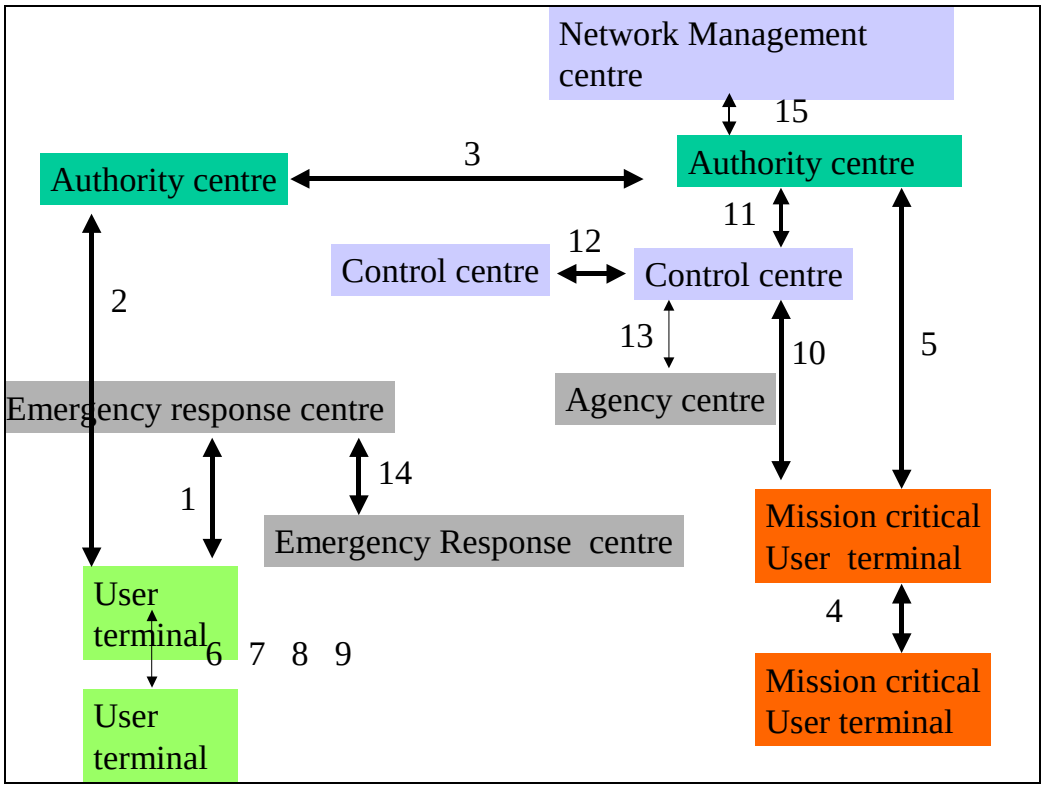


Figure 2: Main information exchange between subsystems

The main information exchanges concern:

- authority (administration) to:
  - authority;
  - control centre;
  - user;
  - mission critical user;
  - network management (coordination) centre.
- control centre to:
  - control centre;
  - authority;
  - mission critical users.
- emergency response centre to:
  - user;
  - emergency response center.

Table 1 identifies 15 reference scenarios.

Table 1: Main scenarios

Action	From	To	Means	Reason	Network problem to avoid	Scenario Number
Emergency call (112 location)	User on disaster, emergency site	Emergency Response Centre (ERC)	Wired, wireless	Need for help, and information	Congestion	1
Broadcast	Authority	User citizen on disaster site, emergency site	TV, Radio, wireless	Warning of danger Information	Congestion	2
Priority Secured Voice and Data communication	Authority	Authority	Wired and wireless VPN	Communicate information, decision	Congestion, lack of security, priority, quality	3
On disaster site communication voice and data	Mission critical users	Mission critical users	Wired Wireless PMR,	Information and Coordination on site Voice and Data	Congestion, lack of security, priority, quality	4
On disaster site communication voice and data	Mission critical users.	Authority	Wireless and wired public and private networks	Report, Voice and Data	Congestion, lack of security, priority, quality	5
Maintain, reconfigure business work forces	Business, SOHO, ROBO	Business	Wired, wireless, VPN	Maintain business	Congestion, lack of Security, QoS	6
IP communication	USER1	USER2	Internet	Rerouted Voice and Data communication	Congestion, lack of security, priority, quality	7
PSTN call	USER1	USER2	Circuit Switched Network	Reroute communication, priority, security	Congestion, lack of security, priority, quality	8
PSTN call	USER1	USER2	Normal route	Urgency	Congestion, lack of security, priority, quality	9
V+D Communication	Mission Critical users	Control Centre	PMR and Private networks	Urgency	Congestion, lack of security, priority, quality	10
V+D communication	Control centre	Authority	Wired and wireless	Information	Congestion, lack of security, priority, quality	11
V+D communication	Control centre	Control centre	Wired and wireless	Exchange of information	Congestion, lack of security, priority, quality	12
Collect information	Control Centre	Agencies, Utilities	Wired and wireless, satellite	Information	Congestion, lack of security, priority, quality	13
Exchange information	Emergency response centre	Emergency response centre	Wired, wireless	Information	Congestion, lack of security, priority, quality	14
Networks status and reconfiguration	Authority	Network management Coordination	Wired and wireless public and private networks	Traffic, load, QoS information	Congestion, lack of security, priority, quality	15

The different scenarios are represented on figure 2, the numbers are referring to the scenario numbers of table 1:

- Administrations communicate with other authorities (see scenario 3).
- Administrations broadcast information to citizens users on the emergency site (see scenario 2).

Citizens users on the emergency site use 112 to call the Emergency Response Centre for help with their location information attached (see scenario 1).

Other possible scenarios are:

- administrations:
  - receive/send information from/to the emergency on site teams (see scenario 5);
  - receive information from the control centres (see scenario 11);
  - communicate with the Network Management coordination centre. (see scenario 15).
- emergency teams communicate with:
  - other emergency teams on the emergency site (see scenario 4);
  - their control centres (see scenario 10).
- control centres communicate with:
  - other control centres (see scenario 12);
  - public utilities, agencies (see scenario 13);
  - authorities (see scenario 11).
- emergency response centres communicate with:
  - users (see scenario 1);
  - emergency response centres (see scenario 14).
- business centres communicate with:
  - business centres (see scenario 6).
- a user wants to communicate to a user 2, he normally uses link 9:
  - due to an emergency in a specific area, another PSTN or IP route (VoIP) is selected (see scenario 7 and 8);
  - the IP route reconfigures itself automatically for data and for VoIP if quality permits (see scenario 7).

Figure 3 represents the main communication scenarios.

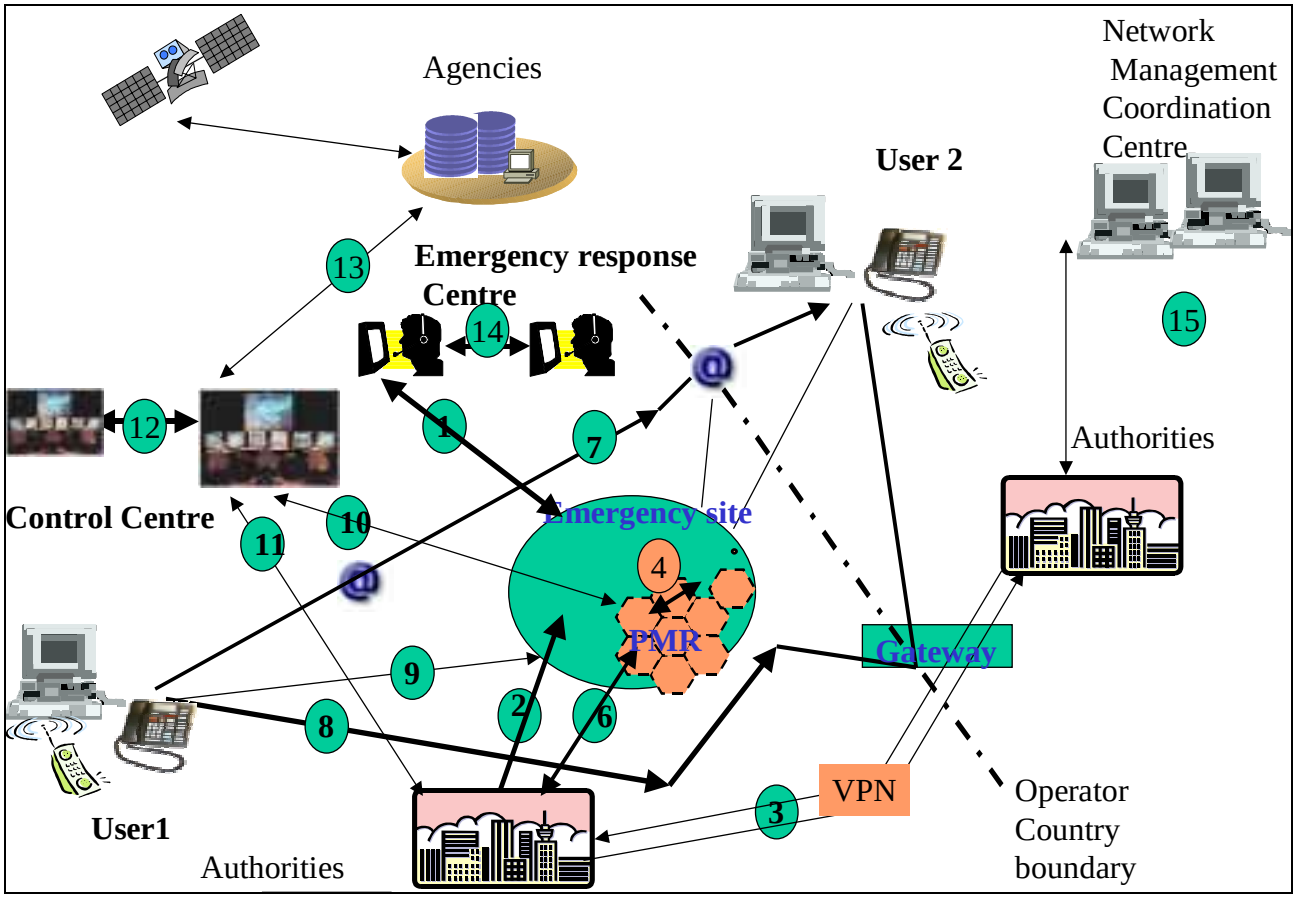


Figure 3: Networks scenarios

Figure 4 represents the different network overlapping planes concerned by EMTEL with part of the networks destroyed. Gateways allow to reroute some traffic and ensure interconnection of the different networks.

They networks represented are:

- the public wired network as PSTN;
- the IP network, VPN;
- the public wireless networks GSM, UMTS;
- the PMR network;
- the Satellite network.

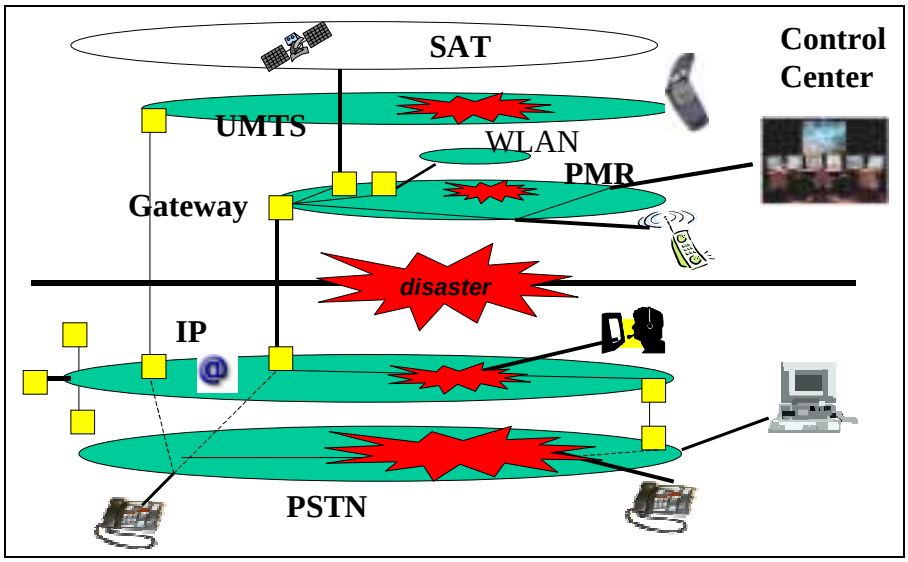


Figure 4: Different planes concerned

7 Services requirements

This clause identifies a first list of services needed. A differentiation is done between services under national regulation and services proposed to be internationally available, for example by the EC and which require standardization. Then it is a national decision to adopt an EC requirement as far as it is technically feasible.

7.1 Features and Services required

From the recent emergency, day to day and disasters situations and the users requirements it appears that the following services are identified to be needed in priority such as:

- (International - EC) - **Access to establish communication to an emergency response centre (e.g. 112)** with priority to avoid in a crisis situation load congestion, and to be able to reach the corresponding emergency response centre.
- (International - EC) **Location information**.
- (National) **Disaster warning** of users by **Broadcasting** information to the users on the appropriate telecommunication mean available to them.
- (National) **Information pushed** to the citizens about the crisis, on what is happening such as danger location, risks, what to do.
- (National and commercial - service providers) **Business continuity to** ensure locally and remotely.
- (National) - **Re establishment and re routing of communications** by introducing gateways between different networks.
- (National) Being able to receive **IAA (I am alive)**.
- (International - EC) **Priority communications** between authorized users in day to day or emergency operation.
- (International - EC) **Secure confidential communications** between authorized users in day to day or emergency operation.

Emergency Response centre requirements

- Emergency calls shall be forwarded to the right local emergency response centre.
- Preventing unauthorized dial-in.
- Identification of the person.
- Security against dialling the wrong number.
- Interruption of free software downloads at the exchange.
- Monitoring emergency call lines.
- Access to emergency calls even if lines are blocked.
- Access for disabled persons.
- Calls made from geographically ported lines: routing information on the changed geographical location is adapted at the new location as soon as the new line is connected.
- Providers of emergency call distribution services shall be able to access any line that is not listed in the directory.
- Display of the network operator identification code in an emergency calls.

Control centres requirements

- Interconnection between them.
- Interconnection with private and public data bases.
- Replication techniques.
- Definition of standard Database model.

User information

Informing the user should be done by any of the communication means available such as:

- fixed telephone line;
- mobile phone;
- internet access;
- television, radio.

Information should be able to be routed to the user by the telecommunication mean which is not congested, to the terminal which is powered on, on which the user is present whatever the communication mean is used: public, private, fixed, mobile, satellite.

User Data

Data type transmitted corresponds to:

- location information;
- short message;
- image transfer (e.g. MMS);
- forms transfer;
- E-Mail;
- file transfer;
- multimedia (e.g. video).

Security

Voice and Data calls end to end should be secured:

- encryption;
- authentication;
- integrity.

Procedures

The use of common EC procedures policies and practices (e procedures) should be defined:

- Translation service (Language) should be offered.

Mediation service to handle different terminals types should be considered.

Middleware service to handle different data formats should be offered.

8 Generic architecture model

The Architecture model should be derived from the Operational model which is outside the scope of the present document but which is under way in different standard bodies:

- Several users requirements and reports are now available, through ETSI EMTEL, ETSI-TIA MESA, IETF IEPREP.
- Regulatory issues should also be considered as well as the necessity to take into account each national policy specificities.
- A technology independent approach should be taken but it should include legacy and future systems.
- Different types of events and phases such as day to day, emergency, disaster operations should be considered.

Figure 5 shows a global proposed WAN architecture with sub networks connected to the WAN named Application Node (AN) and Resource Node (RN).

The Wide Area Network (WAN) includes the physical, commercial and legal components required to enable optimum connection and operation with the RNs and ANs.

The WAN may be composed of:

- Public Wireless (GSM, GPRS, UMTS, Satellite) networks.
- Public Circuit Switched (PSTN) networks.
- Private wired and wireless (VPNs, PMR, Satellite) networks.
- Packet and Cell switched (Frame relay, IP, ATM) networks.
- Gateways.
- Operation and control centre.
- IPBX.
- Network Management centre.
- Security management centre.

Each network standard and technology uses different techniques of:

- Prioritization.
- Segmentation.
- Control of variable delay.
- Voice compression.
- Silence suppression.
- Echo cancellation.
- Signalling;

with different levels of Quality of service and Security.

The sub networks can be seen as composed of Resource Nodes (RN) and Application Nodes (AN):

- **Resource Nodes (RN)** are the access points to service and data providers. The RNs provide an interface to the networks operated by telecommunication operators, earth Observation and Navigation satellites providers as well as appropriate Terrestrial service and Data providers.
- **Application or Users Nodes (AN)** are optimized to serve a number of emergency management applications and End-Users. End user networks may include fixed or mobile terminals, specific applications software, graphical user interfaces, operation information and control centres, Computer Aided Dispatch.

The following generic model is proposed represented on figure 5 where the application nodes are split per operational scenarios as day to day, emergency, disaster as the requirements are different in terms of traffic, priority, resources needs, performance required. Also the means used by the different categories of users are not the same:

- Ad hoc network on a disaster hot spot.
- Secured voice and data communication between administrations.
- High availability and quality communications for mission critical users.

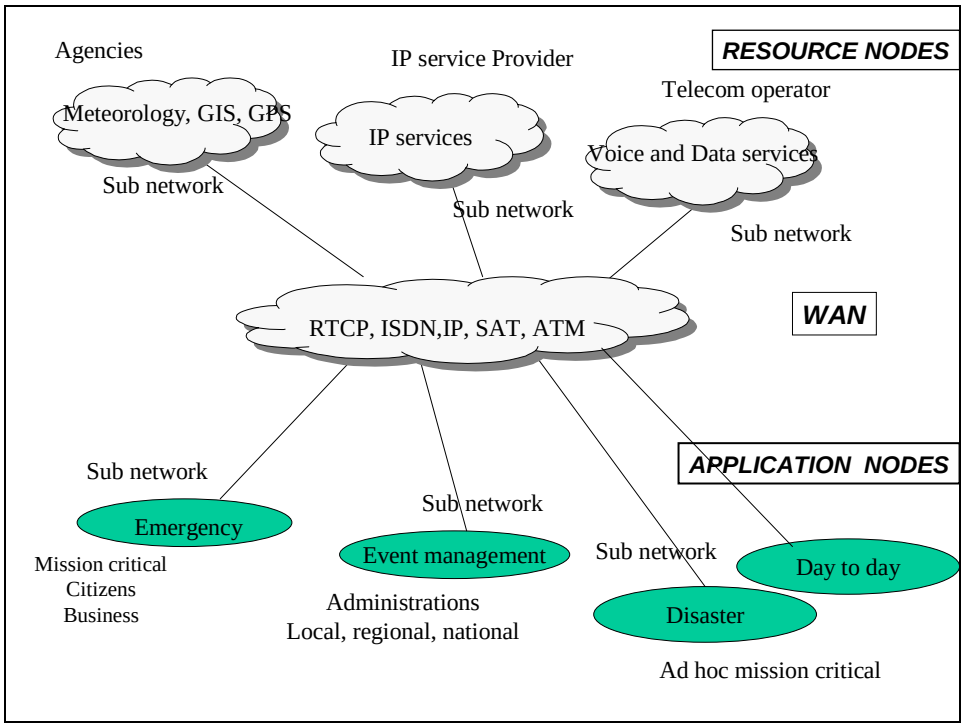


Figure 5: WAN and Resource and Application nodes

This can be summarized as in figure 6 by a generic model.

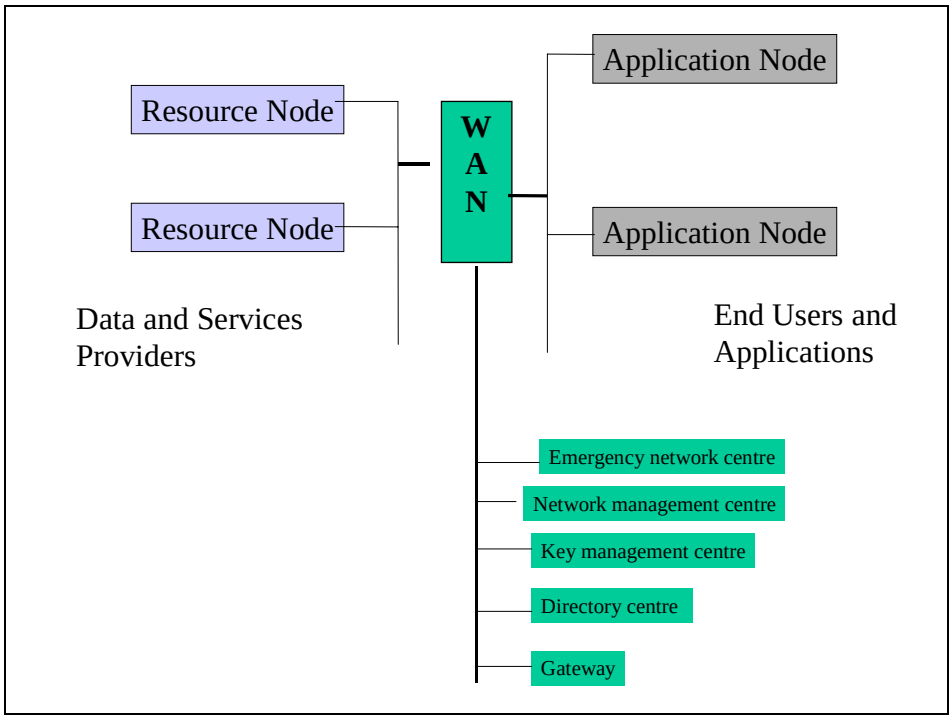


Figure 6: Global architecture

8.1 Functional model

A list of functional requirements is given for WAN, AN and RN and a functional model can be derived.

8.1.1 Functional requirements

- **Resource Node (RN)** requirements should include:
  - promotion, making aware the end user of the available services;
  - ordering, enabling the end user to select and request specific services;
  - delivery, providing services to the end user;
  - utilization, ensuring that end to end users have the correct operational facilities to enable them to make efficient use of the services;
  - support, helping the end user for maximizing the value of service offering;
  - charging and accounting.
- **Application end user node (AN)** requirements should include for example:
  - interrogation, finding out information about services available;
  - ordering, requesting delivery of service;
  - access, gaining authorized access to the facilities;
  - acquisition, taking delivery of requested service;
  - utilization, ensuring resources are available;
  - support, helping the end user for maximizing the value of service offering.
- **WAN requirements** should include the following:
  - security through networks using authentication, encryption;
  - priority mechanisms and management;
  - Quality of Service, Resource management;
  - user management;
  - network management;
  - dynamic routing;
  - redundancy for availability.

8.1.2 Functional model

The functional model derived is split into different sub functions as:

- Functions of the WAN:
  - directory;
  - catalogue;
  - registration;
  - software repository;
  - service specification;
  - ordering.
- Functions of the AN:
  - end user registration and access;
  - directory access;
  - interrogating a catalogue;
  - resource delivery;
  - supporting facilities;
  - end user requirements capture.
- Functions of the RN:
  - populating a directory;
  - providing catalogue information;
  - service specification;
  - charging and accounting;
  - software repository;
  - registration.

8.2 Reference points

The different reference points are at the Application level, for voice and data, between the following end points:

- operation and control centre terminal;
- emergency response centre terminal;
- authority terminal;
- agency terminal;
- end user terminal.

This gives as a first list:

- R1 (PSAP) between end user terminal and Emergency response centre's terminal.
- R2 between end user terminal and Authority terminal.
- R3 between Authority terminal and Authority terminal.
- R4 between Mission critical user's terminals.
- R5 between Mission critical user's terminal and Authority terminal.
- R6 between end user's terminal and end user's terminal.
- R7 between Emergency response centre's terminal and Control centre's terminal.
- R8 between Emergency response centre and Control centre.
- R9 between Mission critical user's terminal and Control centre's terminal.
- R10 between Control centre's terminal and Authority terminal.
- R11 between Control centre's terminal and Control centre's terminal.
- R12 between Agency terminal and Control centre's terminal.
- R13 between Emergency Response centre's terminal and Emergency Response centre's terminal.
- R14 between Authority's terminal and Network management centre's terminal.

Figure 7 shows the positioning of the reference points between the sub systems.

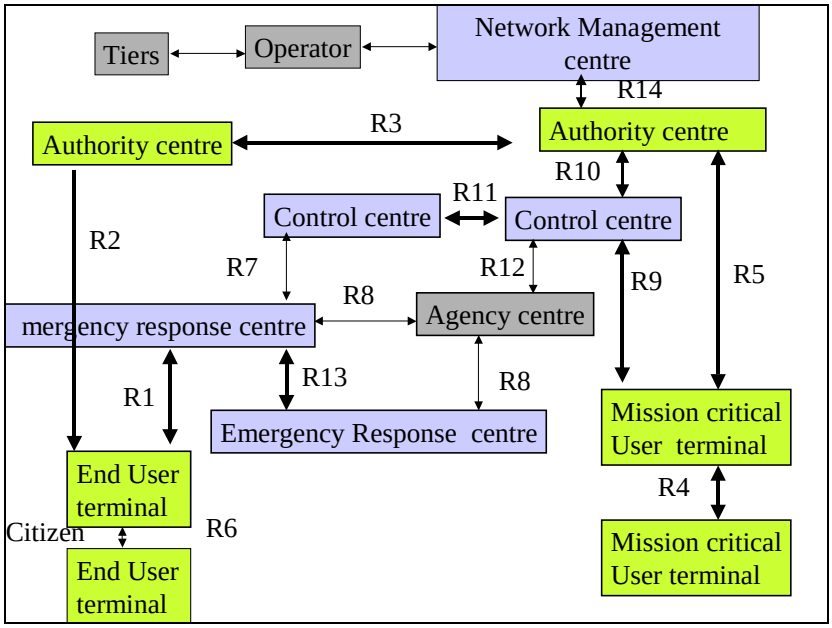


Figure 7: Reference points between the sub systems end points

The R1 interface between Citizen and Emergency Response centre, the R2 interface between Administration and Citizen, the R3 interface between Administrations, [9] are under development.

The R4 interface between mission critical users is specified in the corresponding standards like TETRA, APCO25, TETRAPOL. Interoperability interfaces between standards should be developed in case mission critical users use different standards.

The other Reference points should be specified as well as the global data model and information flow. Data content should not be standardized, only the data services across platforms, applications and programming languages. It includes XML, SOAP. Profiles should be defined.

8.3 Generic reference point model

The approach is a Model Driven Architecture (MDA), top down. UML could be used.

Sub systems are exchanging (Secured) Voice and Data through heterogeneous networks.

The reference model is related to end to end applications on terminals.

A unique generic reference point model Rx at application level can be described:

- Rx between AN and AN.
- Rx between RN and WAN.
- Rx between AN and WAN.
- Rx between RN and RN.

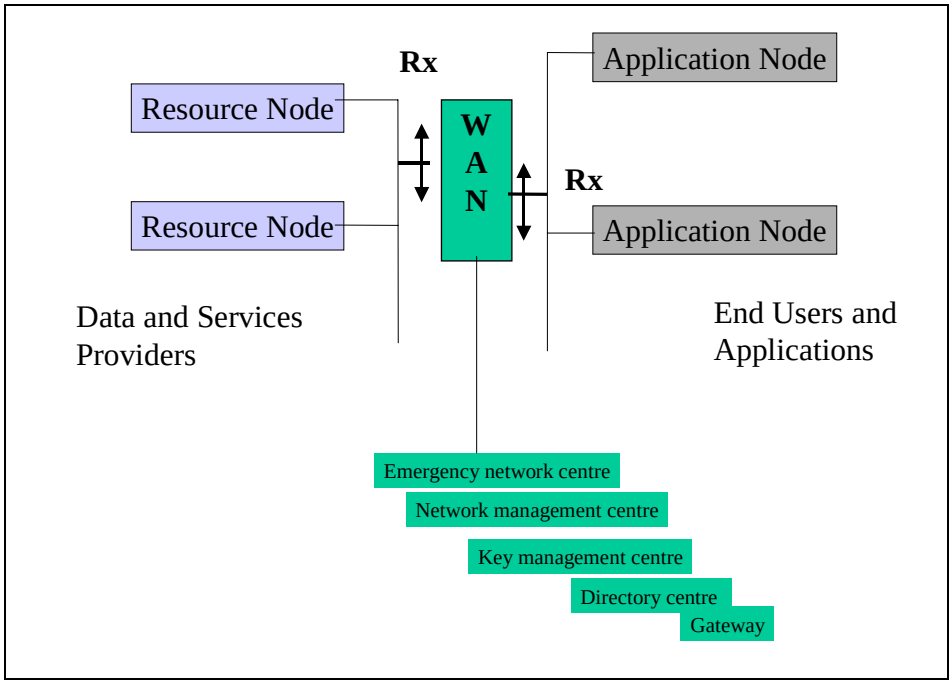


Figure 8: Generic reference points

8.4 Generic protocol model

A generic protocol model can be derived at the reference point Rx, with a unique protocol stack (see FNBDT 220) in each sub system end point:

- An application layer carrying signalling.
- A new application end to end protocol.
- Specific applications, security mechanisms:
  - The specific application depends of the sub system but is outside the present document.
  - The specific cryptography mechanisms can be local, national, multi national.
  - The specific codecs can be negotiated, or a unique (low rate) codec selected.

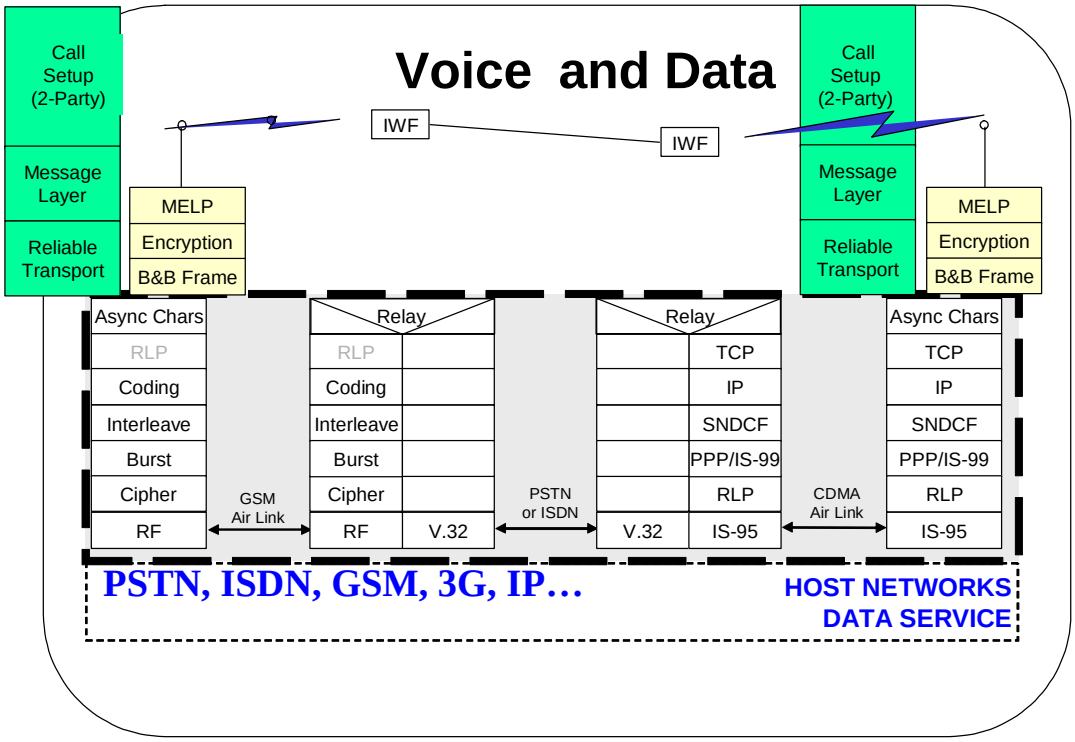


Figure 9: Generic protocol example

Figure 9 is an example locating the generic protocol at the application level.

This protocol allows inter operability through heterogeneous wired and wireless fixed and mobile networks.

8.4.1 Protocol assumptions

In order to be supported by many different transport, the protocol has:

- To be at application level.
- To use a data path end to end, carrying voice and data.
- To be inserted in the data capability.
- To use frame stealing to carry signalling during voice transmission (Blank and Burst (B&B)).
- To use a unique voice codec to have no transcoding (MELP).
- To have mechanisms to negotiate security algorithms, key management.
- To have reliable transport layer, with end to end connections are defined by the concatenation of network segments.
- To be flexible for new applications and cryptographic suites.

9 Conclusion

The present document has set up a top down approach to Public Protection and Disaster Relief including EMTEL. It proposes users and system models and a reference model. This should allow to identify the interfaces to standardize. A protocol architecture for end to end interoperability through heterogeneous networks is proposed. One priority today is user transparent interworking, due to the multiplicity of legacy and new telecommunications networks wired, wireless fixed and mobile.

Annex A (informative): Bibliography

IETF draft Securing prioritized emergency traffic.

IETF draft framework for supporting IEPS in IP telephony.

IETF draft Emergency Telecommunications Service in evolving networks.

ETSI TR 101 300: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of Technical Issues".

FNBDT 220: "FNBDT requirements, interoperable modes".

ETSI standards: http://www.etsi.org

History

Document history			
V1.1.1	July 2004	Membership Approval Procedure	MV 20040903: 2004-07-06 to 2004-09-03
V1.1.1	September 2004	Publication	