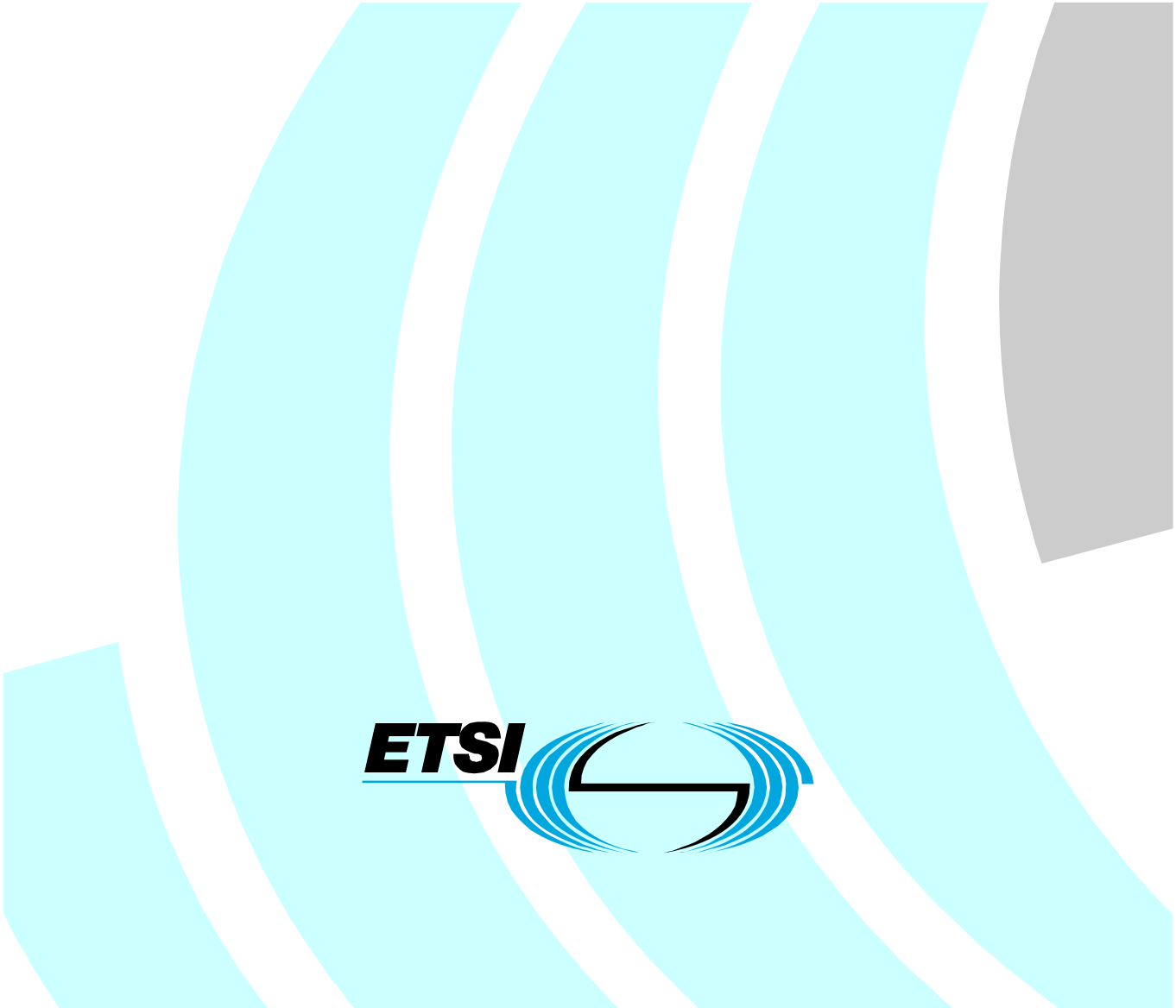
ETSI TS 102 650 V1.1.1 (2008-07)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of Location Information Standards produced by various SDOs



Reference
DTS/TISPAN-03048-EMTEL

Keywords
Emergency, location

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

Introduction

The present document has been produced by an ETSI STF co-funded by EC/EFTA to examine the work of various Standards Development Organizations worldwide in developing and implementing protocols for the transmission of location information over telecommunications networks for use in establishing the location of users of the emergency calling facilities. In order to effectively deliver emergency services to the location of a reported incident, it is essential for the emergency response organization to have timely and accurate information that enables them to correctly identify the location of the incident.

The ability to initiate an emergency communication to summon help when needed is regarded by the European Commission as a right of all citizens and this ability should ideally be independent of the network and access technologies deployed or the physical abilities of the citizen.

The rights of individual users to privacy shall be adhered to according to European regulations and it is therefore essential that all information derived from emergency calls shall only be used for management of the related incident. If applied to non-emergency calls, the use of caller location information for commercial purposes may also be subject to European or national regulation.

In many circumstances, citizens reporting an incident requiring urgent assistance are unable to provide the emergency service with accurate information about the location of the emergency. This may be due either due to the nature of the emergency, the callers' lack of local knowledge, their disabilities or lack of linguistic ability, etc. Young children or cognitively impaired people may not have the language skills to explain their location, speech and/or hearing impaired users may not be able to use voice terminals, visually impaired or otherwise disabled people may not be able to use text terminals, elderly or confused people may not be able to use any form of terminal, etc. For these significantly large categories of users the successful outcome of an emergency call could make the difference between life and death. It is therefore essential for the emergency responders to be provided with accurate location information via an automated process based on the communications network being used by the caller.

Implementation of caller location systems is also likely to result a welcome positive impact on the reduction of malicious calls made by criminal or anti-social persons when they realize that the automatic provision of their location information to the emergency services could enable their almost instant apprehension.

The present document should be read in conjunction with TS 102 660 [19] which reports on the Signalling Requirements and Signalling Architecture for Supporting the Various Location Information Protocols for Emergency Service on a NGN. The object of this work was to determine what, if any, standards existed and had been adopted for signalling details of an emergency caller's location, in order to assist in the response to emergency calls.

It should be recognized that in the present document all references implying that 911 is the common emergency calling number are used only to identify pre-existing work and as part of the titles of other documents. The mandated common European emergency number is 112 with many countries also operating national numbers in parallel.

The present document does not contain a fully detailed technical analysis of location information standards but concentrates on the background information and the ongoing activities by the various standards bodies in different regions. It should be borne in mind that the document is intended to be focussed on what EC/EFTA wanted from their contract, essentially to understand what the work is and what needs to be done. It is for TISPAN to do the in depth analysis and produce the detailed technical recommendations.

1 Scope

The present document represents an analysis of the work done by various ETSI work groups and other standards bodies worldwide on the acquisition and transmission of caller location information in various communications network types. It also contains information about the protocols used and of any known deployments for the location of users making emergency calls. It is not intended to examine the detailed workings of the protocols described or their possible use in other communications network types.

The document does not mandate any new requirements but does report on the normative requirements from other standards and regulatory bodies. It also refers, in part, to operating methods and national regulations in various jurisdictions but does not intend to endorse these as requirements.

The hypothetical accuracy of the caller location and the accuracy achieved by the assessing methods are also documented. Alternative methods for the coding of the emergency location information are also examined.

The present document also indicates a number of scenarios where location information may not be available or may be inaccurate to various degrees and may suggest solutions for improvement.

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] ETSI TS 123 167 (V7.6.0): "Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167 version 7.6.0 Release 7).

[2] ETSI TS 123 041 (V3.5.0): "Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041 version 3.5.0 Release 1999)".

[3] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-system (NASS)".

[4] NENA «I2» architecture: "Interim VoIP Architecture for Enhanced 9-1-1 Services («i2»)".

NOTE: Available at http://www.nena.org/media/File/NENA_08-001_V1_12-06-05_1.pdf.

[5] ISO 3166-1(2006): "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

[6] NIMA Technical Report TR8350.2: "Department of Defence World Geodetic System 1984, Its Definition and Relationships With Local Geodetic Systems"; Third Edition; National Imagery and Mapping Agency, 4 July 1997.

[7] IETF RFC 3046: "DHCP Relay Agent Information Option".

[8] IETF RFC 3825: "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information".

[9] IETF RFC 4776: "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information".

[10] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format".

[11] Coordination Group on Access to Location Information by Emergency Services (CGALIES): "Final Report V1.0".

NOTE: Available at http://ec.europa.eu/environment/civil/pdfdocs/cgaliesfinalreportv1_0.pdf and http://portal.etsi.org/docbox/STF/STF321_TISPAN3_EC_Emergency_Call_Location/Public/Library/EC%20Documents/cgalies_final.pdf.

[12] IP Location Information/04/006 V2 16Jan07: "Report from the IP Location Information Working Group".

[13] draft-arai-ecrit-japan-req-01: "Emergency Call Requirements for IP Telephony Services In Japan".

[14] 2003/558/EC (25 July 2003): "Commission Recommendation on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services" (notified under document number C(2003) 2657 [i.5]).

NOTE: This recommendation is replicated in annex A of the present document.

[15] ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

[16] ETSI TS 123 271: " Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Functional stage 2 description of Location Services (LCS) (3GPP TS 23.271)".

[17] ATIS Technical Report: "Location Acquisition and Location Parameter Conveyance for Internet Access Networks in Support of Emergency Services".

[18] GEOPRIV L7LCP: draft-ietf-geopriv-l7-lcp-ps-07.txt.

[19] ETSI TS 102 660: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Signalling Requirements and Signalling Architecture for supporting the various location information protocols for Emergency Service on a NGN".

[20] DCITA report: " Examination Of Policy And Regulation Relating to Voice Over Internet Protocol (VoIP) Services - Report To The Minister For Communications, Information Technology And The Arts ".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] "GPS-free positioning in mobile Ad-Hoc networks", Cluster Computing, 5(2), April 2002. Srdan Čapkun, Maher Hamdi, Jean-Pierre Hubaux.

[i.2] "Towards Mobile Ad-Hoc WANs: Terminodes", J.-P. Hubaux, J.-Y. Le Boudec, S. Giordano, M. Hamdi, L j. Blazevic, L . Buttyan and M. Vojnovic. IEEE WCNC, September 2000.

[i.3] "Location aided routing (LAR) in mobile ad-hoc networks", Y.B. Ko and N.H. Vaidya, MOBICOM, 1998.

[i.4] "Self-Organizing Wide-Area routing", Lj. Blazevic, S. Giordano and J. Y. Le Boudec, SCI 2000/ISAS 2000, Orlando, July 2000.

[i.5] C(2003)2657 25 (July 2003): "Commission Recommendation of the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services".

[i.6] AS/NZS 4819:2003: "Geographic information - Rural and urban addressing". .

NOTE: Plus draft DR 05191 CP: Amendment 1 to AS/NZS 4819:2003.

NOTE: Australian Standards are available from: http://www.saiglobal.com/shop/Script/Provider.asp?Db=AS.

[i.7] IETF RFC 3693: "Geopriv Requirements".

[i.8] IETF RFC 4676: "Dynamic Host Configuration Protocol Option for Civic Addresses Configuration Information".

NOTE: IETF RFCs are available from: http://www.ietf.org/.

[i.9] NENA: "NENA VoIP Recommended Methods for Determining Location to Support Emergency Calling Technical Information Document (TID)".

NOTE: Available from: http://www.nena.org/media/files/08-505_20061221.pdf.

NOTE: Available from: http://www.3gpp.org/ftp/Specs/html-info/23167.htm.

[i.10] Directive 2002/21/EC on a common regulatory framework for electronic communications and services (the "Framework Directive") (OJ L 108, 24.4.2002).

[i.11] COUNCIL DECISION of 29 July 1991 on the introduction of a single European emergency call number (91/396/EEC). (OJ L 217, 6.8.1991).

[i.12] Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (the "Universal Service Directive") (OJ L 108, 24.4.).

[i.13] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "Directive on privacy and electronic communications") (OJ L 201, 31.7.2002).

[i.14] ETSI TS 123 167: "Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167 version 7.9.0 Release 7)".

[i.15] ETSI EN 300 403: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

[i.16] 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 version 7.12.0 Release 7)".

[i.17] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".

[i.18] DR 05191 CP: "Amendment 1 to AS/NZS 4819:2003 - Geographic information - Rural and urban addressing".

3 Definitions and abbreviations

3.1 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

NOTE 1: In a PLMN this is a radio access via a Base Station.

NOTE 2: c.f. (ITU-T Recommendation Q.931 [i.17], EN 300 403 [i.15], TS 124 008 [i.16]).

disaster: serious disruption of the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether developing suddenly or as the result of complex, long-term processes

disaster mitigation: measures designed to prevent, predict, prepare for, respond to, monitor and/or reduce the impact of, disasters

emergency: urgent need for assistance or relief

emergency call: call from a user to an emergency call centre, PSAP or similar agency charged with routing calls to the relevant emergency response organization

emergency call facilities: mechanisms provided by public or private communications networks, emergency telephone stanchions/boxes, fire alarms, etc. the use of which enables emergency calls to be made

emergency call service: mechanism by which a caller is given a fast and easy means of giving information about an emergency situation to the appropriate emergency organization (e.g. fire department, police, ambulance)

emergency caller: user who calls an emergency service by making an emergency call

emergency control centre: facilities used by emergency organizations used to accept and handle emergency calls forwarded from a PSAP

emergency number: special short code or number which is used to provide callers with immediate access to the PSAP to request assistance from the emergency services

NOTE: There are two different types of emergency numbers in Europe:

- 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 countries.
- National emergency numbers: each country may also have its own national emergency number and/or one or more numbers for alerting specific services.

emergency response organization: local or national force established to prvide assistance to citizens in the event of their being involved in an emergency situation and requiring specialised help, for example, the police, fire service and emergency medical services

emergency service: service 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 (Recommendation 2003/558/EC [14] and C(2003)2657 [14])

emergency situation: abnormal situation of serious nature that develops suddenly and unexpectedly, of which the evolution is uncertain and which may turn into a crisis or cause damage and casualties

enhanced 112 (**E112**): emergency communications service using the single European emergency call number, 112, which is enhanced with location information of the calling user (Recommendations 2003/558/EC [14] and C(2003)2657 [i.5])

enhanced 911 (E911) wireless service: a network based system that associates a physical address with the calling party's telephone number and routes the call to the most appropriate Public Safety Answering Point (PSAP) for that address, thus providing emergency call-takers with the location of the emergency without the person calling for help having to provide it

NOTE Wireless E911 program (in North America) is divided into two parts:

- Phase I requires carriers, upon valid request by a local Public Safety Answering Point (PSAP), to report the telephone number of a wireless 911 caller and the location of the antenna that received the call.
- Phase II requires wireless carriers to provide far more precise location information, within 50 metres to 300 metres in most cases.

health hazard: a sudden outbreak of infectious disease, such as an epidemic or pandemic, or other event posing a significant threat to human life or health, which has the potential for triggering a disaster

geoid: equi-potential surface of the Earth's gravity field which best fits, in a least squares sense, global mean sea level

location acquisition: process of a client device or application requesting, and receiving, location information from the Location Information Server (LIS)

Information 1): in a public mobile telecommunications network, the data processed indicating the geographic position of a user's mobile terminal, and

Information 2): in a public fixed network, data defining the physical address of the termination point. (Recommendation 2003/558/EC [14] and C(2003)2657 [i.5])

INVITE: SIP PDU that is sent by a terminal device asking for connection to another terminal or service

Mobility: ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment

NOTE: The degree of service availability may depend on several factors including the Access Network capabilities, service level agreements between the user's home network and the visited network (if applicable), etc. Mobility includes the ability of telecommunication with or without service continuity.

natural hazard: event or process, such as an earthquake, fire, flood, wind, landslide, avalanche, cyclone, tsunami, insect infestation, drought or volcanic eruption, which has the potential for triggering a disaster

next generation network: public, broadband, diverse and scalable packet-based network evolving from the public switched telephone network, intelligent network and Internet, characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence

nomadism: ability of the user to change his network access point

NOTE: When changing the network access point, the user's service session is completely stopped and then started again, i.e. there is no session continuity or hand-over possible. It is assumed that normal usage pattern is that users shutdown their service session before changing to another access point.

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

priority call: call that has been assigned some higher level of priority for processing by a telecommunications network such that it may be expected to achieve precedence over other traffic

priority service: provides for preferential treatment in the order of path selection in the network to calls originating from and/or addressed to certain numbers

Public Safety Answering Point (PSAP): physical location where emergency calls are received under the responsibility of a public authority (Recommendation 2003/558/EC [14] and C(2003)2657 [i.5])

REGISTER: SIP PDU that is sent by a terminal device to establish its presence and location on a network

relief operations: those activities designed to reduce loss of life, human suffering and damage to property and/or the environment caused by a disaster

roaming: ability of users to access services while outside of their subscribed home network, i.e. by using an access point of a visited network

NOTE: This is usually supported by a roaming agreement between the respective network operators.

telecommunication assistance: provision of telecommunications or other resources or support intended to facilitate the use of telecommunication resources

telecommunication resources: personnel, equipment, materials, information, training, radio-frequency spectrum, network or transmission capacity or other resources necessary for the reliable operation of telecommunications networks

telecommunications:any transmission, emission, or reception of signs, signals, writing, images, sounds or intelligence of any nature, by wire, radio, optical fibre or other electromagnetic system

user access: point of access to a telecommunication network from which a call can be requested. This includes public telephones and "emergency call facilities"

widespread outage: sustained interruption over a considerable area, of telecommunications services that will have strategic significance to government, industry and the general public

3.2 Abbreviations

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

3G	Third Generation
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
ADSL	Asymmetrical Digital Subscriber Line
ALE	Access Location Entity
ALI	Automatic Location Identification
ANP	Access Network Provider
ATIS	Alliance for Telecommunications Industry Solutions
BGCF	Border Gateway Control Function
CAEMS	Committee for the Advancement of Emergency Message Systems
CAMA	Centralized Automatic Message Accounting
CATV	CAble TV
CDMA	Code Division Multiple Access
CGALIES	Co-ordination Group on Access to Location Information for Emergency Services
CLI	Calling Line Identity or Calling Line Identification
CLIR	Calling Line Identity Restriction
CPN	Customer Private Network
CRC	Cyclic Redundancy Check
CS	Circuit Switch
CSCF	Call Session Control Function
DCITA	Department for Communications, Information Technologies and the Arts (Australia)
DECT	Digital Enhanced Cordless Telecommunications
DG INFSOC	(EU) Directorate Information Society
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DT	Deutsche Telekom
E2+/ESP	NENA enhanced Emergency Services Protocol at reference point E2
ECC	Emergency Control Centre
ECRIT	Emergency Context Resolution with Internet Technologies (IETF WG)
ECS	Emergency Call Server, or Electronic Communications Service
E-CSCF	Emergency-CSCF
EMTEL	EMergency TELecommunications
EPFL	Ecole Polytechnique Fédérale de Lausanne

ERDB	Emergency services zZone Routing DataBase
ESGW	Emergency Services GateWay
ESIF	Emergency Services Interconnection Forum
ESP	Emergency Services Protocol
ESP	Emergency Services Proxy

NOTE: DT Core IMS Architecture for Emergency Calling.

ESQK	Emergency Service Query Key
ESRN	Emergency Service Routing Number
ESRN	Emergency Service Routing Name
ETHZ	Eidgenössische Technische Hochschule Zürich
ETSI	European Telecommunications Standards Institute
FLAP	Flexible LIS-ALE Protocol
GEOPRIV	GEOgraphic location/PRIVacy (IETF WG)
GIS	Geographic Information System
G-NAF	Geo-coded National Address File (Australia)
GNSS	Global Navigational Satellite System
GPS	Global Positioning System
GSM	Global Standard for Mobile communication
HELD	HTTP-Enabled Location Delivery protocol
HFC	Hybrid Fibre-Coaxial
HTTP	Hyper Text Transfer Protocol
IBCF	Interconnect Border Control Function
I-CSCF	Interrogating CSCF
ID	IDentifier
IEPREP	Internet Emergency PREParedness (IETF WG)
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
INVITE	SIP PDU - See clause 3.1
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
ISO	International Standards Organization
ISP	Internet Service Provider
ISUP	Integrated Services digital network User Part
ITU-T	International Telecommunications Union - Telecommunications
L7LCP	Layer 7 Location Configuration Protocol (IETF GEOPRIV)
LAN	Local Area Network
LBS	Location Based Services
LCI	Location Configuration Information
LCP	Location Configuration Protocol
LCS	Location Configuration Server
LI	Location Information
LIE	Location Information Element (NENA «i2»)
LIS	Location Information Server
LIS-ALE	Location Information Server - Access Location Entity
LK	Location Key
LLDP-MED	Link Layer Discovery Protocol Media Endpoint Discovery
LREP-SIP	Location Reference Event Packages - Session Initiated Protocol
LRF	Location Retrieval Function
MGCF	Media Gateway Control Function
MGW	Media GateWay
MIC	Ministry of Internal affairs and Communications (Japan)
MLC	Mobile Location Client
MLP	Mobile Location Protocol
MSAG	Master Street Address Guide
MSN	Multiple Subscriber Number
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NENA	(US) National Emergency Number Association
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
NT	Network Termination

OMA	Open Mobile Association
PATS	Publicly Available Telephony Service
PAYG	Pay As You Go
PCRF	Policy and Charging Rule Function
P-CSCF	Proxy CSCF
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PIDF-LO	Presence Information Data Format - Location Objects
POTS	Plain Old Telephone Service
PSAP	Public Safety Answering Point
PSMA	Public Sector Mapping Agencies (Australia)
PSTN	Public Switched Telephone Network
RBP	Regional Broadband Provider
RDF	Routing Determination Function
REGISTER	SIP DPU - see clause 3.1
RELO	Retrieving End-system LOcation information
RFC	Request For Comment
S-CSCF	Serving CSCF
SDO	Standards Development Organization
SIP	Session Initiation Protocol
SME	Small and Medium Enterprise
SMS	Short Message Service
SOHO	Small Office/Home Office
SPA	Self-Positioning Algorithm
SS7	Signalling System No 7
SUPL	Secure User Plane Location
TDD	Telecommunications for Deaf and Disabled
TDM	Time Division Multiplexing
Tel URI	Telephone URI
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TOA	Time Of Arrival
TTY	TeleTYpe
TV	TeleVision
UE	User Equipment
URI	Uniform Resource Identifier
URL	Universal Resource Locator
UTC	Coordinated Universal Time
VDB	Validation DataBase
VDSL	Very high-speed Digital Subscriber Line
VEP	VoIP End Point
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Centre
VPN	Virtual Private Network
VSP	VoIP Service Provider
WGS84	World Geodetic System 1984
Wi-Fi	Wireless Fidelity

NOTE: Synonymous with WLAN with IEEE 802 Technology

WiMAX	Worldwide Interoperability for Microwave Access (IEEE 802.16x)
WLAN	Wireless LAN
WPS	WLAN Positioning System
XML	eXtensible Markup Language
XPS	Hybrid Positioning System

4 Introduction

4.1 Emergency Response Principles

There are several different mechanisms used for making emergency calls; these depend on the local regime, both from the telecoms network point of view and the way in which the emergency responses services are organized. Essentially, there are two approaches. In the first, a single emergency number can be called (for example 112 in Europe) irrespective of the nature of the emergency. A PSAP call taker then determines the nature of the emergency and its location from the caller and connects the call to the relevant ECC. This is the "one emergency call number" approach. In the second approach, the caller has to decide from the nature of the emergency which service to call and dial a specific number which connects directly to the ECC serving the callers area. This is the "Service Specific Call Number" approach.

The single number approach lends itself to centralization particularly where the caller's location can be determined automatically. It can also provide the ability to trigger responses from several emergency services, for example in the case of a road accident. The specific number approach can be confusing to callers, particularly where the numbers are different in different towns within a country.

Call routing and connection is beyond the scope of the present document, as are any local, regional or national variations in the processes used.

4.2 One emergency call number

The emergency response principle intended with a single emergency call number (e.g. «112») is illustrated in figure 1. The single emergency number concept implies that any given locality is served by a single PSAP providing connectivity for callers to any of the emergency response services available in that locality (but see the further explanation below).

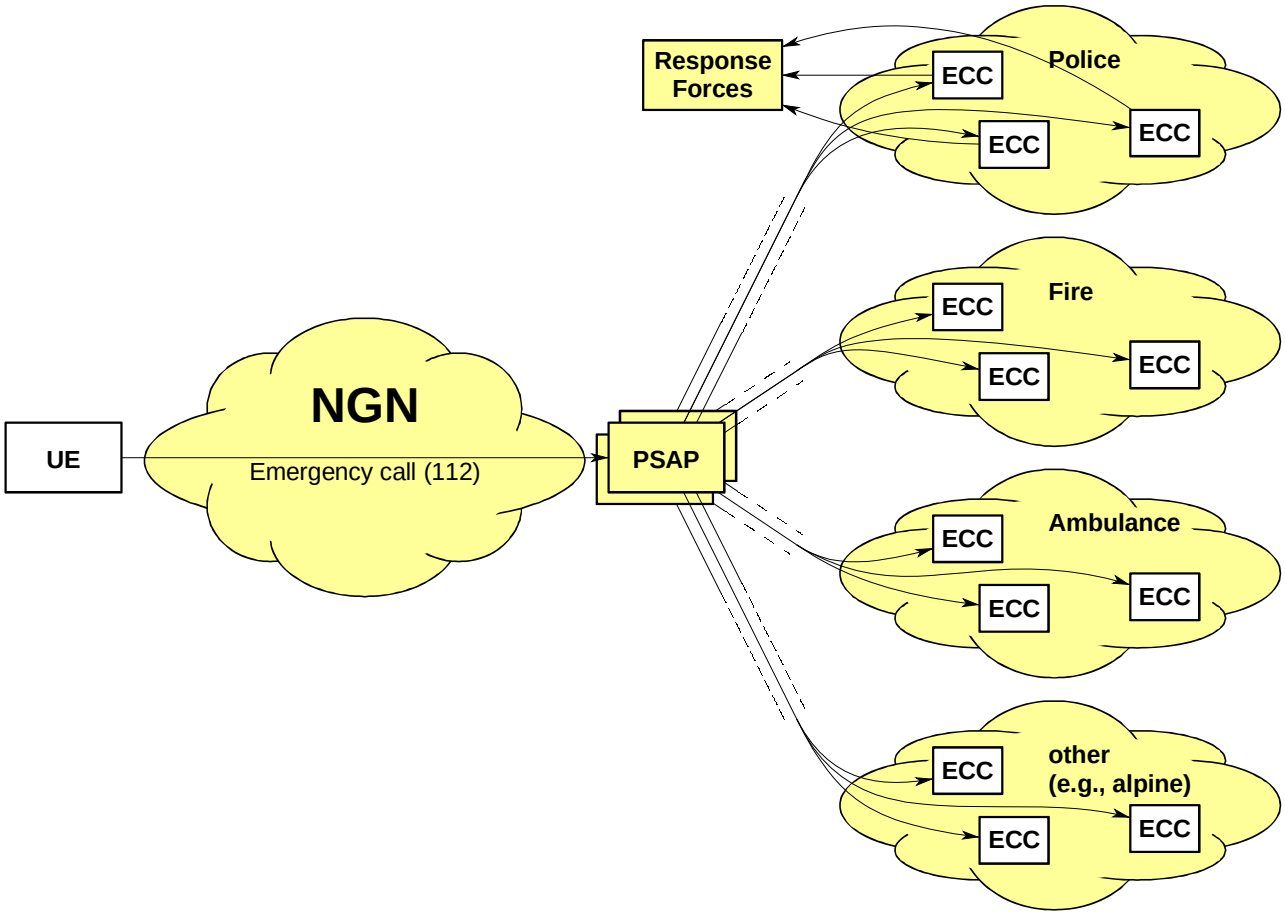


Figure 1: "One-number" Emergency response principle

A "single-number" PSAP may cover any defined area, ranging from a small town to an entire country. This depends only upon the national operating philosophy. Where several "one-number" PSAPs are deployed within a country, their geographical distribution and the areas covered are usually dependent on such factors as language preference or local administrative boundaries.

A single PSAP may be divided between several physical locations to provide system resilience, calls being distributed between the locations with regard only to their capacity to handle the traffic.

Emergency calls are routed by the network operator to the appropriate PSAP where the call is answered by a call taker.

The function of the PSAP is to provide the initial response to all emergency calls originating within its designated area, irrespective of the service for which they are intended. The PSAP call-taker first determines which emergency service is required, and then forwards the call to the appropriate emergency service despatch centre (ECC). The PSAP call taker will usually verify that the call has been answered by the ECC operator and may also perform such tasks as further assistance with caller location, alerting other ECCs to the emergency, etc. These operational issues are outside the scope of the present document.

The ECC operator may need to obtain more accurate emergency location information from the caller. With enough information, the operator decides what resources to despatch. In some countries the functionalities of PSAP and ECC are combined and/or where the PSAP/ECCs are organized by geographical areas, e.g. counties, districts, communities, etc. These, and such issues as the handling of calls from disabled users via relay systems, TDD/TTY and such like, are operational issues and outside the scope of the present document.

Where the "one-number" principle is used, there is only a limited necessity for the network operator to make a decision about location dependent call routing and no need for the caller to make the decision as to which service is required.

4.3 Service specific emergency call numbers

The emergency response principle using service specific emergency call numbers, for example, one number for the police, another for ambulance, etc., requires the emergency caller to make the first decision as to which emergency service to contact. This principle is generally deployed on a local basis with the responsibility for calls being routed to the appropriate facility being that of the network operator, with a clear possibility of errors occurring, such as when the network boundaries do not correspond with emergency service boundaries. In most such arrangements, the functionality of PSAP and ECC are combined (see figure 2) though each emergency service covering the area will usually have its own functional PSAP/ECC, even if these are co-located.

If the call was initially directed to the wrong service, either by the caller or the network operator, the PSAP/ECC will usually have the means to forward the call directly to a more appropriate emergency service or location, though this will clearly cause some delay.

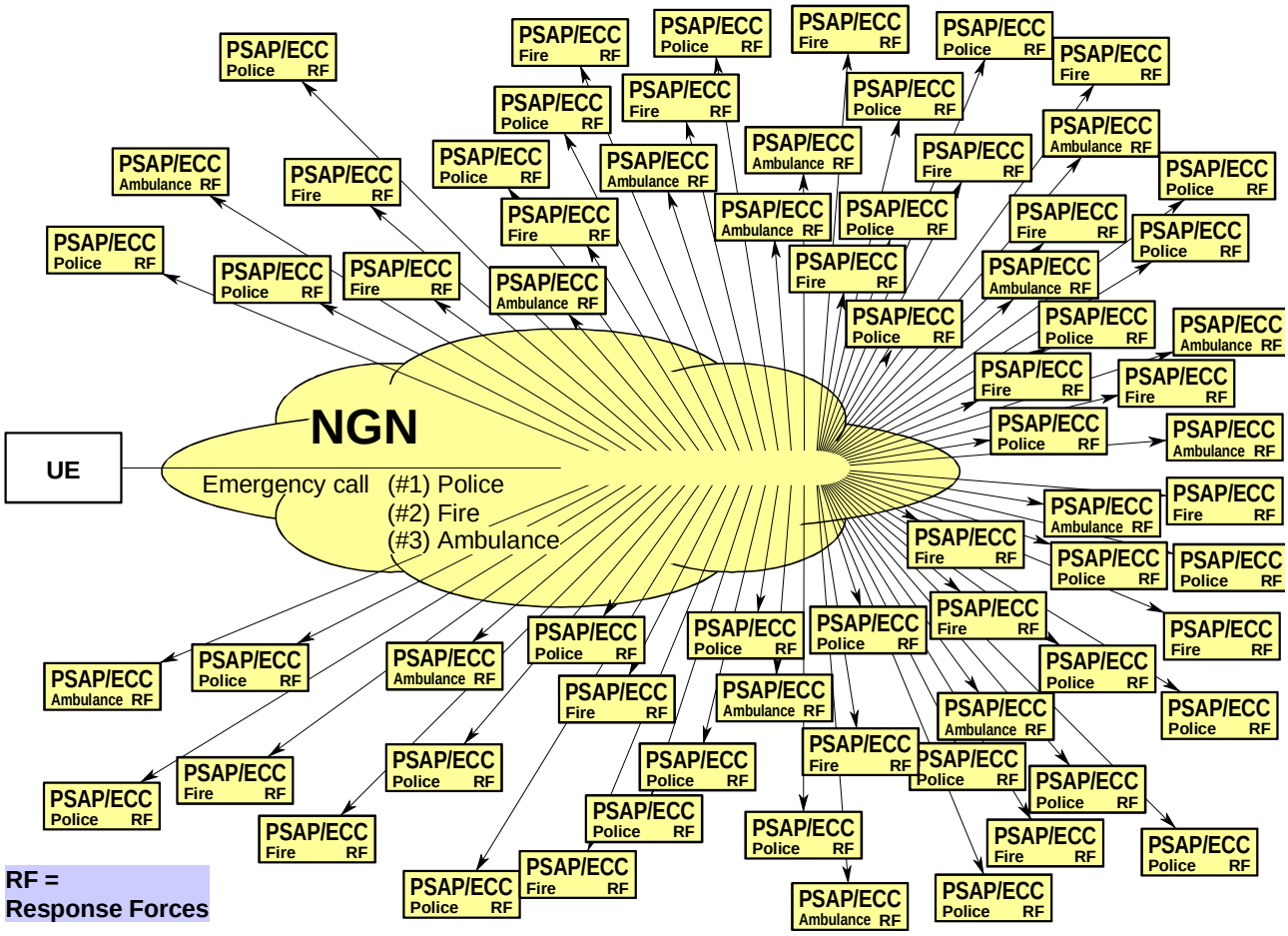


Figure 2: Emergency response principle with emergency service dependent call numbers

4.4 Use of the Location Information

There are three phases of an emergency call, all of which have different requirements for the accuracy of any location information which may be provided:

- Initial call routing, that is the routing of the call to the correct PSAP or ECC.
- Routing of the call for the purpose of dispatch, that is to trigger the dispatch the most appropriate emergency response team; and
- Finding the precise location of the caller and/or incident site by the emergency response team.

Where for the most emergency calls on the fixed network location accuracy is not an issue, in networks using mobile or nomadic terminals accurate location information is vital and may be difficult to obtain. The accuracy requirements are discussed below.

4.4.1 Call routing

Emergency calls in most countries are handled at centralized facilities which may cover areas ranging from single villages to whole countries. It is important that callers are connected to the facility designated to handle calls from their area. For call routing the following accuracies on the location information are usually sufficient:

	Rural	Suburban	Urban	Dense Urban	Indoor
Mobile and nomadic calls	< 35 km	< 10 km	< 1 km	< 1 km	< 1 km

It is usual that arrangements are in place for the rapid transfer of calls arriving at an inappropriate answering point, for example, due to the caller being close to a boundary. Special considerations may need to be given when emergency calls originate close to an international boundary. In some cases, mobile terminals may be roamed to base stations in another country thus adding to the potential for location ambiguity.

4.4.2 Dispatching

The accuracy requirements for dispatching are similar to those for call routing but with the added consideration of geographical obstacles, such as mountain ranges, rivers, lake shores, etc. or on which side of a highway the incident has occurred.

The location information could also be used to recognize that several emergency calls are for the same incident (emergency call clusters). In this case, the accuracy requirements of the location information are as follows:

	Rural	Suburban	Urban	Dense Urban	Indoor
Emergency call cluster detection	< 500 m	< 500 m	< 150 m	< 150 m	< 150 m

It is usual for emergency response teams to co-operate with neighbouring authorities in the event of their being incorrectly despatched, for example, due to the caller being close to a boundary. As above, special considerations may need to be given when emergency calls originate close to an international boundary.

4.4.3 Locating

Finding the caller or the incident can initially be based on any location estimate available from the communications network (see clauses 4.4.1 and 4.4.2) and may be refined by information provided directly by the caller. There are three possible cases:

1) no location estimate is provided by the network but the caller provides location information which appears to be sufficiently accurate to despatch emergency response personnel, though this information must be considered as unverified;

2) a location estimate is available from the network and the caller is able to provide additional information. If the caller's information corroborates the network estimate within the accuracy requirements for call clusters (see clause 4.4.2), the location may be considered as verified;and

3) if a location estimate is available from the network but the caller is unable to provide further location information, the need for accuracy of the network provided information becomes more stringent, as follows:

	Rural	Highway	Suburban	Urban	Indoor
Caller provides location information	50 m to 100 m	20 m to 100 m	30 m to 100 m	10 m to 50 m	10 m to 50 m
Caller provides no information	10 m to 100 m	10 m to 100 m	10 m to 100 m	10 m to 50 m	10 m to 50 m

The location information from the network should be available within a few seconds after call initiation, not least to enable its timely corroboration by the caller.

4.5 Location Information

Location information can be presented in one of two formats: Geodetic or civic.

Geodetic location information refers to a standardized coordinate system whereas civic location information reflects the postal address system, possibly augmented for emergency application with additional information, e.g. floor level.

Geodetic location information is by definition unambiguous; it is based on a specified grid of latitudes, longitudes and elevations.

Civic location information is presented in a variety of structures in different areas, depending on local practice, and might not be amenable to be cast into a common data structure. In addition, the information can be inaccurate, imprecise, incomplete, etc. Hence, before civic location information is presented to the PSAP, it needs to be validated by the Master Street Address Guide (MSAG) or some similar facility available to the PSAP.

4.5.1 Geodetic locating information

Geodetic locating information is based on a geocentric model abstracting the earth. It is geodetic practice, contrary to the mathematical convention, to let the x-axis point to the North and the y-axis to the East.

4.5.1.1 X and Y coordinates

The X-coordinate represents the latitude and is described by a real number. The precision provided by GPS is to six decimal places reflecting a resolution of approximately 10 cm. The values lie within the range -90 to +90 degrees. Positive numbers indicate locations north of the equator.

The Y-coordinate represents the longitude and is described by a real number. The precision provided by GPS is to six decimal places reflecting a resolution of approximately 10 cm at the equator. The values lie within the range -180 to +180 degrees. Positive numbers indicate locations east of the prime meridian (Greenwich).

4.5.1.2 Z coordinate

For engineering purposes, the height of a point in metres above the mean sea level is generally used. Mean sea level is represented by a hypothetical construct called a "geoid". The geoid is essentially the figure of the Earth abstracted from its topographic features. It is an idealized equilibrium surface of sea water (the mean sea level) taking into account all local gravity variations and in the absence of currents, air pressure variations, etc. and is continued under the continental masses. The geoid, unlike the ellipsoid, is irregular and too complicated to serve as the computational surface on which to solve geometrical problems such as point positioning.

GPS provides height information in metres above an ellipsoid. This reference ellipsoid, customarily chosen to have the same volume as the geoid, is described by its semi-major axis (equatorial radius) a and flattening f.
The quantity f = (a-b)/a, where b is the semi-minor axis (polar radius), is a purely geometrical one. The mechanical ellipticity of the earth (dynamical flattening) is determined to high precision by observation of satellite orbit perturbations.

The geometrical separation between the reference ellipsoid and the geoid is called the geoidal undulation. It varies globally between ±110 m, hence may be significant in determining the vertical elevation of a point.

The schematic diagram in figure 3 shows some of the "level surfaces" of the Earth, including the geoid, and their relation to the Earth's crust and local mean sea level.

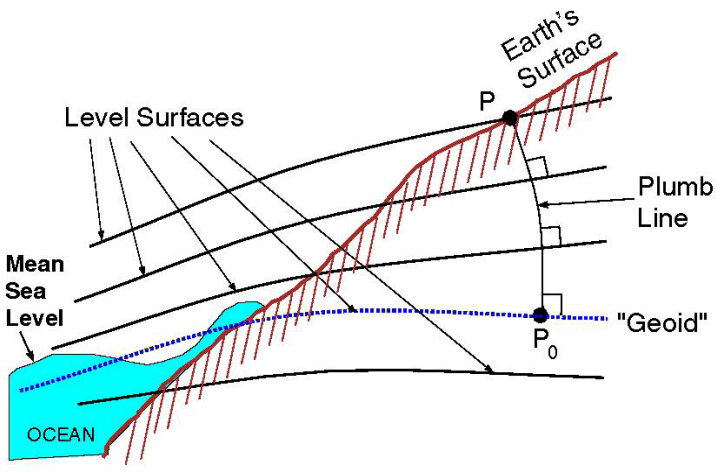


Figure 3: Orthometric height

Figure 4 is a schematic diagram showing the relationship between the geoid, orthometric heights and ellipsoid.

NOTE: The ellipsoid is drawn above the geoid and that it does not coincide with any level surface, but rather cuts across them. This is because the ellipsoid is a geometric invention, and not defined by the actual gravity field of the Earth itself.

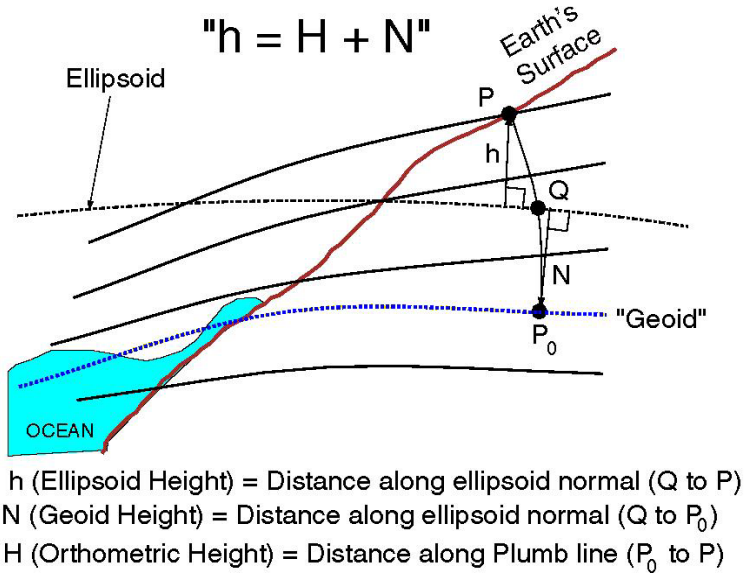


Figure 4: Ellipsoid and orthometric height

For emergency purposes, neither orthometric nor ellipsoidal height is of much value; height above (average) ground level is required. On the other hand, either orthometric or ellipsoid height of average ground can be kept in local databases in a sufficiently narrow mesh such that the determination of the height of a point above ground level can be by a database lookup and a subtraction.

Unlike latitude and longitude, which are internationally agreed, the value for mean sea level used for national mapping is usually determined by the country concerned. GPS uses the WGS84 standard world-wide. Hence there may often be a discrepancy between the GPS Z-coordinate for a particular point and the value shown on a national map. In addition, mapping overlap between adjacent countries may also have differing Z-coordinates due to the differing reference sea levels used. The database lookup mentioned in the previous paragraph should be able to deal with this idiosyncrasy. In addition, different sea level references are no longer an issue as the height of the terrain above the standardized WSG84 ellipsoid is utilized with GPS.

4.5.2 Civic locating information

Civic locating information takes a similar format to a postal address, however, additional informational or vanity fields such as company names, job titles or professional credentials might be included, none of which is strictly necessary to identify the location. In figure 5 two extreme examples can be found.

Detailed	**Adequate**
Dr. med. dent. David M. Newfield Deputy Director Room 488 Dental Tools Ltd. Silver Tower North 4623 E Lower Broadway NW Great Falls, MT 12345-6789 U.S.A.	Rolf Schmidt Wässeristrasse 34 CH-8340 Hinwil

Figure 5: Examples of civic addresses

4.6 Coding principles for location information

Three different coding principles for location information are shown in this clause:

- Specific field definitions with binary values.
- Rigorously structured field definitions with textual information.
- Loosely structured field definitions with textual information.

4.6.1 Specific field definitions

In RFC 4676 [i.8] the information element as shown in figure 6. The "what" field indicates what the location designates (DHCP server, network element believed to be closest to the client, or client itself), the country code is coded according to ISO-3166-1's two letter country code [5], and the civic address elements are a sequence of elements as indicated in table 1 (see clause 4.6.2).

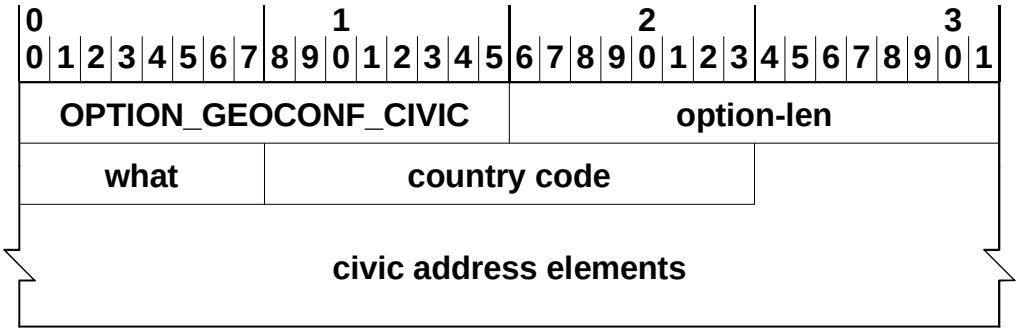


Figure 6: The DHCPv6 civic address option (Example)

For geodetic location information, RFC 3825 [8] defines the following Information element. Latitude, Longitude, and Altitude are fixed decimal point real values, LaRes, LoRes, and AltRes indicate the accuracy of the values. The datum designates the particular international Earth coordinate system, e.g. WGS84 [6].

The parameters LaRes, LoRes, and AltRes can be used to indicate a volume of space.

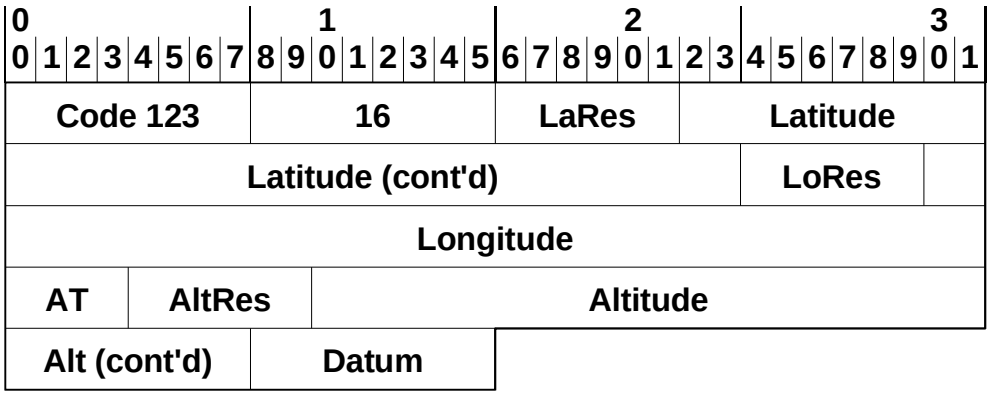


Figure 7: Location Configuration Information (LCI) Elements (Example)

4.6.2 Rigorously structured field definitions

The following example of an XML structure assumes the presence of the civic address fields as shown in table 1.

Table 1: Civic address structure (North America)

Label	Description	Example
country	The country is identified by the two-letter ISO 3166 code [5]	US
A1	national subdivisions (state, region, province, prefecture)	New York
A2	county, parish, gun(JP), district (IN)	King's County
A3	city, township, shi (JP)	New York
A4	city division, borough, city district, ward, chou (JP)	Manhattan
A5	neighbourhood, block	Morningside Heights
A6	street	Broadway
PRD	Leading street direction	N, W
POD	Trailing street suffix	SW
STS	Street suffix	Avenue, Platz, Street
HNO	House number, numeric part only.	123
HNS	House number suffix	A, ½
LMK	Landmark or vanity address	Low Library
LOC	Additional location information	Room 543
FLR	Floor	5
NAM	Name (residence, business or office occupant)	Joe's Barbershop
PC	Postal code	10027-0401
BLD	Building (structure)	Hope Theatre
UNIT	Unit (apartment, suite)	12a
ROOM	Room	450F
PLC	Place-type	Office
PCN	Postal community name	Leonia
POBOX	Post office box (P.O. box)	U40
ADDCODE	Additional Code	13203000003
SEAT	Seat (desk, cubicle, workstation)	WS 181
RD	Primary road or street	Broadway
RDSEC	Road section	14
RDBR	Road branch	Lane 7
RDSUBBR	Road sub-branch	Alley 8
PRM	Road pre-modifier	Old
POM	Road post-modifier	Extended

Figure 8 shows the XML structure extracted from RFC 4119 [10] and figure 9 shows a coding example from the same source.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:tns="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

<xs:import namespace=
     "urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy" />

   <!-- This import brings in the XML language attribute xml:lang-->

   <xs:import namespace="http://www.w3.org/XML/1998/namespace"
     schemaLocation="http://www.w3.org/2001/xml.xsd"/>

   <xs:element name="geopriv" type="tns:geopriv"/>

<xs:complexType name="geopriv">
 <xs:sequence>
   <xs:element name="location-info" type="tns:locInfoType"
      minOccurs="1" maxOccurs="1"/>
   <xs:element name="usage-rules" type="gbp:locPolicyType"
      minOccurs="1" maxOccurs="1"/>
   <xs:element name="method" type="tns:locMethod"
      minOccurs="0" maxOccurs="1"/>
   <xs:element name="provided-by" type="tns:locProvidedBy"
      minOccurs="0" maxOccurs="1"/>
   <xs:any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
 </xs:sequence>
</xs:complexType>

<xs:complexType name="locInfoType">
 <xs:sequence>
   <xs:any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
 </xs:sequence>
</xs:complexType>

<xs:complexType name="locMethod">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute ref="xml:lang" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="locProvidedBy">
 <xs:sequence>
   <xs:any namespace="##other" processContents="skip"
      minOccurs="1" maxOccurs="unbounded"/>
 </xs:sequence>
</xs:complexType>

</xs:schema>
```

Figure 8: XML structure of civic address

```
<?xml version="1.0" encoding="UTF-8"?>
 <presence xmlns="urn:ietf:params:xml:ns:pidf"
    xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
    xmlns:cl=" urn:ietf:params:xml:ns:pidf:geopriv10:civicLoc"
    entity="pres:geotarget@example.com">
  <tuple id="sg89ae">
   <status>
    <gp:geopriv>
      <gp:location-info>
        <cl:civicAddress>
          <cl:country>US</cl:country>
```

Figure 9: Example XML structured data (Part 1)

```
          <cl:A1>New York</cl:A1>
          <cl:A3>New York</cl:A3>
          <cl:A6>Broadway</cl:A6>
          <cl:HNO>123</cl:HNO>
          <cl:LOC>Suite 75</cl:LOC>
          <cl:PC>10027-0401</cl:PC>
        </cl:civicAddress>
      </gp:location-info>
      <gp:usage-rules>
        <gp:retransmission-allowed>yes</gp:retransmission-allowed>
        <gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
      </gp:usage-rules>
    </gp:geopriv>
   </status>
   <timestamp>2003-06-22T20:57:29Z</timestamp>
  </tuple>
 </presence>
```

Figure 9: Example XML structured data (Part 2)

4.6.3 Loosely structured field definitions

Figure 10 shows an example of a loosely structured location information. One or more names are separated from one or more general address lines; the fields for town, zip code, and country are distinguishable. The ISO-3166-1 [5] standard two letter country code gives an unambiguous, short and well known value to designate the country.

```
name=Adalbert H. Miller
name=Adelheide Roslin
a=Silver Tower
a=Floor 15
a=411 Lower Riverside Ave
town=Ottawa
zip=Ont. Q3X 4T0
country=CA
```

Figure 10: Loosely structured location information (Example)

4.6.4 Comparison of field definitions

All three coding principles for location information can be shown to have both advantages and disadvantages:

a) Specific field definitions with binary values can be rigorously defined in a format that is easily machine readable, and easily indexed but are not easily read by humans. This format may make it difficult to enter some addresses, for instance those having long street names or optional district identifiers.

b) Rigorously structured field definitions with textual information, tends to lead to a great many optional and vanity fields, leading to them being unused in many cases. This makes data entry problematic and is likely to lead to errors, even when the unused fields are flagged as optional.

c) Loosely structured field definitions containing textual information are the easiest to read by humans and if limited in their application to a reasonably small number fields should overcome most of the difficulties potentially associated with the two previous cases.

If it is assumed that emergency responses are relatively local and that the civic location information is prepared by trained personnel, a heavily detailed structure such as that shown in clause 4.6.2 might not be necessary. Since, address formatting is extremely variable, both nationally and internationally. This would lead to the likelihood that the number of fields, their size, definition and usage needing to be left as an issue for national or even local resolution.

A closely defined and well structured information format is essential where the data is to be processed by Geographic Location Information Systems as is likely to be the case in the present application. Loosely structured fields will almost inevitably lead to problems for this regard.

Clearly, standardization is necessary for the address data interfaces since it is impossible to provide an individual solution for every local PSAP or address structure. This is an area which, equally clearly, requires further study.

4.7 Conversion of location information

4.7.1 Geodetic to map

The mapping of geodetic location information to a map is demonstrated with the ubiquity of personal navigation devices and a well developed technique. For emergency purposes, the accuracy of satellite images and the streets only map information as available for example via Google map is not sufficient. On the other hand, more detailed maps for the emergency response teems can be derived from local GISs.

It may be the case that the local GIS and the maps derived from it are based on a legacy coordinate system. In this case, the geodetic coordinates must first be transformed into the local coordinate system before the map can be displayed. Such a transformation often follows formulas used with Mercator Projections.

This mapping is useful whenever a human operator is in the stream of decision-making, how best to answer to an emergency. It might also be useful in situations where emergency call clusters may need to be detected by human interventions.

4.7.2 Geodetic to area

The boundary of an area is traditionally approximated by a polygon. Determining whether a point represented by coordinates is inside or outside the polygon is a common problem in computer graphics and easily mastered. There might be a need to apply the same coordinate transformation mentioned in clause 4.7.1.

NOTE: In computer graphics, objects are often approximated by a network of polygons. For ray tracing computations, the computation needs to determine which polygon is hit by a particular ray and in which direction the ray is reflected; this is a computation in three dimensions. For the needs of geodetic information to an area a two dimensional computation suffices.

The computation to derive in which area of a patchwork of areas a coordinate point resides might also be useful for routing and ECC selection as well.

4.7.3 Geodetic to civic

One possibility to solve the mapping of geodetic location information to civic location information could be via the entry of a polygon in the civic address database.

4.7.4 Civic to geodetic

The mapping of civic location information to geodetic location information is achieved by storing a geodetic location in the database with the civic address entry; the geodetic location might indicate the principal entry, for example.

4.7.5 Civic to map and civic to area

The problem of mapping a civic location to a map and/or an area is most easily performed by first converting the civic information into a geodetic location information and then performing the functions described in clauses 4.7.1 and 4.7.2.

5 Categories of impact on location information

5.1 Mobility

The mobility categories are listed in table 2.

Table 2: Mobility categories

Category	Attachment	Hand-over	Access provider	Responsibility
1) wired	wired	N/A	N/A	TISPAN
2) wireless	wireless	not supported	home network	TISPAN (3GPP)
3) nomadic wired	wired	not supported	visited network	TISPAN
4) nomadic wireless	wireless	not supported	visited network	TISPAN (3GPP)
5) mobile	wireless	supported	home	3GPP
6) roaming	wireless	supported	visited network	3GPP

The terms "nomadism", "mobility", and "roaming" are defined in TR 180 000 [15] and reflected in clause 3.1.

1) Wired:
This category represents the situation where the UEs are not moved or stay within the accuracy requirements discussed in clause 4.4 (i.e. limited by the length of the attachment cable).

2) Wireless:
This category represents the situation where the UEs are attached to the **home** network, for example, using Wi-Fi or DECT technology.

3) Nomadic wired:
This category represents the situation where the UEs are attached to a **visited** network via a cable, for example, Ethernet.

4) Nomadic wireless:
This category represents the situation where the UEs are attached to a **visited** network, for example, using Wi-Fi or DECT technology.

5) Mobile:
This category represents the situation where the UEs are operating in the **home** network using a recognized mobile communications technology.

6) Roaming:
This category represents the situation where the UEs are operating in a **visited** network using a recognized mobile communications technology.

5.2 UE attachment

The UE attachment categories are listed in table 3.

Table 3: UE attachment categories

Category	Comment
1) wireline	static
2) Wi-Fi / DECT	wireless, reach indoors typically ~ 30 m in ideal conditions ~ 300 m
3) Tunnel	point-to-point

1) Wireline:
The wireline UE attachment is a static situation, the UE is capable of moving only up to the length of the cord. This is even in extreme cases within the accuracy requirements of the PSAPs and ECCs.

2) Wi-Fi/DECT:
Wi-Fi and DECT technologies are both wireless attachment methods. The reach of the wireless part of the attachment is in both cases within the accuracy requirements of the PSAPs and ECCs, i.e. movement of the UE is irrelevant for the purpose of the emergency location. For the discussion of emergency location there exists no need to distinguish between Wi-Fi and DECT.

3) Tunnel:
The attachment of a UE via a tunnel, e.g. VPN tunnel, is comparable with any other UE attachment, except that it can be located anywhere having appropriate connectivity. At different times, the far end of the tunnel may be at different (geographically widely separated) locations. The tunnel is transparent in the sense that the information is simply transported; it is not interpreted or changed in any way, nor does either end of the tunnel need to have any information about the geographical location of the other end.

5.3 CPN Architecture

The CPN Architecture types are listed in table 4. The table shows the different categories and their classification depending on:

- The number of access network providers (ANP);
- The boundary of the different network attachments to be within or beyond the accuracy requirements of the PSAPs and ECCs (NT Spread); and
- The boundary of the different UEs to be within or beyond the accuracy requirements of the PSAPs and ECCs (UE Spread).

Table 4: CPN Architecture categories

Category	ANP	NT Spread	UE Spread
1) CPN non-existent	one	single	within accuracy
2) CPN / one geographical area	one	within accuracy	within accuracy
3) CPN / different geographical areas	one	within accuracy	beyond accuracy
4) CPN / multi-homing, different areas	one	beyond accuracy	beyond accuracy
5) CPN / multiple access providers, one area	multiple	within accuracy	within accuracy
6) CPN / multiple access providers, different areas	multiple	beyond accuracy	beyond accuracy

1) CPN non-existent:
This category represents the typical traditional attachment of UEs directly to an NT. Multiple UEs may be attached to the NT, nevertheless, there exists no switching functionality to allow direct communication between those UEs. All UEs are located within the accuracy requirements of the PSAPs and ECCs (see figure 11).

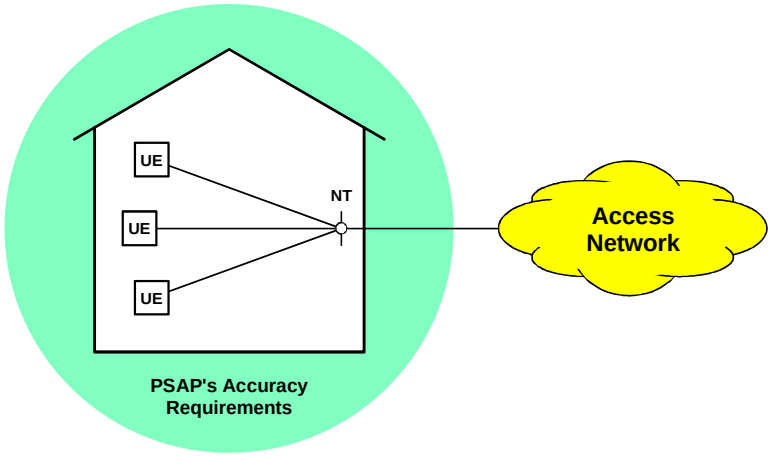


Figure 11: Example CPN category 1

2) CPN / one geographical area:
This category represents local area networks typically present in residential or SME situations; these LANs allow communication among the different UEs. All UEs are located within the accuracy requirements of the PSAPs and ECCs (see figure 12).

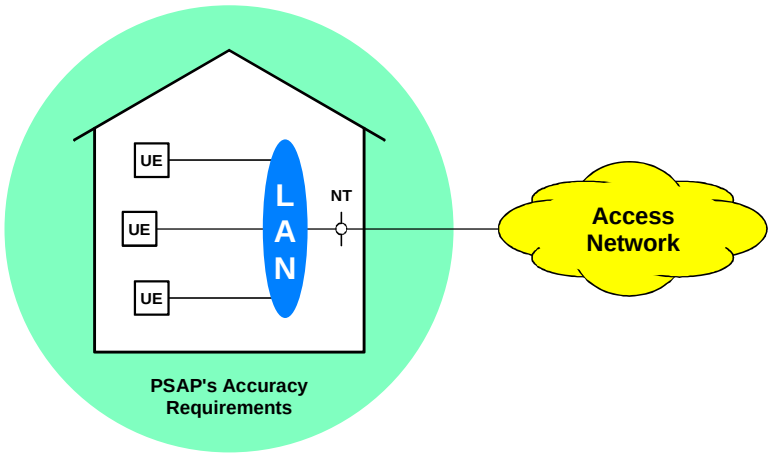


Figure 12: Example CPN category 2

3) CPN / different geographical areas:
This category represents local area networks in larger complexes where one access network provider uses one or more NTs for the LAN attachment all within the accuracy requirements of the PSAPs and ECCs. On the other hand, the UEs are spread beyond the accuracy requirements of the PSAPs and ECCs, e.g. in multiple buildings (see figure 13).

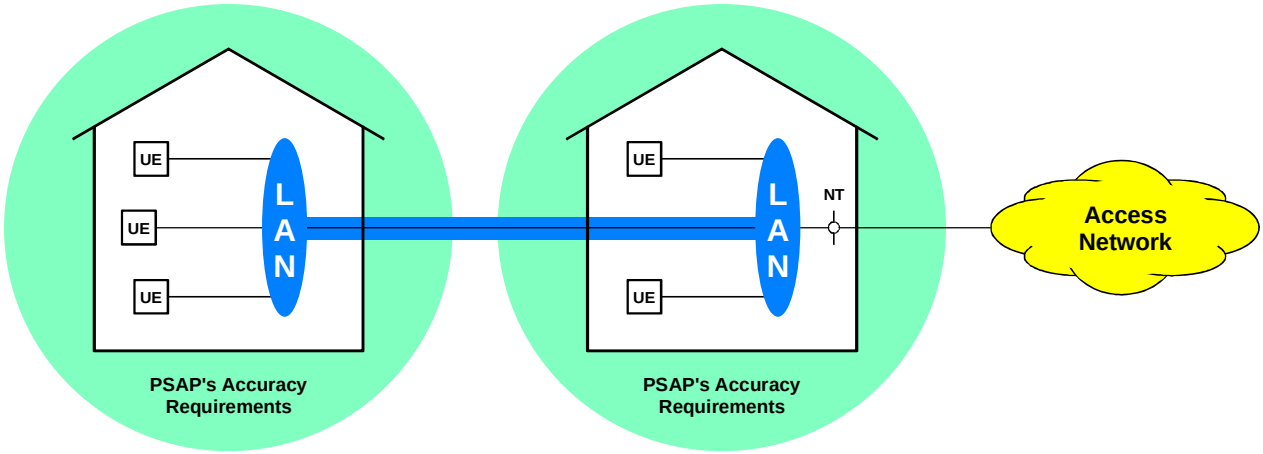


Figure 13: Example CPN category 3

4) CPN / multi-homing, different areas:
This category represents local area networks for corporations that consist of offices dispersed for example throughout a country. One access network provider realizes LAN attachments at more than one location and those NTs are spread beyond the accuracy requirements of the PSAPs and ECCs, e.g. in widely separated offices (see figure 14).

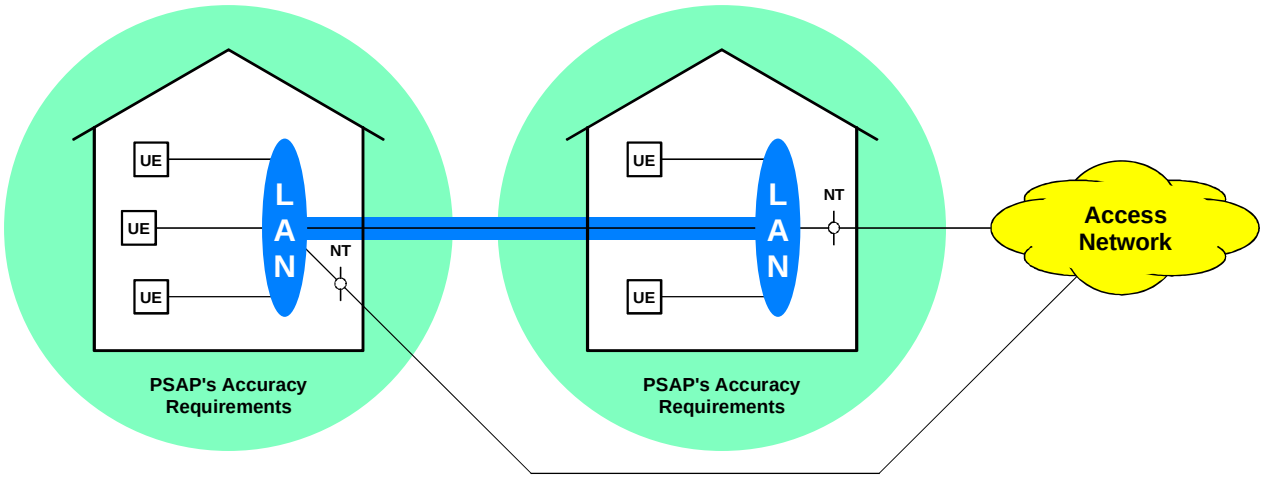


Figure 14: Example CPN category 4

5) CPN / multiple access providers, one area:
This category represents local area networks similar to category 4 above. The NTs, however, represent attachments from different access network providers; this may augment the fail-safe capability of the attachment (see figure 15).

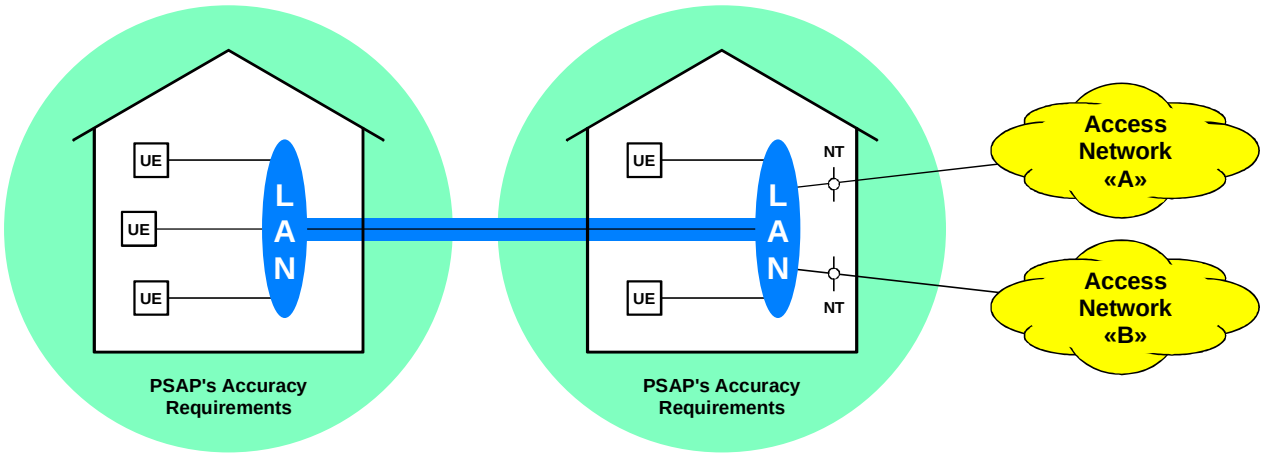


Figure 15: Example CPN category 5

6) CPN / multiple access providers, different areas:
This category represents local area networks similar to category 5 above. The NTs, however, represent attachments from different access network providers. Such different attachments might be required if the "local" network crosses international boundaries or be required for an augmented fail-safe capability (see figure 16).

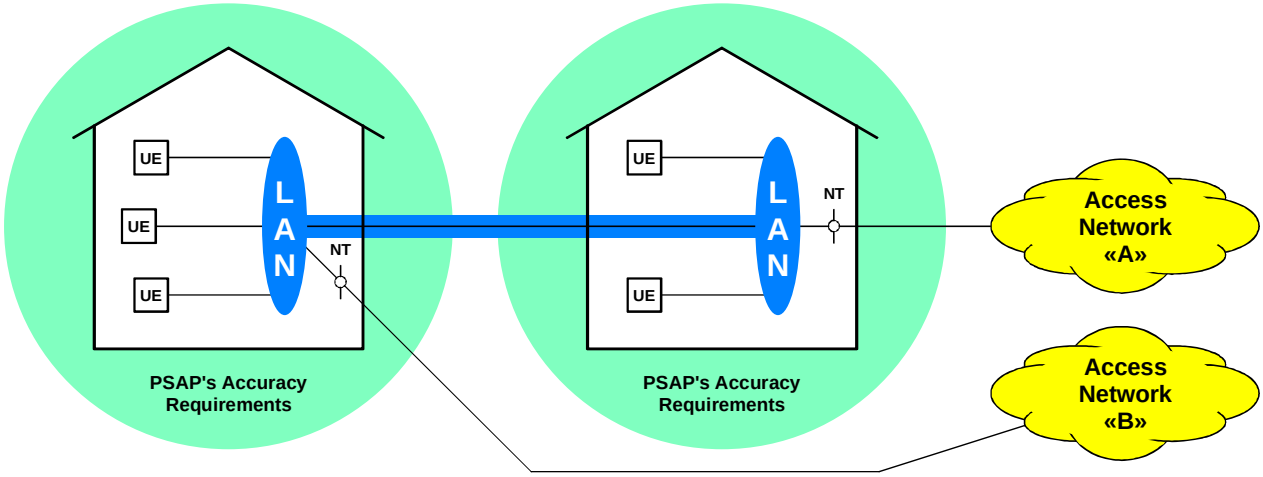


Figure 16: Example CPN category 6

5.4 Location information

The location information categories are listed in table 5.

Table 5: Location information categories

Category	Comment
1) User Equipment	maintained by GNSS client capability
2) Wi-Fi Access Point / DECT Base Station	aintained by CPN administration and DHCP Relay Agent Information
3) Network Termination	maintained by access provider
4) Network Termination WiMAX/Cable (CATV)	maintained by access provider

1) User Equipment:
If the UE is enabled with a GNSS client capability, this is the most accurate location available for the origin of the emergency communication. In addition, it can also provide accurate speed and direction of movement of the caller.

2) Wi-Fi Access Point/DECT Base Station:
Where the location of a DECT base can be maintained by the same procedures as the location of wireline endpoints, the Wi-Fi Access Points require the support of the DHCP Relay Agent Information Option [7] and the option for Location Configuration Information [8] and [9]. In addition, if the UE knows its location (GNSS or DHCP provided), it should insert this Location Information in its communication with the PSAP.

NOTE: If all UEs are located within the accuracy requirements of the PSAPs and ECCs (see 2) in clause 5.3) the specific locations of Wi-Fi Access Points and DECT Bases need not be maintained nor determined at DHCP request time.

3) Network Termination and CATV:
The location information of the NT, the WiMAX client, and the cable modem are maintained by the access provider similar to the maintenance of wireline terminations. This information could be made available for retrieval by E-CSCF, PSAP, and/or ECC.

6 Cascading networks

6.1 Direct attachment to NGN access networks

Figure 17 shows nomadic UE attachment (hotspot) and attachments to SOHO networks. Typically, the UEs are located close enough to the hotspot base station or the DSL router to be within the accuracy requirements of the PSAP/ECC organizations.

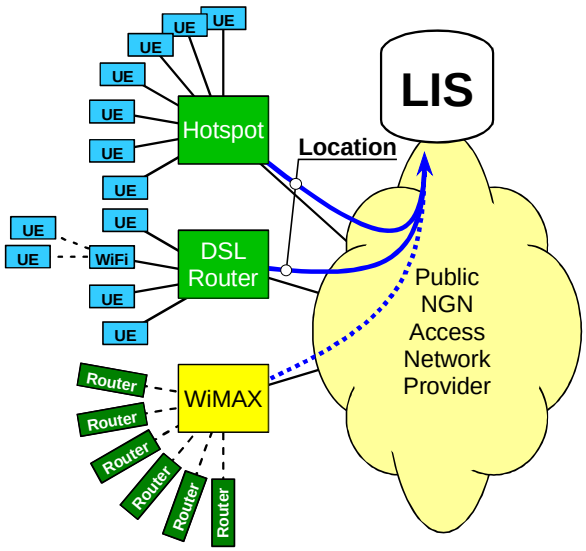


Figure 17: Direct attachment to NGN access networks

Access network hotspots are at known locations like the telephones in the POTS; these locations must be made known to the LIS (Location Information Server). The UEs' locations are within the reach of the hotspots' radio signals and, therefore, within the accuracy requirements of the PSAP/ECC organizations.

The DSL routers discussed in this clause are those serving residential direct attachments and/or in house networks. These DSL routers with fixed IP addresses are similarly configured as the hotspots and the UEs are located within the accuracy requirements of the PSAP/ECC organizations. Even if a WLAN technology is included in these small networks, the accuracy requirements are still satisfied.

ISPs are required to associate assigned IP addresses with the location of NTs (DSL routers, access points, etc.) and, depending on local regulation, keep this association available even after its dissociation. The currently active associations and the possibility to retrieve this information reflect the intention of the LIS in this clause; the actual entity performing this functionality might be named differently and provide additional functionality not relevant to this clause.

DSL routers that obtain temporary IP addresses from DHCP servers provide no fixed association between IP address and Router location. An example method of achieving the binding when an IP address is assigned requires the use of the "Relay Agent Information Option" (RFC 3046 [7]) that traces requests through the network; with such a trace the location can be derived via a network configuration database.

Residential and SME network attachment via WiMAX poses a further problem as the reach of a WiMAX radio link exceeds the accuracy requirements of the PSAP/ECC organizations. Although the WiMAX routers are at fixed and known locations, there is no guarantee that such routers will not be moved to locations beyond the accuracy requirements of the PSAP/ECC organizations.

6.2 Attachment of an NGCN to an access network

Figure 18 illustrates the attachment of a NGCN (Next Generation Corporate/Customer/Campus Network) to the NGN access network via VDSL. Usually, the VDSL router deploys a NAPT.

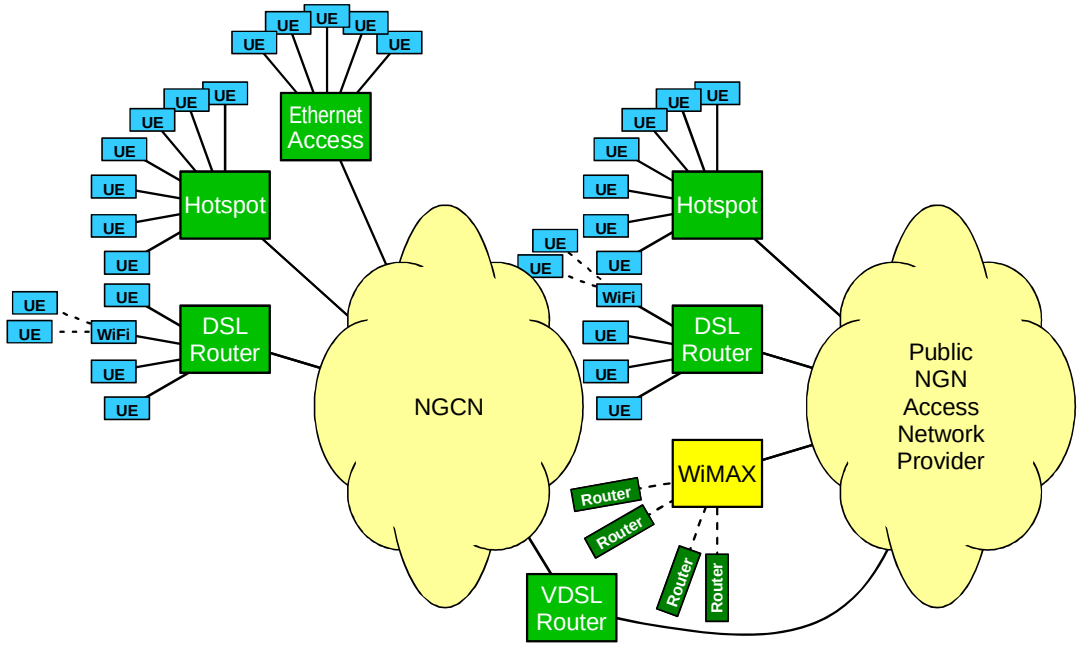


Figure 18: Attachment of NGCN to an access network

Using Ethernet access, the wall sockets are at known fixed locations similar to the DSL routers mentioned in clause 6.1. If there are fixed IP addresses associated with either of these, there exists a one-to-one correspondence between IP address and location of the UE. This correspondence can be used for retrieving location information during emergency calls.

If for UEs on Ethernet wall sockets, DSL routers or Wi-Fi hotspots temporary IP addresses need to be retrieved from DHCP servers, no fixed association between IP address and location of Routers, Ethernet wall sockets, or Wi-Fi hotspots are given. However, to achieve a temporary binding, the method described in clause 6.1 can be used, i.e. use the method defined in RFC 3046 [7] to trace a path through the NGCN from the router, hotspot, or Ethernet wall socket.

The NAPT in the VDSL router toward the NGN access network mentioned above poses another kind of problem. The public NGN receives an emergency call that presents a source or via address known within the NGCN whereas the media use a translated address of the VDSL. There must exist a possibility to allow the access network to know the location of the caller within the NGCN. This problem will be discussed in clause 6.4.

6.3 Cascaded NGCN

Figure 19 illustrates the situation where a worldwide parent company deploys two level of NGCNs, one that carries the traffic between centres or countries and attached via one or more routers to the country or centre NGCNs. Smaller offices may be attached via links attached either to a country NGCN or the worldwide NGCN. Again, the routers will usually employ NAPTs.

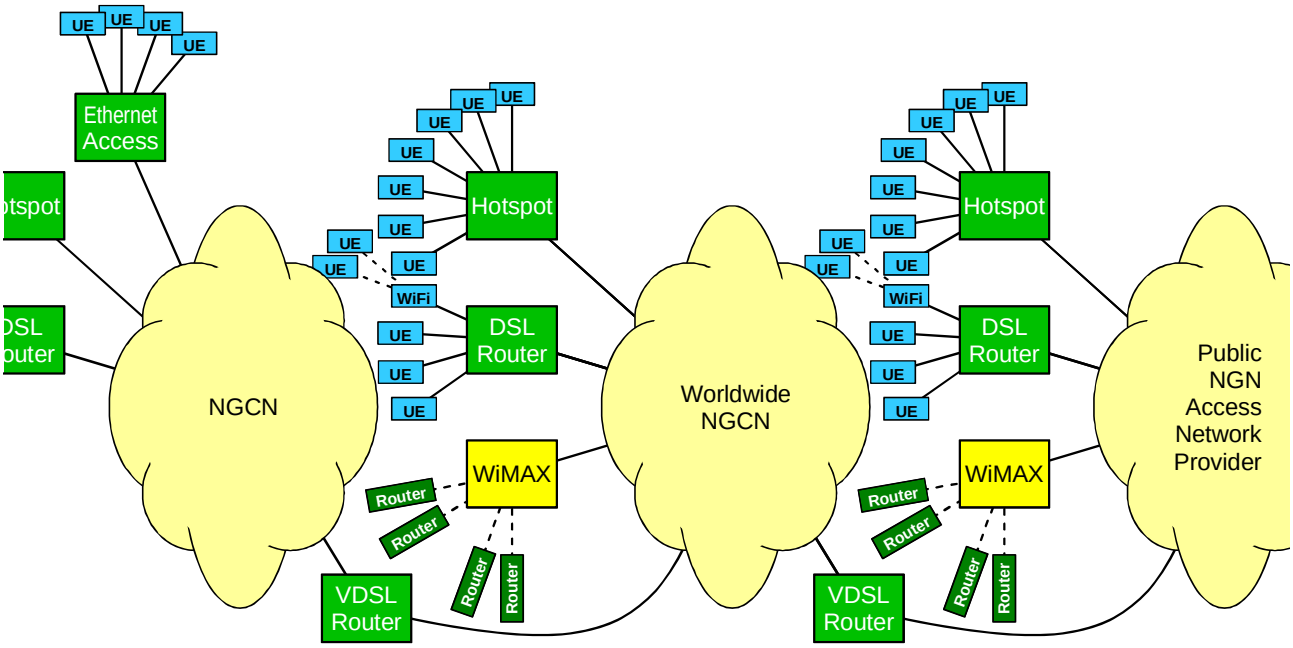


Figure 19: Cascaded NGCN

Through this cascading of NGCNs, the situation detailed in clause 6.2 is replicated, i.e. the location information in the NGCN for fixed addresses or addresses leased from a DHCP server are known in the NGCN and must, in case of an emergency call, be communicated to the worldwide NGCN. The worldwide NGCN itself knows the location of its UEs at hotspots and behind DSL routers; however, although it knows the location of the VDSL router to the NGCN, the location of UEs behind this VDSL router remain hidden.

The NAPT in the VDSL router toward the worldwide NGCN network poses the same kind of problem as mentioned in the previous paragraph. The worldwide NGCN receives an emergency call that presents a source or via address known within the NGCN whereas the media use a translated address of the VDSL. The same possibility as required in the previous paragraph will allow the worldwide NGCN to know the location of the caller within the NGCN and communicate this information on the NGN access network. As mentioned, this problem will be discussed in clause 6.4.

6.4 Location acquisition protocol and Proxy LIS querying

In the previous two clauses the problem of NAPT was addressed. In the IETF/NENA/ATIS approach (see clause 8) the communication between Location Information Servers (LIS) is also discussed (see clause 8.5 and figure 27). In that approach, the LIS (Location Information Server) of the NGN communicates with the LIS of the next lower level NGCN, i.e. either the worldwide NGCN (as shown in clause 6.2) or directly the NGCN (as shown in clause 6.1). When there exists a worldwide NGCN between the NGCN and the NGN access network (as detailed in clause 6.2) the same communication takes place between the LIS of the worldwide NGCN and the LIS of the NGCN as if the NGCN were attached to an NGN access network. This situation is illustrated in figure 20.

EXAMPLES:

If an emergency call originated from a UE attached to an Ethernet wall socket in the NGCN at the left in figure 20, the UE can communicate its location (if known) with the INVITE PDU. The socket's location communicated to the UE during the information exchange with the DHCP server could also be attached to this PDU. The association between the IP address and the socket's location is available from the Proxy LIS of the NGCN.

In the worldwide NGCN, the association between the IP address and the router location is available from the Proxy LIS of the worldwide NGCN. Finally, in the Public NGN Access Network, the association between the IP address and the router location is available from the General LIS of the Access Network.

If the General LIS is queried by the E-CSCF, the PSAP, and/or the ECC, it uses the Location Acquisition Protocol to retrieve further, more precise location information from the worldwide NGCN's Proxy LIS. The latter then propagates the query to the NGCN's Proxy LIS. Finally, the location of the Ethernet socket is communicated via a further Proxy LIS to the Access Network's General LIS and from there to the requestor.

As an alternative, the General LIS might provide a list of three locations to the requestor reflecting the path of the emergency communication. This list might be used for consistency checking of the information retrieved.

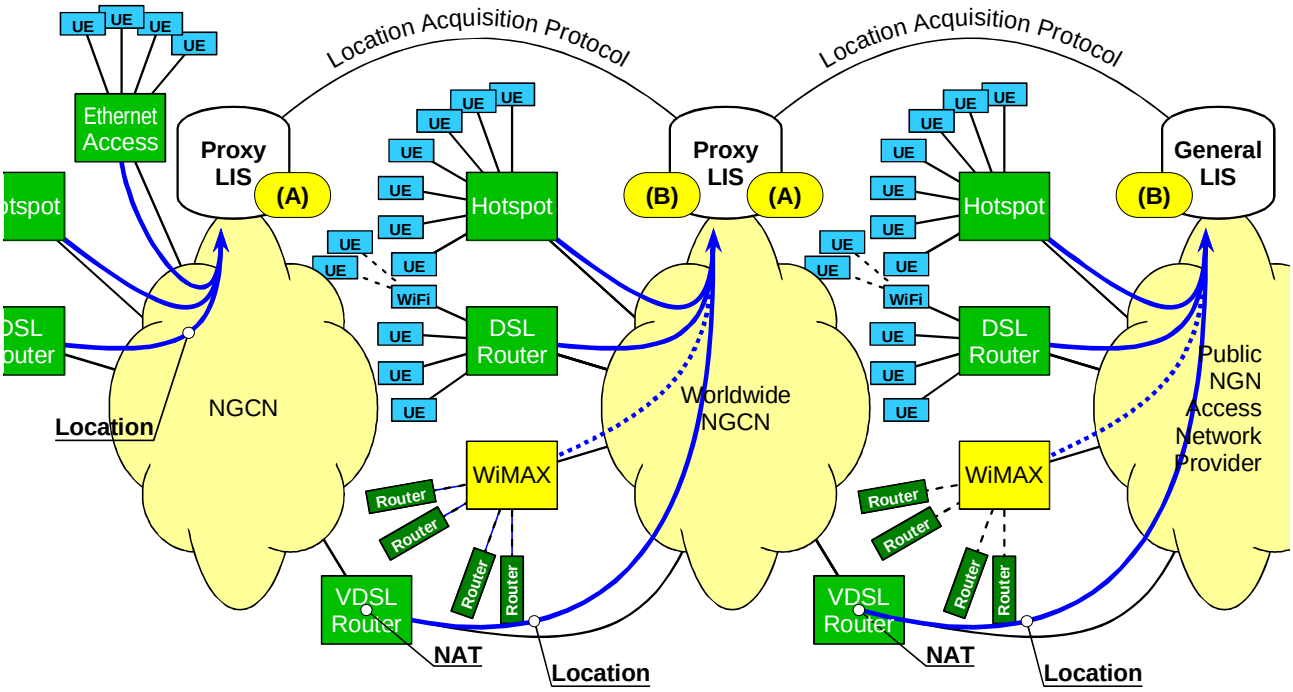


Figure 20: Location acquisition protocol and Proxy LIS querying

6.5 The problem of the tunnel

Figure 21 shows the effect of establishing a VPN tunnel between a UE and a home LAN.

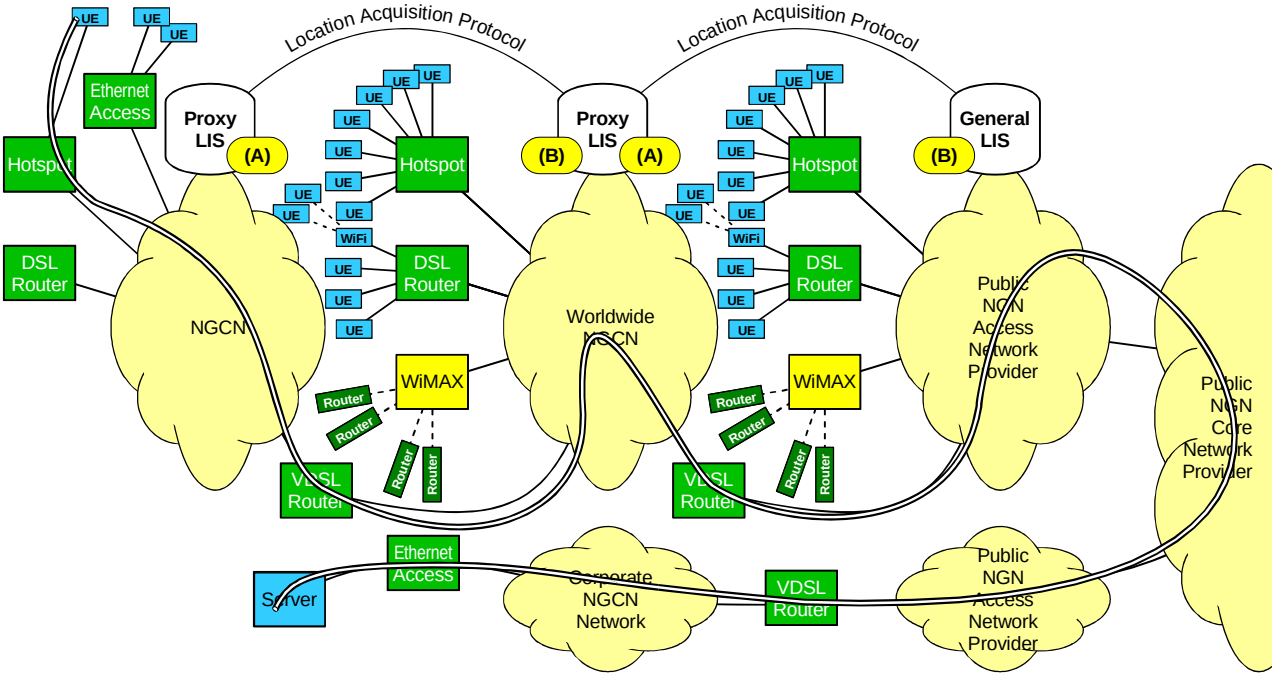


Figure 21: The problem of the tunnel

VPN tunnels form an ingenious method of enabling distant employees to communicate via their home LAN without having any concerns regarding security of the Internet at large. From the point of view from emergency call establishment, use of a VPN tunnel seems to counteract any notion that emergency calls will trigger timely help to a caller in an emergency situation wherever he is.

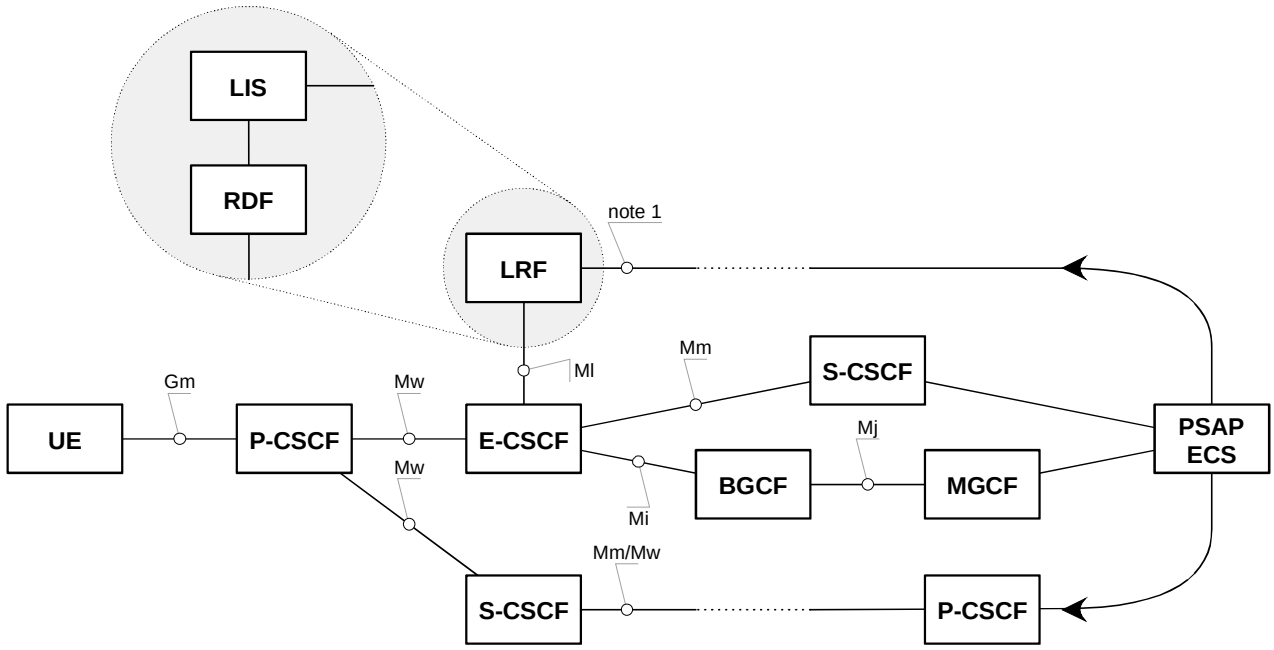
Consider the example of a Swiss banker at a meeting in Paris with colleagues from London and New York, when an American delegate is taken ill. One of the French colleagues may try use the telephone-like device attached to the Swiss-owned laptop computer to call for help, without knowing that the computer is linked via a tunnelled connection to the bank's home network in Zurich. The call will likely be answered by a German speaking call-taker some 500 kilometres away. By the time the problems of the language barrier, location, distances, etc. are all solved, the poor employee might well have ceased his struggle for life, even if the British banker was competent in CPR!

7 Handling of emergency sessions in 3GPP

This clause is an excerpt of TS 123 167 [1]; the present text is based on V7.6.0 [1] though this may be superseded.

7.1 Architecture

The architecture for the handling of emergency IMS sessions is shown in figure 22.



NOTE 1: This interface is not standardized by 3GPP, there might even be regional differences depending on regulations and application services employed. TS 123 271 [16] recognizes four different categories of location services. These are the Commercial LCS, the Internal LCS, the Emergency LCS and the Lawful Intercept LCS.
NOTE 2: Gm, Mw, Mm, Mi, Mj, and Ml are designation of reference points in the 3GPP reference architecture.

Figure 22: E-CSCF and reference architecture

P-CSCF and E-CSCF are always located in the same network; this may be a visited network.

For simplicity, some functional components, e.g. IBCF, I-CSCF, MGCF and BGCF, are not shown in figure 22.

It shall be possible to support configurations where the Location Retrieval Function (LRF) may consist of a Routing Determination Function (RDF) and a Location Information Server, the interface between Location Information Server and RDF is out of scope of the 3GPP specification. On the other hand, the RDF may be integrated in the Location Information Server (e.g. in the LRF).

7.2 User equipment (UE)

7.2.1 Requirements

1) The UE should be able to detect the establishment of an emergency session and include an appropriate indication in the request.

2) The UE should use a special emergency Public User Identifier in the IMS emergency registration request.

3) The UE may perform an IMS emergency session establishment without prior emergency registration when already IMS registered and it is in the home network. Otherwise, the UE shall perform an IMS emergency registration.

4) The UE should include an emergency service indication in the emergency session request.

5) The UE should include an equipment identifier in the request to establish an emergency session for "anonymous user". An "anonymous user" in this context is a person who does not have sufficient credentials for IMS registration.

6) The UE should attempt the emergency call in CS domain, if capable.

7) The UE should handle a 380 (Alternative Service) response with the type set to "emergency" as a result of emergency attempt.

8) The UE should handle a response with an indication, IMS emergency registration required as a result of emergency session establishment attempt.

7.2.2 Emergency session establishment request

The UE initiates the emergency session establishment request, and for the purpose of properly processing the request in the network the following specific information is supplied in the request message:

- Emergency session indication.
- Emergency Public User Identifier if an IMS emergency registration is performed. If not, any registered Public User Identifier is used.
- Optionally, type of emergency service. It could be implied in the above emergency session indication.
- UE's location information, if available, and
- The Tel URI associated to the emergency Public User Identifier, if available.

7.3 IMS Functional entities

7.3.1 Proxy Call Server Control Function (P-CSCF)

Upon receipt of an emergency session establishment request from a UE the P-CSCF shall perform the following actions:

- The P-CSCF shall handle registration requests with an emergency Public User Identifier like any other registration requests. The P-CSCF may set the proposed registration expiration time according to the local policy and change the expiration value in the REGISTER requests, and then forward the request to the IBCF or I-CSCF in the user's home network. If the registration expiration time is changed by the P-CSCF in the visited network, the S-CSCF in the home network should obtain the proposed registration expiration value from the REGISTER request and use the same registration expiration time.
- The P-CSCF shall detect an emergency session establishment request. Dependent on local policies, it shall reject or allow unmarked or anonymous emergency requests.
- The P-CSCF shall prevent the assertion of an emergency Public User Identifier in non-emergency requests
- The P-CSCF may query IP-CAN for a location identifier.
- The P-CSCF shall select an E-CSCF in the same network to handle the emergency session request. This selection is based on local procedures.
- The P-CSCF shall establish the emergency session with the locally defined priority for emergency sessions.
- The P-CSCF shall check the validity of the caller Tel URI if provided by the UE and shall provide the Tel URI in the session establishment request if it is aware about the Tel URI associated with the emergency Public User Identifier.
- The P-CSCF may respond to the UE with an indication, IMS emergency registration required as a result of processing the emergency session establishment attempt.

- The P-CSCF should be able to identify the service data flow associated with emergency service and inform PCRF accordingly.

7.3.2 Emergency Call Server Control Function (E-CSCF)

Upon receipt of an emergency session establishment request from a P-CSCF the E-CSCF shall perform the following actions:

- If location information is not included in the emergency request or additional location information is required, the E-CSCF may request the LRF to retrieve location information.
- If required, the E-CSCF requests the LRF to validate the location information if included by the UE.
- The E-CSCF determines or queries the LRF for the proper routing information/PSAP destination.
- The E-CSCF shall route emergency session establishment requests to an appropriate destination including anonymous session establishment requests.
- Subject to national requirements, the E-CSCF may send the contents of the P-asserted ID or UE identification to the LRF.
- Based on local policy, the E-CSCF may route the emergency IMS call to an ECS for further call process.

7.3.3 Location Retrieval Function (LRF)

The LRF is responsible for retrieving the location information of the UE that has initiated an IMS emergency session. It shall be possible to support configurations where the LRF may consist of a Routing Determination Function (RDF) and a Location Information Server (LIS), the interface between LIS and RDF is out of scope of the 3GPP specification.

The LRF utilizes the RDF to provide the routing information to the E-CSCF for routing the emergency request. The RDF can interact with a location functional entity that provides real-time information about the location of Mobile Station and manage ESQK allocation and management. The ESQK is used by the PSAP to query the LRF for location information and optionally a call-back number. The LRF-PSAP interactions are outside the scope of the 3GPP specification.

Information provided by the LRF to the E-CSCF includes the routing information and other parameters necessary for emergency services, which are subject to local regulation. For example, this information may include the ESQK, ESRN, PSAP SIP URI or Tel URI.

In order to provide the correct PSAP destination address to the E-CSCF, the LRF may require interim location information for the UE.

In some regions, for example in North America, it is commonplace to provide the PSAP with an initial location estimate for the UE and to provide an updated, more accurate location estimate for the UE when requested by the PSAP. Where this requirement exists, the LRF may store a record of the emergency session including all information provided by the E-CSCF and only releases this record when informed by the E-CSCF that the emergency session has terminated. The information provided by the LRF to the E-CSCF (for example, from the ESQK) will include correlation information identifying both the LRF and the emergency session record in the LRF, information which was transferred to the PSAP during session establishment (for example, in a SIP INVITE or via SS7 ISUP signalling from the MGCF). The PSAP may use this information to request an initial location estimate from the LRF and/or to request an updated location estimate.

The TISPAN NGN Endorsement of the 3GPP architecture enables location retrieval from a TISPAN CLF (ES 282 004 [3]) though the CLF interface is not explicit.

7.4 Procedures for IMS Emergency Services (Overview)

7.4.1 Procedures without Location Retrieval Function (LRF)

Figure 23 contains a high level description of the emergency service procedures performed when the UE can detect the emergency session is being requested.

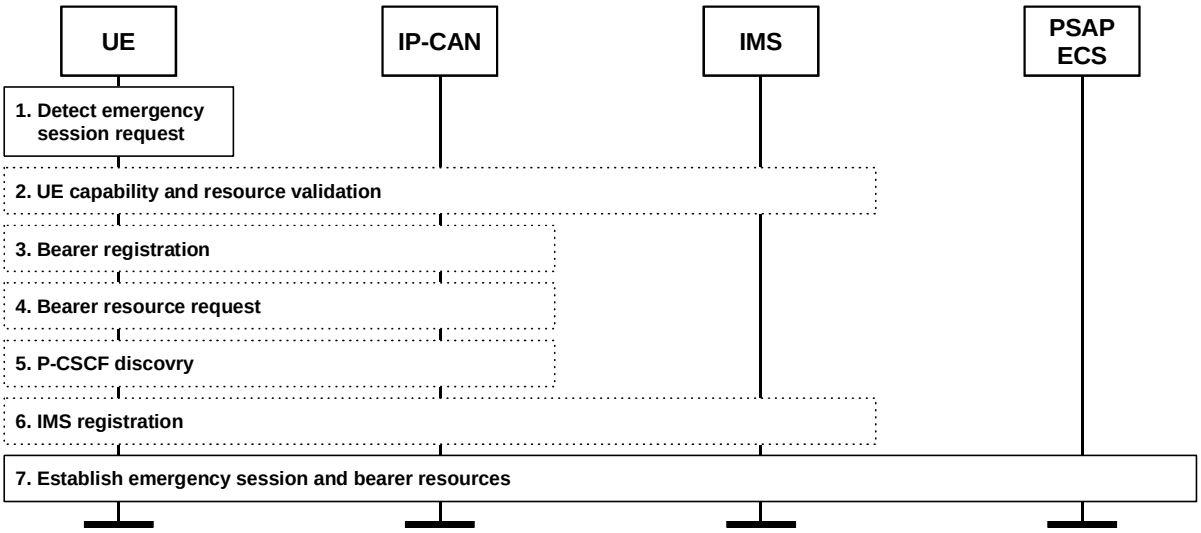


Figure 23: UE detected emergency call

7.4.2 Procedures involving the Location Retrieval Function (LRF)

Figure 24 illustrates a high level call flow for the IMS emergency session establishment procedure using LRF/RDF to retrieve location and routing information.

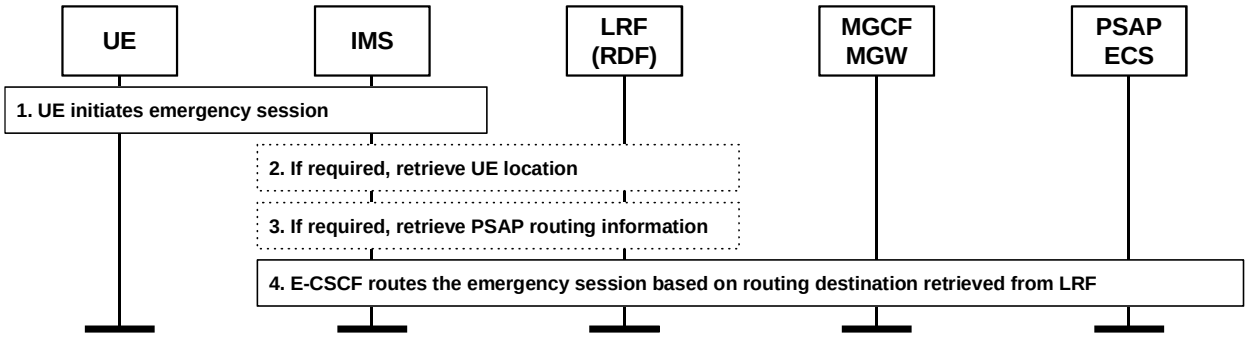
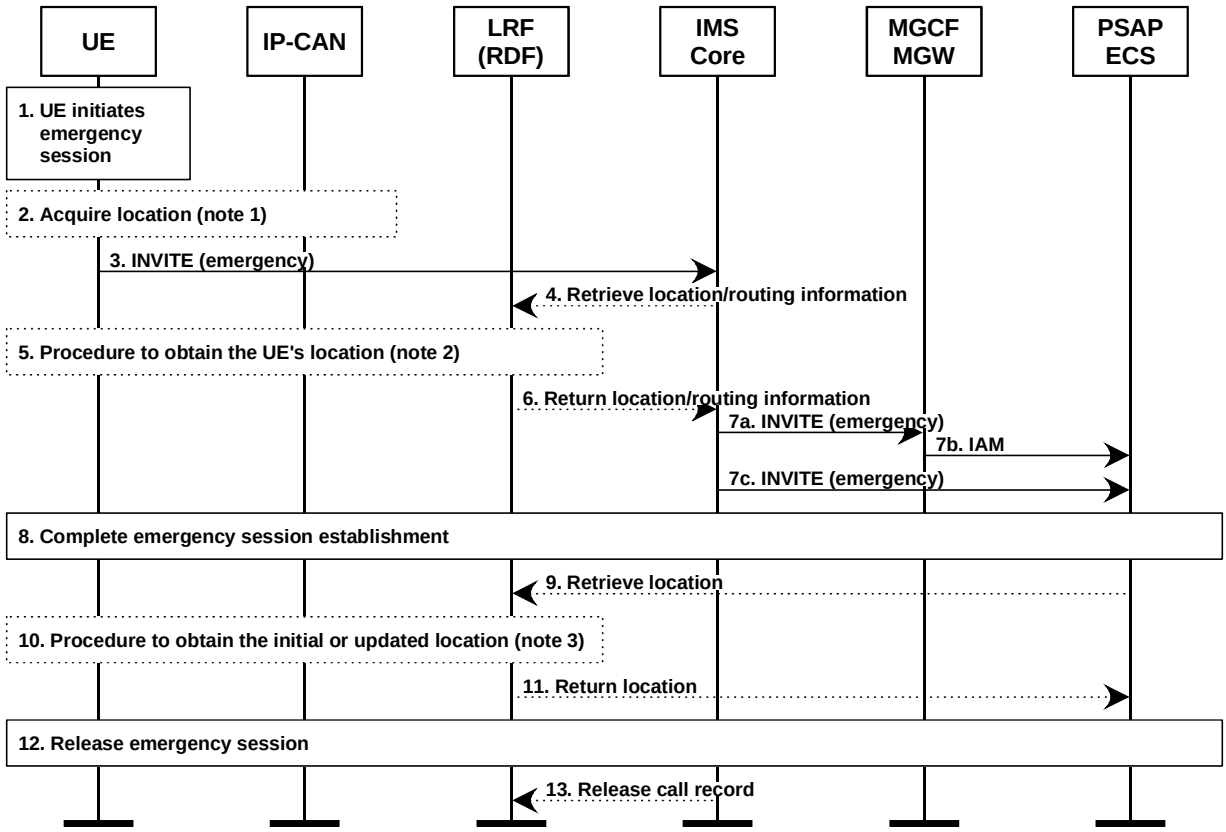


Figure 24: Emergency Session Establishment procedure using LRF/RDF

7.4.3 Acquiring location information from the UE and/or the network

Figure 25 shows a high level sequence of flows that illustrate the location information acquisition of both the UE, the IMS core, and the PSAP.



NOTE 1: The UE determines its own location or location identifier if possible. If the UE is not able to determine its own location, the UE may, if capable, request its location information from the IP-CAN, if that is supported for the used IP-CAN. If applicable, the IP-CAN delivers to the UE the UE's geographical location information and/or the location identifier.

NOTE 2: The LRF may already have the information requested by IMS core or LRF may request the UE's location information. The means to obtain the location information may differ depending on the access technology the UE is using to access the IMS.

NOTE 3: The LRF determines the target UE's location using one the same means as in step 5. The LRF may use the correlation information received in step 9 to retrieve information about the UE that was stored in step 5.

Figure 25: Handling of location information in IMS emergency calls

8 The IETF, NENA, ATIS Approach

This clause provides a synopsis of the ATIS Technical Report [17]. The document was circulated widely to SDOs and was received by ETSI TC TISPAN and SC EMTEL as a liaison statement on which ATIS requested comments. This synopsis is intended to assist TISPAN and EMTEL delegates in their consideration of the ATIS document. Note that the present document does not intentionally express any opinions regarding the content of the report.

8.1 Abstract

The ATIS [20] document describes the specific areas of location acquisition and location parameter conveyance in IP access networks and is concerned with both the architectures and protocols for supporting these functions. It describes the manner in which IP devices request location information from the LIS function in an access network and the manner in which the LIS function obtains information from the access net-work supporting the requesting IP device in order to calculate the device's location.

The LIS function is identified as an essential component of the NENA-defined «i2» architecture for VoIP emergency services and continues to be required in the «i3» architecture currently under definition. The ATIS document [17] describes the LIS requirements, as specified by NENA in terms of those architectures, examines the candidate protocols for location acquisition (HELD, DHCP, and LLDP-MED) and provides a gap analysis.

The concepts of location parameter conveyance are described and a specific architecture (the LIS-ALE architecture) is described. A flexible LIS-ALE protocol is described (FLAP) and examples are provided of its application in some common forms of broadband access networks.

The technical report [17] is intended to be used as input to further decision-making processes leading to any necessary policy and/or American National Standards formulation and as a vehicle for communicating concepts in liaisons with other relevant SDOs.

8.2 Introduction/Executive Summary

The NENA VoIP migratory working group defined the «i2» network architecture to support emergency service calls originating from VoIP services on the Internet. The architecture identifies a network element called the Location Information Server (LIS) that provides location data used for call routing and for display at the PSAP operator terminal.

The «i2» specification did not detail the protocol to be used by the LIS for providing location information to the VoIP device or proxy nor the manner in which location should be determined for different Internet access technology types. A separate NENA document defined the requirements for the LIS.

The ATIS document [17] divides the subject into two areas. The first is "Location Acquisition" which describes the manner in which LIS clients interact with the server to obtain location. Candidate location acquisition protocols (DHCP, LLDP-MED, HELD, and RELO) are compared against the NENA defined requirements. The second area is "Location Determination" which is the manner in which a LIS determines the location of a device in specific access network types. A variety of access technologies are examined and a generic architecture based on access location entities (ALE) providing network parameters to the LIS is described. A protocol called the Flexible LIS-ALE Protocol (FLAP) is described which supports this architecture.

The results of the location acquisition protocol comparison and the description of the LIS-ALE architecture and FLAP protocols are provided as a basis for discussion and decision-making. Input from a range of SDOs in response to the present document is solicited.

8.3 NENA «i2» Architecture

The NENA «i2» initiative was proposed with the intent of addressing the immediate need of providing consistent emergency services support to next generation Residential Broadband VoIP phone users. The NENA architecture is shown in figure 26 and is specified in the NENA document [4].

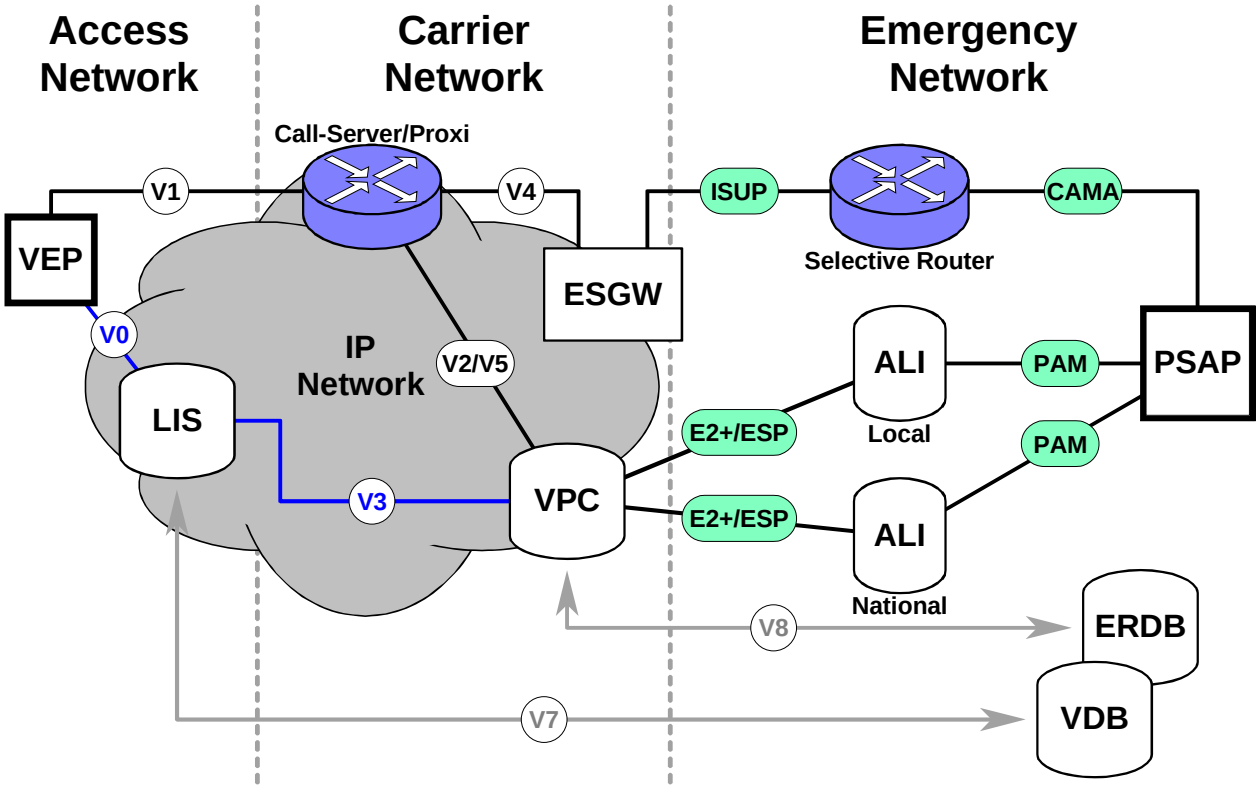


Figure 26: NENA «i2» architecture

The requirements for the Location Information Server (LIS) cover the following three areas:

- Location determination and acquisition.
- Location representation.
- Location security and dependability.

The ATIS document [17] asserts that global inter-operability could be enhanced if the «i2» architecture were widely adopted and that the two key functions of emergency call routing and the delivery of location information that the «i2» architecture provides are common to emergency services world-wide. In support of this assertion, the report notes the requirement to service roaming and nomadic subscribers and suggests that rather than requiring a call server implementation to adapt to an arbitrary number of systems, protocols, and interfaces, there might be a major benefit if all jurisdictions adopt the same approach.

8.4 Location Determination in Broadband Access Networks

The ATIS report [17] also examines a range of common access technologies and provides examples of how location determination is possible, and the key parameters that need to be captured in order to permit location determination. The examples provided are illustrative and not comprehensive nor definitive. The descriptions of ADSL, cable, and 3G technologies appear to be accurate in terms of representing actual deployment topologies and signalling scenarios though there is scope for variation in detail in the real world. WiMAX standards are still under definition by the IEEE and references to the types of network parameters that contribute to location determination and the signalling scenarios by which those parameters may be extracted from the network are more speculative.

8.5 LIS Operational Considerations

The conceptual role of the Location Information Server (LIS) is to provide location information (optionally digitally signed) to its clients. This is straightforward from a conceptual perspective but may have significant operational implications. For example, the organization that delivers broadband Internet access to users may actually be made up of separate business entities and the relationship between the different entities impacts the practical implementation of the, otherwise logical, LIS function and has a bearing on the specific functionality that a given LIS entity will have.

The types of LIS operators (organizational entities that may own and operate a LIS) include, though may not be limited to, the following:

- Access infrastructure providers.
  - RBPs for DSL, Cable, 3G, WiMAX, etc.
  - Municipal and community Wi-Fi network operators.
- Internet Service Providers.
  - Providers of Internet access to the public.
  - May own or use third party access infrastructure.
- Geo-distributed LAN operators.
  - Commercial enterprize with broad geographic coverage.
  - Government enterprize operator.
  - Academic and research network operator.
  - Extensive private estate network operator.
- Geo-point LAN operator.
  - Residential LAN.
  - Single access point hotspot.

As described in the introductory text, the form and function of the LIS implementation in each of the above cases will vary. The form and function that a specific instance of a LIS has will vary depending on the nature of the network it is supporting and the role that the operator of that network plays in the larger picture of Internet access. The specifics of form and function will inevitably be influenced by these aspects and the business and other relationships that exist between network types.

Some variants of LIS implementation that can be identified from these different network scenarios can be labelled as

- General LIS.
- Gateway LIS.
- Proxy LIS, and
- Relay LIS.

Figure 27 shows an overall network topology illustrating the relationships between these types of LIS implementations.

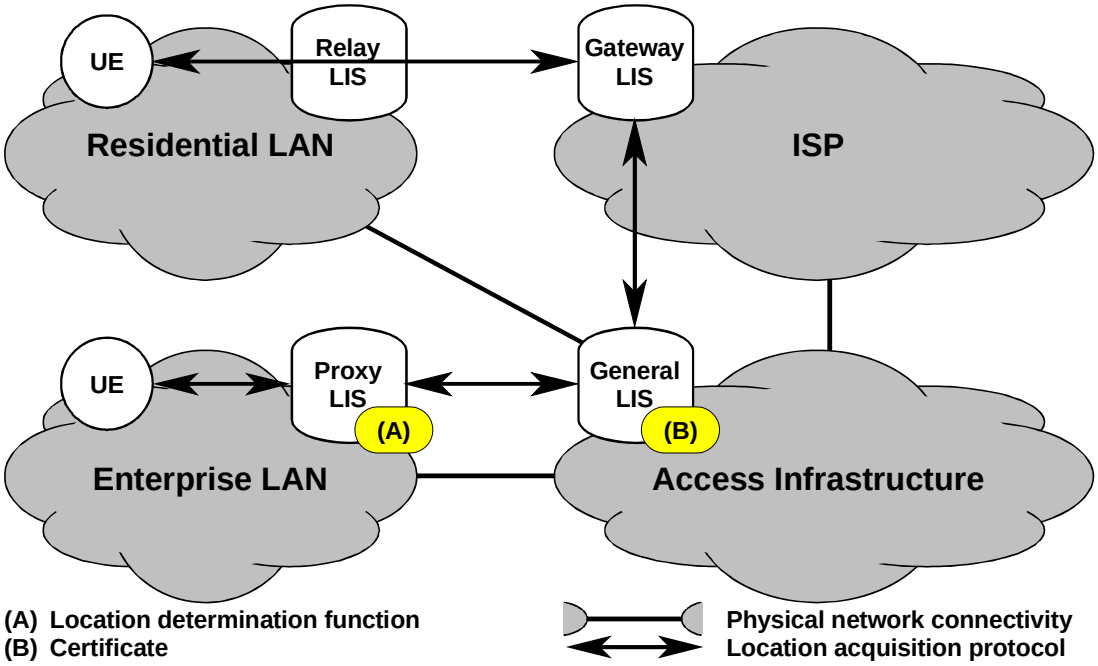


Figure 27: LIS Types and associated network types

8.6 Location Acquisition Protocols

The term "location acquisition" refers to the process of a client device or application requesting, and receiving, location information from the LIS. There are a number of approaches and philosophies related to this acquisition process and the protocols that support it. The following candidates are analyzed:

- Dynamic Host Configuration Protocol (DHCP) RFC 3825 [8].
- Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED).
- HTTP Enabled Location Delivery (HELD).
- Retrieving End-System LOcation information (RELO).
- A Location Reference Event Package for the Session Initiated Protocol (LREP-SIP), and
- Location Configuration Protocol (LCP).

Table 6 is the result of a gap analysis and shows the support of the 23 NENA provided applicable requirements on location acquisition and determination by the candidate protocols.

Table 6: Support of the NENA requirements

Protocol	full support	partial support	no support	not applicable
DHCP	10	2	8	3
LLDP-MED	10	1	9	3
HELD	21	-	-	2
RELO	13	1	6	3
LREP-SIP	13	-	8	2
LCP	12	1	7	3

8.7 Location Parameter Conveyance

To capitalize on this common characteristic, a logical network function called an Access Location Entity (ALE) can be defined. The function of the ALE is to provide the LIS with the set of network parameters pertinent to location determination for the particular type of access network with which the ALE is associated. While the ALE is technology specific, the communication of a "set of network parameters" to the LIS is a common function. For this purpose, the Flexible LIS-ALE Protocol (FLAP) is proposed.

FLAP is currently only informally documented and has not been specified under the auspices of any SDO. Location measurement has, in the past, typically been done on a technology specific basis.

9 Comparison between 3GPP and NENA

Table 7 draws a comparison of the availability of a number of the principal features of the NENA and 3GPP solutions.

Table 7: Feature differences between NENA and 3GPP

Feature / Implementation	NENA («i2» and «i3»)	3GPP
Support of Fixed and Nomadic wireline access	Yes	Yes for fixed broadband access according to TISPAN No for others
Wireless access support	Not in scope, though possible with changes To be addressed explicitly in «i3»	Yes
Use of IMS	No in «i2», architecture is currently SIP based Yes in «i3», 3GPP solution was added to «i3»	Yes
Location Solution for wireline access	References IETF solutions some of which are complete and some still in development	Enables location retrieval from a TISPAN CLF (ETSI ES 282 004[3]) though the CLF interface is not explicit
Location Solution for wireless access	Yes - WLAN access No - Cellular access	Yes
Interface to legacy PSAPs	Yes, using existing US solution	Yes, using existing solutions for US and Europe
Interface to IP capable PSAPs	No, covered in «i3» which is still in development	Yes, but the solution (like «i3») is not yet complete
TISPAN support	Not explicit	Yes
NOTE: The principal differences between «i2» and «i3» are noted in the relevant cells.		

NOTE: From this table of comparisons that there is already considerable convergence between the NENA «i2» the and 3GPP work. This is further enhanced in NENA «i3», with the principal areas requiring additional development being:

- The support of nomadic wireline access.
- Support of wireline access.
- Interfaces to IP capable PSAPs.

10 Developments in Europe (EU)

The Coordination Group on Access to Location Information by Emergency Services (CGALIES) was established as an initiative of the European Commission (DG INFSO), with the mission to define requirements for a Pan European common location provisioning mechanism that could be accessed and used by the European 112 community and emergency service operators. It was to study the potential requirements for emergency caller location and the conveyance of location information across telecommunications networks. Its membership included representatives from the public and the private sector, and from a wide range of interests.

The final report of CGALIES was not intended to establish normative requirements and a synopsis is included here as part of the analysis or work done by other standards bodies, again without attempting to establish normative requirements.

According to the limited inputs received during the compilation of the present document, the UK and Germany seem to be almost alone in Europe in planning for Emergency Caller Location from IP networks, though the existing, centralized PSTN emergency call arrangements in the UK are possibly more conducive to an easy migration than is the predominantly local PSAP structure in other countries. So far as we have been able to determine, the UK is also almost alone in Europe in having largely centralized its PSAP operations.

10.1 The CGALIES survey - Excerpt from Final Report

The «Final Report V1.0» of the Coordination Group on Access to Location Information by Emergency Services (CGALIES) [11] to the European Union and its Member States including the public and the private sector for consideration in 2002. This is in consideration that a smooth and successful introduction of enhanced emergency services cannot be taken for granted.

10.1.1 Type of areas

a) **Rural** environment: Sparsely inhabited areas, fields, forests, etc.

b) **Rural extreme** environment: A rural environment with a very large cell size.

c) **Suburban** environment: Populated areas, residential houses, villages.

d) **Suburban extreme** environment: A suburban environment with abundant shadowing, blocking and multi-path possibilities.

e) **Urban** environment: Densely populated areas, multi-story buildings, offices, city centres.

f) **Urban extreme** environment: Extremely densely populated areas, high-rise buildings

g) **Indoor** environment: …

h) **Highway and Crossroad** environment: …

10.1.2 Type of information

a) Master Street Address Guides (MSAGs) ***must*** be established for fixed lines.

b) Master Street Address Guides (MSAGs) ***must*** contain both **tabular** (physical streets and boundaries) and **spatial** (X- and Y-coordinates).

c) Master Street Address Guides (MSAGs) ***must*** be available for all fixed line numbers, i.e. include private, non-listed, and MSN numbers.

d) An Automatic Location Identification (ALI) database ***must*** be updated at least every 24 hours.

e) The tabular information must include an indication whether the Calling Line Identity (CLI) is an entry to a customer network (company or private).

f) Customer networks ***should*** maintain their own Automatic Location Identification (ALI) database and provide this information to outgoing emergency calls.

g) In urban environments the height ***should*** be indicated.

h) Emergency services indicate that the provision of the caller's direction and speed ***would*** be useful in the following situations:

- Detection whether the caller is moving or static.
- Establish whether the caller could be a "Good Samaritan".
- Establish whether the caller is involved in the reported incident.

- Locate the caller during a suspected kidnapping incident.
- Estimate speed and direction as an estimate of the location of the reported incident.
- Determine which side of a carriageway an incident has occurred.

Interpretation of multiple location estimates (location history) can be used to provide direction and speed indication.

The direction and speed indication ***should*** be provided at the time the call is initiated. It may also be acceptable if the information is provided as a separate update during the call or even after call completion.

i) Location and velocity (i.e. direction and speed) information ***can*** be used to identify whether multiple calls refer to the same incident or whether the call originates from a "Good Samaritan".

10.1.3 Use of the Location Information

a) Routing: The Location Information is used to route the call to the correct stage 1 Public Safety Answering Point (PSAP).

b) **Dispatching**: The Location Information is used to route the call to the correct stage 2 Public Safety Answering Point (PSAP) and/or Emergency Service Centres (i.e. fire, police, ambulance/medical).

c) **Finding**: The Location Information is used to find the caller and/or incident.

d) **X- and Y-coordinates**: Routing, dispatching, and finding ***shall*** be based on X/Y-coordinates. Tabular information ***may*** be useful for finding the final steps to the caller.

10.1.4 Accuracy

a) First rough estimate: This estimate is used for routing and dispatching and should be available within 7 seconds after call initiation. The required accuracy for this initial location information is between 200 m to 300 m for all environments.

b) The caller's location information for caller finding must be available within 30 seconds after call initiation. The accuracy requirements are summarized in the following table.

	Caller can provide general information	Caller cannot provide general information
Indoor	10 m to 50 m	10 m to 50 m
Urban	25 m to 150 m	10 m to 150 m
Suburban	50 m to 500 m	10 m to 500 m
Rural	100 m to 500 m	10 m to 500 m
Highway / crossroads	100 m to 500 m	10 m to 500 m

c) The vertical accuracy requirement for caller finding in urban environments is 10 m to 15 m. There exists no requirement for other environments.

10.2 Developments in the UK

10.2.1 Background

British Telecom (BT) operates a single, networked call centre system (at five locations) which receives emergency calls from anywhere in the kingdom, both from its own customers and those from a number of other operators who contract with BT for its answering services. Cable and Wireless (C&W) operates a similar facility at a single location. These six centres answer emergency calls and extend them to the relevant emergency service at the appropriate emergency control centre according to pre-defined criteria.

Emergency calls from fixed networks are accompanied by the calling number, the civic address at which that number is registered, the subscriber's name and any other relevant information which is held by the network operator. Emergency calls from mobile networks are accompanied by whatever location information is available; at the very least this identifies the network operator, the cell site and its coverage. The PSAP also receives the name and address at which the handset is registered, when this is available (many "pay as you go" (PAYG) telephones in the UK do not have a registered user). Location information is normally available to the PSAP operator within four seconds, i.e. before the call is handled, since there is a short delay to trap accidental calls emanating from line faults simulating loop-disconnect dialling in the PSTN network (a by-product of the use of 112 as the emergency number!).

It is a regulatory requirement in the UK that operators of publicly available telephony systems (PATS) must provide an emergency calls facility; all fixed line and mobile operators are so designated, as are some VoIP providers. Terminals that are dependent on power supplies at the customer premises are required to carry a label, warning that in the event of power failure emergency service will not be available. VoIP telephones not providing an emergency call service are required to be labelled as such.

10.2.2 Progress

The UK telecommunications regulator, has established an Emergency Calls Task Force to examine the issues around the location of calls from IP-connected, possibly nomadic users. This group has determined a strategy based on the IETF/ATIS/NENA «i2» solution and is developing a tactical solution for fixed, nomadic and mobile VoIP users.

The group is adopting a phased approach, looking first at "standard" UK users calling from within the UK, to be followed by those with «i2» compliant endpoints, foreign users in the UK with «i2» compliant endpoints, standard UK users abroad and finally, UK «i2» compliant users calling from abroad.

It is recognized that these deliberations must not produce "dead-end" solutions not capable of being extended to cater for future developments, particularly in access technology, and also that as a non-revenue producing service the solutions must be cost-effective in their implementation. It is expected that formal proposals catering for the first two phases will shortly be made.

The group has also recognized that in some cases there is no incentive for the public network operator to provide a standardized Location Information Server (LIS) since it has no immediate application in the operator's network and the information may be held more cost-effectively in some other way. Equally, although the LIS concept is necessary in almost any network, a private network operator may choose to hold terminal location data in any one of a multitude of ways, most of which are likely to be incompatible with the «i2» approach. It is expected that regulatory intervention may be required to solve this problem.

10.3 Developments in Germany (Core IMS Emergency Calling Architecture)

10.3.1 Introduction

Deutsche Telekom (DT) provides a variety of telecommunications services on a national basis and which must comply with the current German/EU regulations. DT currently provides VoIP services based on the IMS core standards and has plans to implement IMS Access in the future.

For VoIP emergency calling, DT intends to implement an architecture based on the existing organizations and accounting models in Germany and by upgrading the existing infrastructure in steps. In particular, the German emergency calling architecture does not assume the existence of a dedicated national Emergency Services Provider (ESP) or NENA-like VPCs. The proposed architecture is said to comply with the current regulatory requirements in Germany and EU. The proposal, a "two-step" architecture, is referred to as the "DT Core IMS Emergency Calling Architecture" and is described in clause 10.3.2.

Additionally, DT proposes a harmonized NENA/3GPP-IMS/DT-Core-IMS Emergency Calling Architecture. The goal of this architecture is to enable emergency calling for internationally nomadic SIP users, by allowing at the same time, different countries and carriers to build an emergency calling infrastructure based on their own requirements, existing infrastructures and specific business cases. The proposed architecture is described in clause 10.3.3.

It is acknowledged by DT that the proposal for the harmonized architecture still needs a great deal of discussion and technical work and also that it does not currently consider harmonization with the IETF/ECRIT architecture, though this may be included in a later stage.

In the following clause 10.3.4 DT describes why it is felt that the NENA «i2» architecture cannot be adopted in Germany and also defines what they see as major requirements for the TISPAN architecture. Some arguments against the DT position are also outlined here.

10.3.2 Description of the DT Core IMS Emergency Calling Architecture (for DSL-access)

The architecture proposed for Germany should be developed in two steps. Step 1 is intended to be implemented in the near future, enabling Emergency Calling for existing VoIP end and intermediary devices.

Figure 28 shows the proposed Step 1 "DT Core IMS emergency calling architecture".

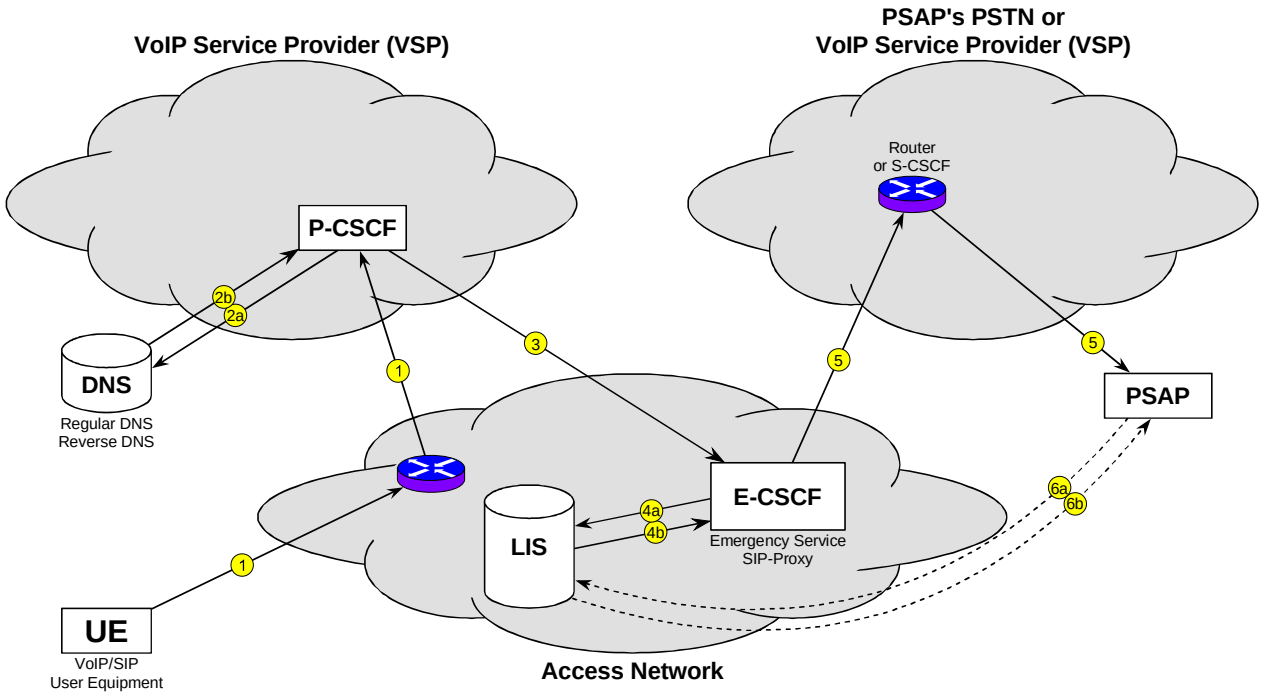


Figure 28: Step 1 of the Core IMS emergency calling architecture

DT asserts that this architecture works for end devices and small private networks with public IP addresses and supports national nomadic VoIP usage. Automatic determination of the location of callers in large private networks is not possible in stage 1.

Most large IP-connectivity providers in Germany also provide SIP services. The Emergency Services SIP-Proxy (E-CSCF) belongs to the IP-connectivity provider or to another local SIP provider trusted by the IP-connectivity provider, for example, the local carrier providing the IP-connectivity to the IP-connectivity provider. IP-connectivity providers which enable SIP Emergency Calling must add the E-CSCF URI to their SVR-record in DNS.

10.3.2.1 Step 1

1) An end user dials the emergency calling dial string (for example 112), causing the end device to send an INVITE to its VoIP Service Provider's SIP proxy.

2) The SIP-proxy authenticates the caller, recognizes the emergency call and determines:

   - the public IP-address of the end device (for example, by using STUN or other mechanism);
   - the IP-connectivity provider's domain name using Reverse DNS;

- the E-CSCF URI provided for this domain in DNS.

3) The SIP-proxy inserts the public IP-address of the end device and the domain name of IP-connectivity provider into the INVITE and forwards it to the E-CSCF.

4) The E-CSCF gets a Location Reference (for example the HTTP/SOAP URIs) and the PSAP URI from the LIS in the local domain, based on the IP-address of the end device.

5) It routes the INVITE, which contains the Location Reference to the PSAP.

6) The PSAP queries the LIS to get the precise Location Information.

10.3.2.2 Step 2

Step 2 is a longer term architectural proposal and an upgrade to Step 1. In addition to the Step 1 features it enables automatic localization of users in large private networks by requiring end- and intermediary-device support. As in Step1, the private networks must have to have a SVR-record containing the E-CSCF URI.

Figure 29 shows the proposed Step 2 emergency calling architecture.

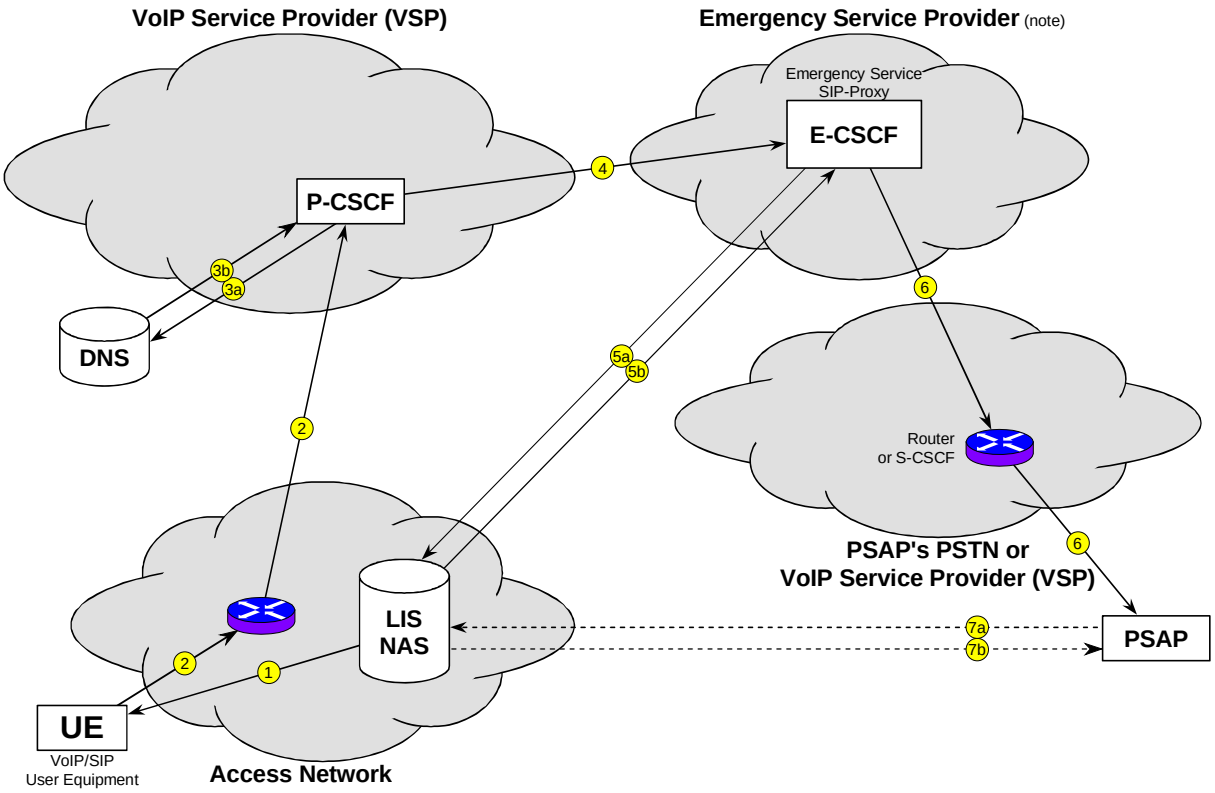


Figure 29: Step 2 of the Core IMS emergency calling architecture

1) At IP-login or at the end device's request, the IP-connectivity provider may provide to the end device a Location Information Element (LIE), which contains the precise Location Information (LI) or a Location Key (LK), for example, the local IP-address, and the local domain name. The IP-connectivity provider sends LIE updates to the end device whenever the LIE changes.

2) When a user makes an emergency call, the end device sends an INVITE for sos@LocalDomainName to the VoIP Service Provider's SIP-proxy. The INVITE may or may not contain a LIE.

3) The SIP-proxy authenticates the caller and recognizes the emergency call and then checks the INVITE to determine if the end device sent a LIE. If the INVITE did not contain a LIE, then the procedure continues as in the Step 1 architecture. If the INVITE contains a LIE, the SIP-proxy queries the DNS to determine the E-CSCF URI for this domain.

4) The SIP-proxy forwards the INVITE to the E-CSCF.

5) When an E-CSCF receives an INVITE for an emergency call it sends a query (HTTP/SOAP or HELD) which contains the LIE to the LIS. The LIS sends the precise Location Information or a Location Reference and the PSAP URI.

6) The E-CSCF routes the INVITE, which contains the Location Reference, to the PSAP.

7) The PSAP queries the LIS using HTTP/SOAP or HELD to get the precise Location Information.

10.3.3 Proposal for a Harmonized International Emergency Calling Architecture (NENA «i2», 3GPP IMS and DT Core IMS)

As described in clause 10.3.1, the proposal below is targeted to cover the NENA («i2»), 3GPP IMS and DT Core IMS models for emergency calling and to enable emergency calls for internationally nomadic users, without forcing the different countries to adopt completely new Emergency Calling models.

In this proposal, IP-connectivity providers which are not also 3GPP IMS providers must enter an SVR record containing a URI (for the E-CSCF or for the NENA VPC, depending on the national Emergency Calling model), which the VoIP Service Provider can contact when it receives an emergency call from an end device located in this domain.

The following paragraph describes the proposed procedure for a harmonized emergency calling:

1) IP-connectivity provider behaviour:

   At IP-login or at the end device's request, the IP-connectivity provider may provide to the end device a Location Information Element (LIE), which contains the precise Location Information (LI) or a Location Key (LK), for example, the local IP-address or the Cell-ID, and the local domain name. The IP-connectivity provider sends LIE updates whenever the LIE changes.

NOTE 1: IP-connectivity providers which comply to the NENA- or to the DT Core IMS Step2 model will send a LIE. IP-connectivity providers which comply to the 3GPP IMS or to the DT Core IMS Step 1 models will not send a LIE.

NOTE 2: IP-connectivity providers may use Layer 2 protocols, DHCP, PPPoE or GEOPRIV L7LCP [i.1] (draft-ietf-geopriv-l7-lcp-ps-07.txt) to provide the end device with the LIE.

2) End device behaviour

   The end device may receive a LIE from the IP-connectivity provider (with or without a request from the end device). The end device may also use any precise Location Information of which it is aware (for example, its GPS location) as a LIE.

   The end device must add to each LIE a tag containing the source of the LIE (IP-connectivity provider or end device itself).

   When the end user initiates an emergency call, the end device sends an INVITE for sos@LocalDomainName to its outbound SIP-proxy. The INVITE contains none, one or two LIEs.

   The DT proposal notes that 3GPP IMS end devices do not send a LIE and that other end devices may or may not send a LIE. The proposal also requires that non-3GPP IMS devices must send the international "sos" string (possibly with extensions) or the emergency calling dial strings known to the VoIP service provider (VSP).

NOTE 3: Emergency calling dial strings only have local significance and therefore may not be recognized by the VoIP service provider's SIP proxy.

3) SIP outbound proxy behaviour.

   The SIP outbound proxy is either a 3GPP IMS P-CSCF (and located in the Access Network) or the SIP-proxy of the VoIP service provider. When an outbound proxy receives and recognizes an emergency call, it takes following actions:

   - If the SIP outbound proxy is a 3GPP IMS P-CSCF and therefore in the Access Network, it is able to authenticate the caller, to determine the E-CSCF URI and the Location Information. The P-CSCF proceeds as specified by 3GPP.

NOTE 4: The P-CSCF receives the INVITE via the IPSec-tunnel which was set-up at the end device registration.

- If the outbound proxy is the VoIP service provider's SIP-proxy and therefore it is not in the Access Network, it authenticates the user and inspects the LIEs.
  - If the INVITE does not contain a LIE (the DT Core IMS Step 1 model), the SIP-proxy obtains the end device's public IP-address (for example, by using STUN), the domain name in which the end device is currently located and the E-CSCF URI using DNS and Reverse DNS. Then it routes the INVITE to the appropriate E-CSCF.
  - The SIP-proxy queries the DNS SRV record for emergency calling service of the local domain.
    - If the SRV record contains a NENA VPC URI, the SIP-proxy queries the VPC-directory using the LIE, to obtain the Location Reference (or ESQK) and the PSAP URI (or ESRN). Then the SIP-proxy sends the INVITE which contains the Location Reference (or ESQK) to the PSAP URI (or ESRN).
    - If the SRV record contains an E-CSCF SIP URI, the SIP-proxy sends the INVITE, which contains the LIE and the local domain name to the E-CSCF.

4) VPC behaviour:

- A NENA VPC-directory which receives a query behaves according to the NENA specifications. It returns the Location Reference (ESQK) and the PSAP URI (ESRN) to the SIP-proxy.

5) E-CSCF-behaviour:

- When an E-CSCF receives an INVITE for an emergency call it behaves as described in clause 10.3.2, Step 2.

6) PSAP behaviour:

- On receipt of an emergency call, the PSAP may request the precise Location Information using the Location Reference (ESQK). The Location Information may be stored at different servers, for example in the LIS, NENA VPC or E-CSCF data base, according to the national Emergency Calling model, national regulatory rules or with the bilateral agreements between the IP-connectivity provider and the E-CSCF-provider.

10.3.4 Additional Requirements to the TISPAN Emergency Calling Architecture

DT believes it cannot agree to adopt the NENA «i2» architecture and also defines some requirements with which it believes the TISPAN architecture and mechanisms for Emergency Calling should comply in order to be adopted in Germany.

10.3.4.1 NENA «i2» architecture drawbacks

1) The NENA «i2» architecture does not support the IMS model currently used by TISPAN and 3GPP. Many VoIP providers in Germany have developed NGN based on TISPAN/3GPP.

2) The current NENA «i2» architecture is based on the Emergency Calling infrastructure and model which already exists in the US, especially on the existence of a national Emergency Services Provider which runs a separate Emergency Services Provider Network and of the VPCs. There are countries in the EU where the Emergency Calling today is based on a similar model. For these countries, the NENA «i2» model is the model of choice.

   However, there are other countries like Germany where there is no national Emergency Services Provider. In Germany, the PSAPs currently use DT PSTN connectivity, but in the future they may also use other SIP providers. Today, PSTN carriers route emergency calls based on the area code (e.g. 069) in the Calling Party Number. The routing is done using a simple, static table which contains telephone area codes and phone number of the corresponding PSAP. PSAP phone numbers are hexadecimal and can not be dialled directly by end users. Carriers sending emergency calls to DT are responsible for the correctness of the Calling Party

Number and pay for the terminating of emergency calls according to the bilateral billing agreement. For the end users, the emergency calls are free of charge.

The adoption of the NENA «i2» architecture would require for Germany completely new infrastructure and billing models. This is not likely to happen any time soon. On the other side, with VoIP/IMS/NGN becoming more and more the technology of choice for telecommunication services, a compatible "up and running" Emergency Calling Service is needed soon.

3) For existing VoIP services, implementing NENA «i2» would require changes in the end- and intermediary-devices. Our experience is that many customers do software upgrades (also automatic upgrades) very seldom or not at all.

10.3.4.2 Requirements to the TISPAN Emergency Calling Architecture

The requirements for the architecture for Emergency Calling are identified below, they should:

R1: Support the migration to a full 3GPP IMS model (with a P-CSCF in the visited network) in the future.

R2: Enable the EU countries to provide VoIP Emergency Calling in the context of their existing organizations and billing models and by upgrading their existing infrastructure in steps. In particular, Emergency Calling must not assume the existence of a dedicated national Emergency Services Provider, otherwise the TISPAN architecture will probably not be adopted in some countries.

R3: Enable VoIP Emergency Calling for older end- and intermediary-devices.

R4: Enable the full compliance with the regulatory requirements of all EU countries.

R5: Support Emergency Calling for IMS implementations where the P-CSCF is located in the Home Network

R6: Support Emergency Calling for nomadic users on private networks which use a public VoIP service.

11 Developments in North America

The developments in North America are reflected in the IETF NENA ATIS approach (see clause 8).

12 Developments in Australia

Most of the text in this clause is derived from the "Report from the [Australian] IP Location Information Working Group" [12] but it is noted that much of the content is likely to be applicable elsewhere, particularly that in clause 12.3.

12.1 Location information options

A summary of the main long term options under consideration for location information when using a VoIP service are to develop a solution that:

1) is based on the current IP Multimedia Subsystem (IMS) architecture (developed in 3GPP/3GPP2/ETSI-TISPAN, see clause 7);

2) is based on an «i2»-style architecture (developed in NENA [4]) with eventual migration to an «i3»/IETF ecrit architecture (see clause 8);

3) is some hybrid of options 1 and 2 e.g. IMS for large, managed networks (i.e. fixed and/or mobile networks), «i2» migration to «i3»/ECRIT for any network and for interfacing with managed networks;

4) waits for the «i2»/NENA/«i3»/ecrit and IMS/3GPP approaches to converge;

5) is specific to Australia.

At present no single solution is recommended. Further guidance on the above options is as follows:

d) a preference between Option 1 and Option 2 would probably depend on one's starting assumptions about network architecture;

e) option 3 is a possible outcome in Australia, given previous examples of implementing more than one particular standards development e.g. Australia implemented multiple national CDMA and GSM networks;

f) option 4 is the "wait" option;

g) option 5 is not feasible, see further comments below.

Canada is progressing its implementation of IP location information with funding from the Canadian government for IT systems development. Other countries such as the USA and UK are also making progress on similar implementations. All are aligned with the activities of the National Emergency Number Association (NENA) in North America and the IETF.

12.2 Supplementary comments on the options

1) Current IMS (3GPP/3GPP2/ETSI-TISPAN) architecture.
This would suit the providers of large scale managed networks and other providers of networks and services that are based on the IMS architecture. It would require broadband providers to support a location determination function. There would be the associated need for roaming agreements between all IMS (VoIP) operators and all Internet access providers. It places a larger burden, and associated impediment to deployment, on broadband providers.

2) «i2», migration to «i3/ECRIT».
«i2» is based on an Internet services model supporting decoupling between the access provider and voice service provider. It has been defined in a North American context, is transitioning into deployment in the Canadian context and has momentum in the UK. An evolution of the Australian emergency network functionality can be laid out to work into this architecture. It may support accurate cellular caller location as well.

3) Hybrid.
A hybrid may offer a compromise between options 1 and 2 but will add complexity in implementation (e.g. tracking of multiple location information sources) and the potential duplication of resources. However the reality is that there are a number of 3G networks deployed or in development in Australia that will align with 3GPP specifications, and a number of networks that will look to implement a solution for location information based on IETF RFCs.

4) Wait for NENA and 3GPP to converge.
Liaison statements between standards development organizations (SDOs) indicate that there has been consideration of the various developments in different SDOs and there is likely to be some convergence between options 1 and 2 in future.

5) Australian specific - Not recommended.
There is no compelling evidence to suggest that the particulars of the Australian environment are any different from other environments. Such differences that may exist, due to regulatory or business legacy, are fairly second order and could be addressed without needing a unique architectural approach. As well, it would be inconsistent with Recommendation 8 of the DCITA Report [20] which refers to a "global solution".

12.3 Potential barriers to adoption

Potential barriers to adoption, and options for addressing those barriers, identified in the Working Group include:

1) Lack of incentive.
The lack of incentive for an ISP to support a Location Information Server (LIS) when the ISP does not offer a voice service. This may be addressed by extending the LIS application to non-voice services and creating a commercial benefit from maintaining the LIS e.g. payment per request for location information.

2) Privacy concerns.
Options for addressing these concerns include the use of:

   a) existing arrangements, because they may be adequate;

   b) an opt in/opt out choice for sending location information; and

   c) variable resolution e.g. full resolution for emergencies and law enforcement, moderate resolution for commercial interactions with a trusted organization, less resolution for commercial interactions with an unknown organization.

3) The maturity of international standards.

4) The development of available equipment.

5) The deployment of NGNs. The scope for Communications Alliance to speed up international activity is only limited by industry willingness to contribute resources to the international standards developments. Other options are to leave development and deployment to commercial incentives, or to drive deployment through policy decision(s).

6) The (in)accuracy of databases such as for cable records or DHCP information. This includes establishing and using processes to maintain the databases. A commercial benefit from the use of location based services can provide an incentive to maintain databases.

7) Achieving an acceptable level of location accuracy (which is linked to the need for database maintenance in vi above). This can be addressed by growing the number of trusted parties that also support the supply/transfer of location information.

12.4 The role of the access network(s)

12.4.1 The NGN access network

Access networks affect the available resolution for location information. For example, a network manager can more readily resolve location to:

a) a Digital subscriber line access multiplexer (DSLAM) port in a DSL network;

b) a head-end for a cable modem network; or

c) a base station for a mobile network,

than to identify the location of an individual device or end user.

A key point emerging from the above is the central role of network providers in the access link (e.g. infrastructure owner, DSL provider, ISP) in determining location. A core network is not able to determine a user's location. Also, the large number of endpoints, with substantial diversity in capability, cannot be relied upon to provide or to contribute to accurate location information. In contrast, location information linked to the access network offers the best balance of a smaller number of points of contact (than the number of endpoints), with more reliable information sources that are more likely to be kept up-to-date.

Location information resolution can be further improved by additional methods. For example, in a HFC cable network the cable from the head-end to customers' premises is shared among a number of users and DHCP may be used to dynamically allocate addresses. A database look up linking the allocated network address to a cable modem and then linking that cable modem to a customer's street address improves the resolution of location information from the cable head-end to the customer premises.

12.4.2 The NGCN access network

A trusted device can provide better resolution of location information. For example, a campus network might have a default location that identifies the position of the interface to a public network. If the campus is a trusted network, it can improve the provided location information through its more detailed knowledge of the campus network e.g. by maintaining a database with the location of individual network ports, by using a process for locating portable/mobile devices on campus.

12.5 Alignment of activity with International Standards Developments

The [Australian] IP Location Information Working Group based its findings on input received about the latest international activity on location information for emergency calls and telecommunications networks, from a number of international standards groups including:

- the National Emergency Number Association (NENA) in North America;
- the Open Mobile Alliance (OMA);
- the ATIS Emergency Services Interconnection Forum (ESIF) in North America;
- the 3rd Generation Partnership Project (3GPP);
- the 3rd Generation Partnership Project 2 (3GPP2); and
- liaisons between:
  - NENA and ESIF;
  - 3GPP and ESIF;
  - ESIF and 3GPP;
  - NENA and 3GPP2;
  - ATIS and 3GPP, 3GPP2,ETSI TISPAN, ETSI EMTEL, IEEE 802, IETF-ecrit, IETF-geopriv, IETF-ieprep, ITU-T SG13, OMA, TR-41.4 and TR-45.2.

13 Developments in the Far East

13.1 Developments in Japan

Most of the text in this clause is derived from the document "Emergency Call Requirements for IP Telephony Services in Japan" [13].

13.1.1 Introduction

Two types of public IP telephony services exist in Japan, the potentially nomadic "050" service (area code 050) and the service using E.164 style telephone numbers of the form "0AB-J", whose terminals are at known, fixed locations.

Japanese regulations require that the "0AB-J" type of IP telephony service adheres to the following:

- Provides voice quality equal to PSTN telephone.
- Enables the use of the emergency calls.
- Installed location of the IP telephone device is fixed and the devices are not portable.

No similar requirements exist for the IP telephony services of the "050" prefix type.

There is a general opinion, however, that emergency calls should be enabled also for the "050" type of IP telephony services (as is required for the "0AB-J" type of IP telephony service) as long as users consider these services as alternatives to the PSTN telephone.

A Committee for the Advancement of Emergency Message Systems (CAEMS) including ECC organizations, people with an academic background, the telecommunications carrier, the IP telephony equipment manufacturer, etc. was formed to advise the Ministry of Internal Affairs and Communications (MIC) on emergency calls from IP telephones. A draft proposal that outlines the service and functional requirements was compiled and submitted to public review. The final report that incorporates the public comments will be submitted to the minister of the MIC. The purpose of the present document was to provide requirements for the CAEMS to develop a detailed specification.

The CAEMS discussion assumed the following preconditions

- IP Telephony Network:

  There will be two types of network configuration:

  - ECCs are connected to IP network via PSTN using existing emergency lines, and
  - ECCs are connected directly to IP telephony network via a new IP line.

- Types of IP telephony services:

  - Fixed IP telephone.
  - Portable IP telephone.
  - IP telephone with mobile capability.

13.1.2 Emergency numbers

In Japan, there are three emergency telephone numbers:

110 - Police.

118 - Japan Coast Guard, and

119 - Fire station and ambulance.

Upon dialling one of these emergency numbers, the emergency call is established directly to the organization that handles the particular type of emergency for the area from which the call originates.

Emergency calls can be established to:

- Police (110):
  52 head offices (1 in each 47 prefectures, except 2 in Tokyo and 5 in Hokkaido);
- Japan Coast Guard (118):
  11 jurisdictions;
- Fire station and ambulance (119):
  Slightly less than 900 districts (defined locally along with the district of about 3 000 municipalities).

13.1.3 IP Telephony Requirements for Emergency Calls

13.1.3.1 Basic requirements

The following list provides the basic requirements for the support of emergency calls from IP telephones in Japan:

1) Emergency calls MUST be delivered to the correct Emergency Call Centre (ECC), which covers the area from where the emergency call originates.

2) Emergency calls MUST be redirected to an alternative ECC that the organization designates as an alternative in case the original ECC is unable to answer the call.

3) Information for identifying the network operator that can provide the caller's subscription information MUST be presented to ECC.

4) Emergency calls MUST NOT be released even if the caller hangs up; they can be released only by the ECC, not by the caller.

5) The emergency call originating terminal MUST be made ringing if the ECC intends to resume the call during "keeping connection" is activated; another call in progress MUST be released (reversing call).

6) If the ECC places the emergency caller on hold, intending to resume the call, the terminal originating the emergency call MUST be given ringing tone and prevented from accepting another incoming call.

7) The caller's CLI MUST be presented to ECC even if the caller activated CLIR.

8) Location Information of the terminal that originated the emergency call MUST be presented to ECC.

9) The Location Information MUST consist of (see clause 13.1.3.2):

- for fixed IP-phone:
  subscriber's name, address, address code and telephone number;

- for portable/mobile IP-phone:
  subscriber's name, geographical location information, telephone number, and mobile-use or not.

10) Emergency call MUST have priority over all other calls.

11) Operators MUST prevent malicious calls supplying incorrect geographical location of the origin of the emergency call.

13.1.3.2 Acquiring and presenting geographical location information

In Japan, there is a requirement for geographical location information of the caller to be presented to the ECC that answers the call when the ECC requests this information from the IP telecommunication provider.

Two methods are foreseen:

- two separate connections between the ECC and the IP service provider, one for the emergency call itself and a second to request the geographical location information; or

- a single connection is established for both the emergency call and the associated geographical location information.

HTTP (Hyper Text Transfer Protocol) is used for transferring the geographical location information; the latter is formatted using XML (eXtensible Markup Language).

The content of the location information must be accurate enough such that the fire department, the police, or ambulance are able to respond to the emergency promptly.

The following three tables show the contents of the location information.

Table 8: The location information for a fixed IP telephone

Element	Tag	Comment
Caller ID	repo_tele	caller's telephone number
Address	add_area	caller's address
Zip code	add_post	postal code number
Address code	add_code	JIS (Japanese Industrial Standard) address code
Address name	add_name	literal information corresponding to the address code (name of prefecture, city or county, etc.)
Address number	add_num	house number, street number etc.
Others	add_others	house name, building number, room number, or building name and floor
Name	name_area	caller's name
Name in kana	name_kana	pronunciation of caller's name
Name in kanji	name_kanji	caller's name in kanji letters

Table 9: The location information for a nomadic IP telephone

Element	Tag	Comment
Caller ID	repo_tele	caller's telephone number
Location	loc_area	caller's geographical location information
Zip code	loc_post	postal code number
Address code	loc_code	JIS (Japanese Industrial Standard) address code
Address name	loc_name	literal information corresponding to address code (name of prefecture, city or county, etc.)
Address number	loc_num	house number, street number etc.
Others	loc_others	house name, building number, room number, or building name and floor
Name	name_area	caller's name
Name in kana	name_kana	pronunciation of caller's name
Name in kanji	name_kanji	caller's name in kanji letters

Table 10: The location information for the mobile IP telephone

Element	Tag	Comment
Caller ID	repo_tele	caller's telephone number
Terminal type	term_type	whether caller's terminal is fixed- use or mobile-use
Location type	loc_type	indicating either location of dispatch information or present location information
Location	loc_area	caller's geographical location information
Zip code	loc_post	postal code number
Address code	loc_code	JIS (Japanese Industrial Standard) address code
Address name	loc_name	literal information corresponding to address code (name of prefecture, city or county, etc.)
Address number	loc_num	house number, street number etc.
Others	loc_others	house name, building number, room number, or building name and floor
Measured position	CircularArea	circular area including measured position
Latitude	X	latitude of Centre of CircularArea
Longitude	Y	longitude of Centre of CircularArea
Radius	Radius	radius of CircularArea
Altitude	Alt	altitude of caller's location(optional)
Precision of Altitude	alt_acc	precision of Altitude (optional)
Name	name_area	caller's name
Name in kana	name_kana	pronunciation of caller's name
Name in kanji	name_kanji	caller's name in kanji letters

13.1.4 Japanese address code for location information

The address code is used as one element of the location information that is transferred as a geographical location information to an ECC as described in clause 13.1.3.2. It is an 11-digit code, which consists of a 2-digit prefecture code, a 3-digit municipality code, a 3-digit section code and a 3-digit subsection code. Currently, approximately 500 000 codes are registered.

Table 11: Structure of the address code

Digit	Name of code	Value	Remarks
1 and 2	prefecture code	01- 47	prefecture
3-5	municipality code	100-199 201-299 301-799	ward (in an ordinance-designated city) and special-ward city other than above town and village (in a district)
6-8	section code	001-999 10A-99Y(note)	section of a municipality and by-name of an area
9-11	subsection code	001-099	"Chome" that divides a section
		101-849	by-name of an area
		851-899	it is used when areas that are shown in the same place name have different postal codes
		901-999	for address name of Kyoto City
NOTE: The capital letters of the Roman alphabet are also used on 8th digit. In order to prevent misreading them as numerals, 'O', 'I', 'S' and 'Z' must not be used there.			

13.2 Other developments

No other developments are known.

14 Problems solved and unsolved

14.1 Problems solved

14.1.1 NGCN with Location Acquisition Protocol

As discussed in clause 6.4, the acquisition of location information during emergency calls can be resolved. This is dependent on the following required points:

- The location of Ethernet wall sockets are listed in an electronically accessible database, the location, in addition to a local grid (building number, floor, room number, etc.), could be maintained also in geodetic form.
- The location of Wi-Fi base stations are listed in an electronically accessible database, the location, in addition to a local grid (building number, floor, room number, etc.), could be maintained also in geodetic form.
- The location of DECT base stations are listed in an electronically accessible database, the location, in addition to a local grid (building number, floor, room number, etc.), could be maintained also in geodetic form.
- The DHCP server traces all requests for a temporary IP address through the NGCN using methods to determine the origin, e.g. deploying the "DHCP Relay Agent Information Option" (RFC 3046 [7]).
- The DHCP server communicates the location (in civic or preferably in geodetic form) to the UE.
- The UE includes the location information from its GNSS device (if available and operational in the specific environment (tunnels, large buildings, etc.) in the emergency call establishment (INVITE).
- The UE includes the location information received from the DHCP server in the emergency call establishment.

and most of all:

- This is dependent on the existence of a regulatory requirement that NGCNs maintain their information in the LIS; inaccurate location information from the LIS might harm human life!

14.1.2 Cascading networks

Cascading networks are discussed in clause 6.4, the acquisition of location information during emergency calls can be resolved. This is dependent on the following points (in addition to the ones in clause 14.1.1):

- LISs (Location Information Servers) exist at each level in the cascade.
- The LISs are able to communicate with each other to guarantee the best location information during an emergency session.

and most of all:

- This is dependent on the existence of a regulatory requirement that NGCNs maintain their information in the LIS in an international environment; inaccurate location information from the LIS in any part of the worldwide NGCN might harm human life!

14.1.3 Geodetic or civic location information

Geodetic addresses are concise and therefore require few resources in transport. They also are transmitted with variable accuracy and, therefore, are able to reflect the knowledge of the vagueness of the information.

For little costs, a visual translation from geodetic address to a civic visual map information is easily available (if nothing else, Google Map should do). The transformation into a visual map should be sufficient for despatching rescue forces in the appropriate direction. Further, more accurate location information obtained from LISs can later improve the destination of the emergency intervention.

14.1.4 Conversions from geodetic to civic addresses are country specific

The conversion from geodetic to civic addresses is easily achieved when using a map where the location is displayed as a transparent icon. For despatching emergency response teams satellite or aerial derived images, when tied to the WSG84 datum - are sufficient.

For closer zoom-ins the resolution of satellite data is insufficient. For such purposes, cadastral (location) information would need to be rendered in image form; with each modification in the real world, (e.g. construction of new buildings, major additions to existing buildings, removal of buildings, new roads, etc.) the images for the ECCs and emergency response teams require updating.

14.1.5 From TDM based to IP based NGN emergency communication

3GPP provides a migration path from TDM based emergency handling to IP based emergency communication (see [1] clause 5.1 or clause 7.1 and figure 22). Eventually, the TDM paths and equipment will be replaced by NGN paths and equipment in a graceful progression.

14.2 Problems unsolved

14.2.1 GNSS receipt inside buildings or tunnels

GNSS reception is not possible in tunnels and difficult inside buildings. Unfortunately, this inadequacy correlates with the fact that in such locations, emergencies (e.g. fire) are critical and dangerous and require prompt intervention.

Possible solutions to remedy the situation are:

1) Linear tunnels (e.g. roads, railways, etc.):
   Leaky antennas might measure «round trip delay» like base stations (mobile, DECT) or Wi-Fi access points; an estimate of the location in the tunnel can be derived.

2) Tunnel systems (e.g. underground metro systems):
   Leaky antennas deployed in sectors may indicate the sector and a «round trip delay» derived location thus also providing an estimate of the location in the tunnel.

3) Large buildings (possible solution):
   Seeded by stationary equipment at known geodetic locations, user equipment may cooperate as a self organizing network to derive geodetic location with enough accuracy for emergency purposes (see annex D).).

14.2.2 "Tree and Branch" scenarios

Any "tree and branch" structured distribution network with a head end and one or more levels of branching (such as WiMAX, TV cable systems, etc.) suffer the possibility that UE may be moved by the end user without the knowledge of the network operator. The recorded location of the UE might, therefore, not coincide with the location from which it is used to initiate an emergency session.

14.2.3 VPN tunnels

VPN tunnels by their nature bypass any systems en route from the UE to the home network (see clause 6.5). This may be realized by the user of the UE; however, other people may try to use the UE in an emergency situation; where this emergency call terminates is likely not the PSAP responsible for the area.

14.2.4 Accuracy of location information in the LIS

The use of «Proxy LISs» is described in clauses 8.5 (figure 27) and 6.4 (figure 19). These «Proxy LISs» play an important role when providing location information known to NGCNs to PSAPs. The quality of the location information reflects the sincerity with which the LIS information is maintained.

This might remain a regulatory issue; but there remains some doubt as to whether national regulators can enforce the appropriate updating of the «Proxy LISs», particularly those in private networks extending beyond national boundaries.

Annex A (informative): Recommendation of the Commission (2003/558/EC)

The Recommendation of the Commission (2003/558/EC [14]) of 25 July 2003 on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services is reproduced here in full, for information.

A.1 Considerata

Having regard to the Directive 2002/21/EC [i.10] on a common regulatory framework for electronic communications and services (the "Framework Directive") (OJ L 108, 24.4.2002, p. 33. See note) and in particular Article 19 thereof,

Whereas:

1) Decision 91/396/EEC [i.11] on the introduction of a single European emergency call number (OJ L 217, 6.8.1991, p. 31.See note) required Member States to ensure that the number 112 was introduced in public telephone networks as the single European emergency call number by 31 December 1992, with under certain conditions, a possibility for derogation until 31 December 1996.

2) Directive 2002/22/EC [i.12] on universal service and users' rights relating to electronic communications networks and services (the "Universal Service Directive") (OJ L 108, 24.4.2002, p. 31. See note), requires public telephone network operators (hereafter "operators") to make caller location information available to authorities handling emergencies, to the extent technically feasible, for all calls made to the single European emergency call number 112. Directive 2002/58/EC [i.13] concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "Directive on privacy and electronic communications") (OJ L 201, 31.7.2002, p. 37. See note) establishes that providers of public communications networks and services may override the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organizations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

3) Although this Recommendation is concerned with location- enhanced 112, it is understood that parallel national emergency call numbers will be enhanced with the same functionality and following the same principles. Organizations operating private telecommunication installations are not affected by this Recommendation.

4) For the successful implementation of E112 services throughout the Community, implementation issues must be addressed and timescales for the introduction of new systems coordinated. The Coordination Group on Access to Location Information by Emergency Services (CGALIES) established by the Commission in May 2000 as a partnership of public service and private sector players has allowed players of different sectors to discuss and find agreement on the principles for harmonized and timely implementation.

5) Following on from the recommendation by CGALIES, providers of the public telephone network or service should use their best effort to determine and forward the most reliable caller location information available for all calls to the single European emergency call number 112.

6) During the introductory phase of E112 services, application of the best efforts principle is considered preferable to mandating specific performance characteristics for location determination. However, as public safety answering points and emergency services gain practical experiences with location information, their requirements will become more defined. Moreover, location technology will continue to evolve, both within mobile cellular networks and satellite location systems. Therefore, the best effort approach will need to be reviewed after the initial phase.

7) It is important for all Member States to develop common technical solutions and practices for the provision of E112. The elaboration of common technical solutions should be pursued through the European standardization organizations, in order to facilitate the introduction of E112, create interoperable solutions and decrease the costs of implementation to the European Union.

8) A harmonized solution across Europe would serve interoperability for advanced safety applications, such as calls which can be originated manually or automatically by an in-vehicle telematics terminal. These calls can provide additional information, for instance on the number of passengers in a car or bus, on compass-direction, on crash-sensor indicators, on the type of load of dangerous goods or on health records of drivers and passengers. With the high volume of cross-border traffic in Europe, there is a growing need for a common data transfer protocol for passing such information to public safety answering points and emergency services in order to avoid the risk of confusion or a wrong interpretation of data passed.

9) The arrangements for forwarding location information by operators to public safety answering points should be established in a transparent and non-discriminatory way including, where appropriate, any cost aspects.

10) The effective implementation of location-enhanced emergency call services requires that the caller's location as determined by the provider of the public telephone network or service is transmitted automatically to any appropriate public safety answering point that can receive and use the location data provided.

11) Directive 2002/58/EC [i.13] concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "Directive on privacy and electronic communications") generally requires that privacy and data protection rights of individuals should be fully respected and adequate technical and organizational security measures should be implemented for that purpose. However, it allows the use of location data by emergency services without consent of the user concerned. In particular, Member States should ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or service may override the temporary denial or absence of consent of a user for the processing of location data, on a per-line basis for organizations dealing with emergency calls and that are recognized as such by a Member State.

12) Actions conducted in the context of the Community action programme in the field of Civil Protection (hereinafter "Civil Protection Action Programme") (OJ L 327, 21.12.1999, p. 53. See note) should aim to contribute to the integration of civil protection objectives in other Community policies and actions as well as to the consistency of the programme with other Community actions. This entitles the Commission to implement actions aiming at increasing the degree of preparedness of organizations involved in civil protection in the Member States, by enhancing their ability to respond to emergencies and improving the techniques and methods of response and immediate aftercare. This may include the handling and use of location information associated to E112 emergency calls by public safety answering points and emergency services.

13) To achieve the objectives of this Recommendation, the need for a continued dialogue between public network operators and service providers and public authorities including emergency services becomes even stronger.

14) When reporting on the situation of E112 implementation, national authorities should address any relevant technical feasibility issue that hinders the introduction of E112 for specific categories of end-users, as well as the technical requirements for handling emergency calls that may originate from SMS and telematic data services.

15) The measures set out in this Recommendation are in accordance with the advisory opinion of the Communications Committee set up by Article 22 of Directive 2002/21/EC [i.10].

A.2 Recommendation

1) Member States should apply the following harmonized conditions and principles to the provision of caller location information to emergency services for all calls to the single European emergency call number 112.

2) For the purposes of this Recommendation, the following definitions should apply:

   (a) "emergency service" means a 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;

   (b) "location information" means in a public mobile network the data processed indicating the geographic position of a user's mobile terminal and in a public fixed network the data about the physical address of the termination point;

(c) "E112" means an emergency communications service using the single European emergency call number, 112, which is enhanced with location information of the calling user;

(d) "public safety answering point" means a physical location where emergency calls are received under the responsibility of a public authority.

3) Member States should draw up detailed rules for public network operators, to include, inter alia, the provisions in points 4 to 9 below.

4) For every emergency call made to the European emergency call number 112, public telephone network operators should, initiated by the network, forward (push) to public safety answering points the best information available as to the location of the caller, to the extent technically feasible. For the intermediate period up to the conclusion of the review as referred to in point 13 below, it is acceptable that operators make available location information on request only (pull).

5) Fixed public telephone network operators should make available the installation address of the line from which the emergency call is made.

6) Public telephone network operators should provide location information in a non-discriminatory way, and in particular should not discriminate between the quality of information provided concerning their own subscribers and other users. In the case of the fixed networks, other users include users of public pay phones; in the case of mobile networks or mobility applications, other users include roamers or visiting users, or, where appropriate, users of mobile terminals which can not be identified by the subscriber or user number.

7) All location information provided should be accompanied by an identification of the network on which the call originates.

8) Public telephone network operators should keep sources of location information, including address information, accurate and up-to-date.

9) For each emergency call for which the subscriber or user number has been identified, public telephone network operators should provide the capability to public safety answering points and emergency services of renewing the location information through a call back functionality (pulling) for the purpose of handling the emergency.

10) In order to facilitate data transfer between operators and public safety answering points, Member States should encourage the use of a common open interface standard, and in particular for a common data transfer protocol, adopted by the European Telecommunications Standards Institute (ETSI), where available. Such a standard should include the necessary flexibility to accommodate future requirements as they may arise, for instance from in-vehicle telematics terminals. Member States should ensure that the interface is best suited to the effective handling of emergencies.

11) In the context of the obligation for E112 services prescribed by the Universal Service Directive, Member States should provide adequate information to their citizens about the existence, use and benefits of E112 services. Citizens should be informed that 112 connects them to emergency services all across the European Union and that their location will be forwarded. They should also be informed about the identity of the emergency services that will receive their location information and of other necessary details to guarantee fair processing of their personal data.

12) In the context of the continuous evolution of concepts and technologies, Member States are encouraged to foster and support the development of services for emergency assistance, for instance to tourists and travellers and for the transport of dangerous goods by road or rail, including handling procedures for forwarding location and other emergency or accident related information to public safety answering points; to support the development and implementation of common interface specifications in ensuring Europe-wide interoperability of such services; and to encourage the use of location technologies with high precision such as third generation cellular network location technologies and Global Navigation Satellite Systems.

13) Member States should require their national authorities to report to the Commission on the situation of E112 implementation by the end of 2004 so that the Commission can undertake a review taking into account the emerging requirements from public safety answering points and emergency services and the evolutions and availability of technological capabilities for location determination.

14) This Recommendation is addressed to the Member States.

NOTE: Done at Brussels, 25 July 2003. For the Commission. Erkki LIIKANEN Member of the Commission.

Annex B (informative): List of Technology Recommendations

B.1 Location information format

The IETF's Presence Information Data Format - Location Object (PIDF LO) has emerged as the primary option for defining location information format. PIDF-LO permits the location information to be provided as either a civic (e.g. street) address or geodetic information (e.g. latitude/longitude plus uncertainty).

PIDF-LO is defined in RFC 4119 [10]. IETF RFCs that complement RFC 4119 [10] include RFC 3825 [8], which defines the DHCP option for "coordinate-based" (e.g. geodetic) location Information, and RFC 4676 [i.8], which defines the DHCP option for civic address information.

RFC 4119 [10] is also referenced as an example in the definition of "Geographical Location Information" in TS 123 167 [1].

B.2 Location information acquisition protocol

The protocol specified in the NENA «i2» architecture for the acquisition of PIDF-LO is the HTTP Enabled Location Delivery (HELD). HELD is used by a device to query its location on a network and is independent of network type. The Open Mobile Alliance specified application protocols "Mobile Location Protocol" (MLP) and "Secure User Plane Location" (SUPL) for use in mobile networks.

B.3 Signalling/transfer of location information

The definition of PIDF-LO information is independent of the choice of signalling. The following signalling procedures are able to transport location information:

- the Session Initiation Protocol (SIP is able to transfer PIDF-LO);
- 3GPP specifications (3GPP includes PIDF-LO as an example in TS 123 167 [1]); and
- PIDF-LO can also be sent in HTTP to a web service.

B.4 Related Conventions/Standards

Related working groups/standards that might be of use in bilateral agreements include:

1) IETF activity in the Geographic Location/Privacy (geopriv) Working Group.
2) IETF activity in the Emergency Context Resolution with Internet Technologies (ecrit) Working Group.
3) ETSI-TISPAN activity in Emergency Telecommunications (EMTEL).
4) ETSI TS 123 167 [1] (V7.6.0): "Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) emergency sessions (3GPP TS 23.167 version 7.6.0 Release 7).
5) The Geocoded National Address Format (G NAF).
6) AS/NZS 4819:2003 [i.6] Geographic information - Rural and urban addressing.

See also the list of URLs and references in Annex C.

Annex C (informative): URLs and References

C.1 Organizations

ATIS Emergency Services Network Interfaces Task Force (ESIF): http://www.atis.org/esif/index.asp

National Emergency Number Association (NENA): http://www.nena.org/

ETSI Emergency Telecommunications (EMTEL): http://www.emtel.etsi.org/overview.htm

IETF Emergency Context Resolution with Internet Technologies (ecrit) Working Group: http://www.ietf.org/html.charters/ecrit-charter.html

IETF Geographic Location/Privacy (geopriv) Working Group: http://www.ietf.org/html.charters/geopriv-charter.html

C.2 Documents

Public Sector Mapping Agency (PSMA) Australia Geo-coded National Address File (G-NAF).
Information on G-NAF is available from: http://www.psma.com.au/g-naf/

AS/NZS 4819:2003 [i.6].

IETF RFC 3693 [i.7].

IETF RFC 3825 [8] DHCP option for Coordinate-based Location Configuration Information.

IETF RFC 4119 [10] A Presence-based GEOPRIV Location Object Format.

IETF RFC 4676 [i.8].

NENA "NENA VoIP [i.9].

ETSI TS 123 167 [1].

Annex D (informative): Location determination without GNSS

D.1 Self-Organizing position determination in Ad-Hoc networks

Node positioning in ad-hoc networks has been a research topic for several years. This clause summarizes one approach that has been elaborated at the Swiss Federal Institute of Technology (EPFL). The project investigates large area, wireless, mobile networks referred to as mobile ad-hoc wide area networks [i.2]. The main design points of the project are to eliminate any infrastructure and to build a decentralized, self-organized and scalable network where nodes perform all networking functions (traditionally implemented in backbone switches/routers and servers).

This clause summarizes an algorithm for GNSS-free positioning of the nodes in an ad-hoc network [i.1]. This shows that in the scenarios where an infrastructure does not exist and GNSS cannot be used, there is a way to obtain positions of the nodes by distributed processing. GNSS-free positioning is desirable, notably when the GNSS signal is too weak (e.g. in-doors), or if for cost or integration reasons the inclusion of a GNSS receiver has to be avoided.

The algorithm described is referred to as the Self-Positioning Algorithm (SPA) and is based on the Time of Arrival (TOA) method to obtain the distance between two participating devices. Despite the range measurement errors, and the motion of the nodes, the algorithm provides enough stability and location accuracy to sustain basic localization functions.

NOTE 1: The project described in [i.1] does not use GNSS at all. Nevertheless, the Self-Positioning Algorithm provides enough information to every node to support Location Aided Routing [i.3] and Geodesic Packet Forwarding [i.4]; this is based on the relative coordination system derived by the algorithm. On the other hand, nodes that know their position in a fixed coordinate system, e.g. WGS84, provide anchors and seeds to allow all other participating nodes to derive their location within the fixed coordinate system.

NOTE 2: For convenience, in this clause the term "node" is used to designate "user equipment" and all nodes participating in the algorithm are called the "cluster". In addition, the term "one-hop neighbour" designates nodes that can communicate directly, i.e. in one hop.

D.1.1 Step 1 - Time synchronization

This step is not discussed here; methods are publicly available. It is sufficient that the clock is set to a time common to the cluster. A clock running at 1 GHz provides for a distance measurement resolution of 300 mm. Considering that DECT, Wi-Fi, etc. typically cater for a maximum range of 300 m (factor 1 000) not more than 16 bits would be needed for the clock data; these 16 bits could be the lower part of a UTC time string.

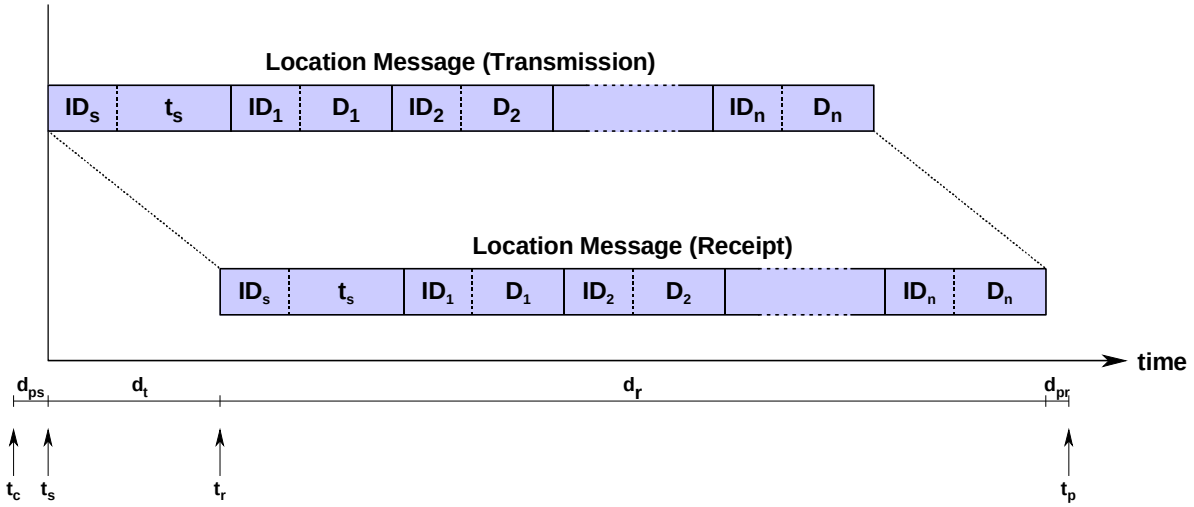
D.1.2 Step 2 - Local coordinate system

In this step, the node becomes the centre of its own coordinate system with the position (0, 0) and the positions of its neighbours are computed accordingly. The algorithm works under the assumptions that all wireless links between the nodes are bidirectional and that the nodes make no use of information from directional antennae. It should be noted that many nodes will use omnidirectional antennae and that links may be unidirectional due to differing signal strengths; such links are not used by the algorithm.

Every node periodically broadcasts a location message with the following information:

- the node's ID and the time of the start of transmission of the message; and
- for all one-hop neighbours their ID and the measured distance.

When a location message is received, the ID of the sender is remembered and the distance of the sender is computed based on the transit delay as shown in figure 30.



Legend:

t_c	Start compose time	d_{ps}	Sender processing delay	ID_s	Sender's ID
t_s	Start transmit time	d_t	Transit delay	ID_n	Sender's one-hop neighbour ID
t_r	Start receive time	d_r	Message receive delay	D_n	Distance between sender and its
t_p	Start processing time	d_{pr}	Receiver processing delay		one-hop neighbour

Figure 30: Receipt of a location message

The processing delay of the sender can be estimated by the sender and used to offset the timestamp before insertion into the message body. The receive delay can be computed by dividing the message length (including preambles, CRC, etc.) by the transmission rate. Finally, the receiver processing delay can be estimated by the receiver itself and considered when deriving the "start receive time" t_r and the transit delay.

With this procedure, every node knows its one-hop and some of the two-hop neighbours and some of the distances between them. A number of distances cannot be obtained due to the power range limitations or the obstacles between the nodes. Figure 31 shows node A at the origin and its one-hop neighbours and some of its two-hop neighbours. Continuous lines represent the known distances between the nodes.

Selecting two nodes P and Q that are also one-hop neighbours of each other leads to the determination of the local coordinate system as follows:

- Node A is placed at the origin.
- Node P is on the x-axis, and
- The y-coordinate of node Q is positive.

The coordinates of nodes A, P, and Q are shown in table 12.

Table 12: Initial coordinates in the local coordinate system

Node	x-coordinate	y-coordinate
A	0	0
P	D_{AP}	0
Q	$D_{AQ} \bullet \cos \gamma$	$D_{AQ} \bullet \sin \gamma$
NOTE: γ is derived from the distances D_{AP}, D_{AQ}, and D_{PQ} using the cosine rule of triangles.		

The coordinates of other one-hop neighbours can be computed if at least three other nodes exist whose coordinates are already known and the distance to the new node is known as well (see clause D.1.4).

The coordinates of node W in figure 31 cannot be computed, node W could lie anywhere on the dashed arc.

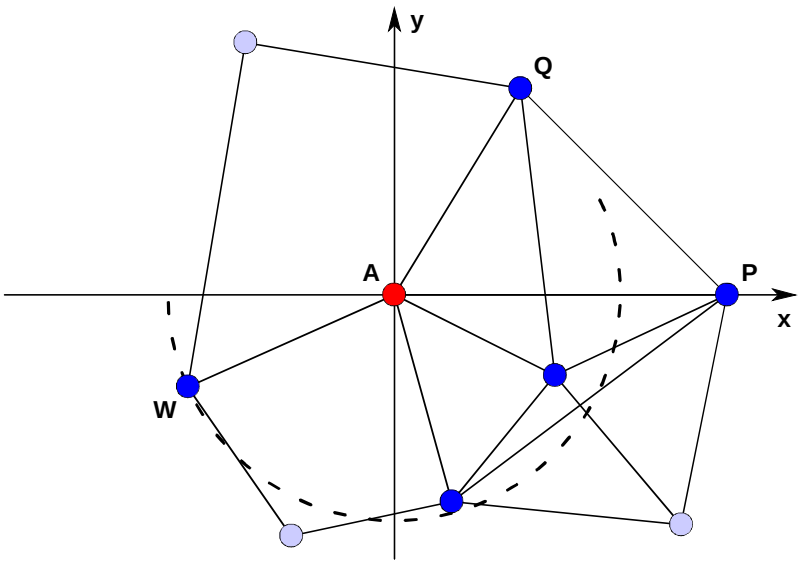


Figure 31: Local coordinate system

D.1.3 Step 3 - Network coordinate system

The local coordinate systems are, in general, not aligned. In order to achieve common network coordinate systems, the different local coordinate systems must be rotated and perhaps also mirrored. In figure 32, the direction of node B in node A's local coordinate systems is at angle α, the opposite direction from node's B view at angle β. Angle α needs to be communicated to node B that the can rotate its coordinate system by $\beta-\alpha+\pi$.

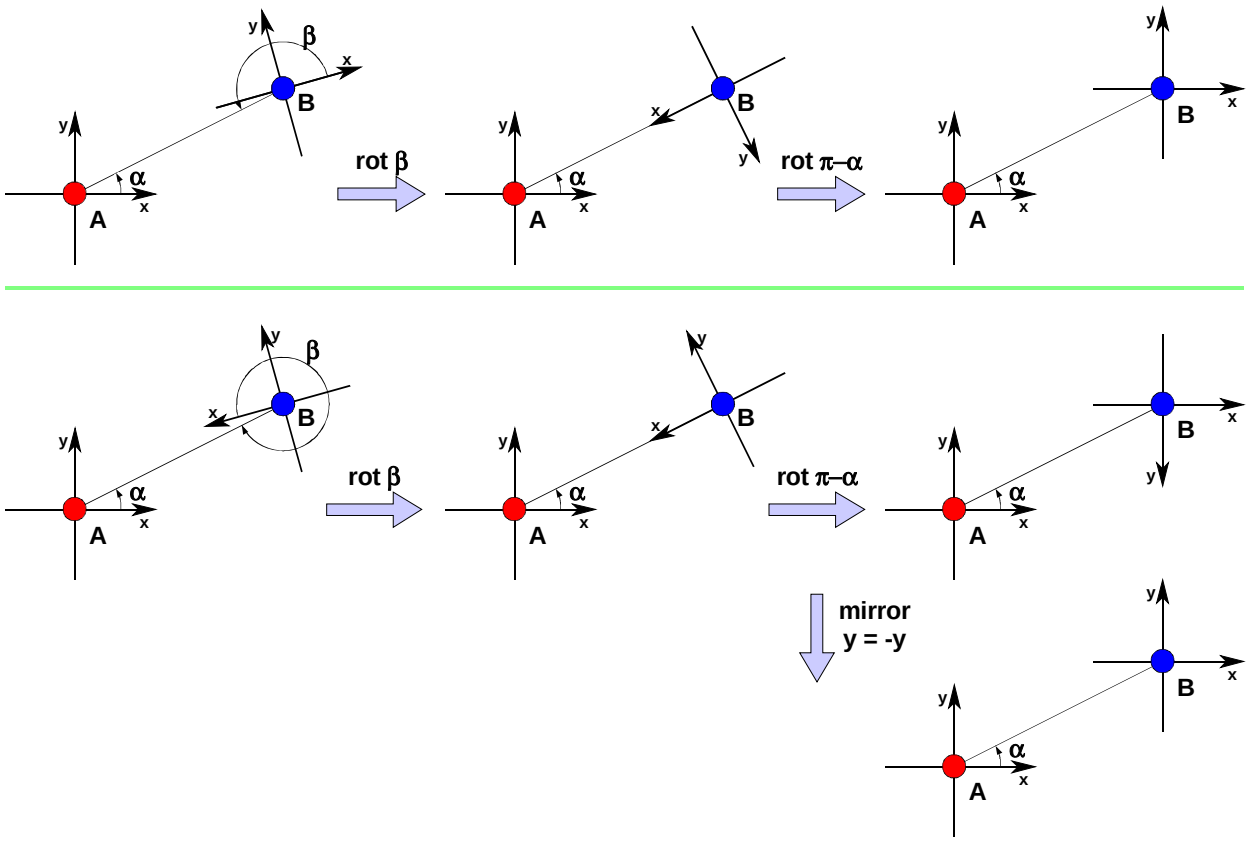


Figure 32: To mirror or not to mirror, two procedures for aligning local coordinate systems

For the determination whether the y-coordinates need to be mirrored, a third node C is required. The mechanism is illustrated in figure 33 (4a and 4b show the case without mirroring, 4c and 4d with mirroring). The algorithm is as follows:

- **if** (α_C-α_B < π **and** β_C-β_A > π) **or** (α_C-α_B > π **and** β_C-β_A < π) **then** mirroring is not required; and
- **if** (α_C-α_B < π **and** β_C-β_A < π) **or** (α_C-α_B > π **and** β_C-β_A > π) **then** mirroring is required.

The mirroring procedure is required because of the arbitrary decision for the y-coordinate of node Q to be positive (see clause D.1.2).

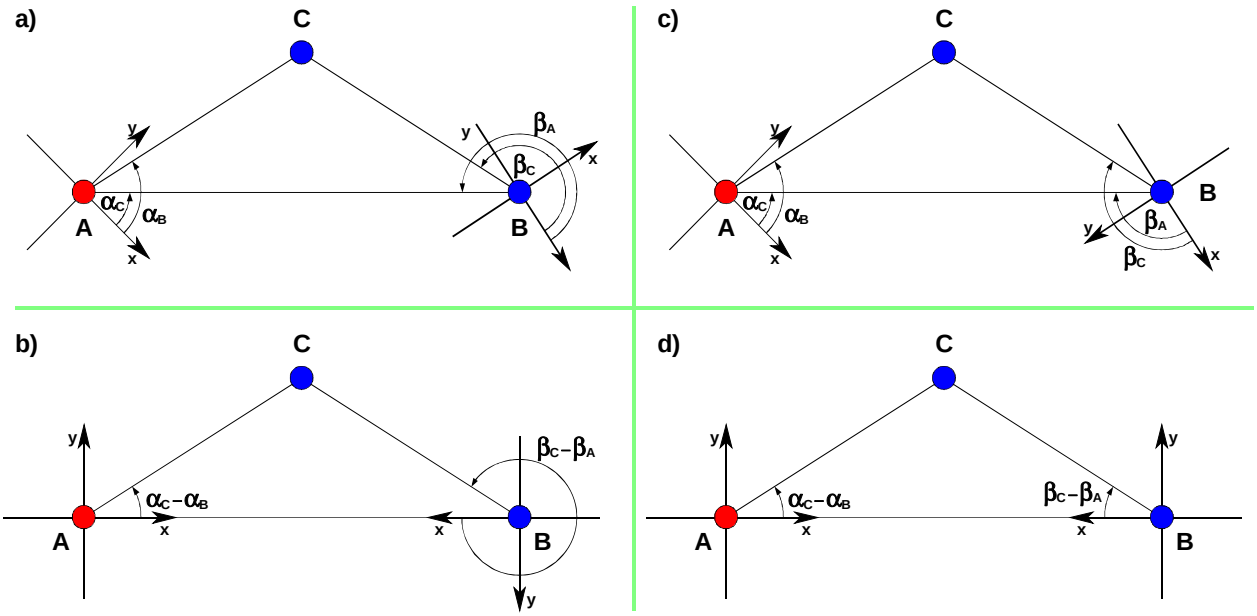


Figure 33: Determination whether mirroring of the y-coordinate is required

The complete procedure is as follows: Node A, B, and C are all one-hop neighbours of each other and know their distances from each other. A instructs B to adjust its coordinate system by giving node B the identity of node C, the angle α_B, and the coordinates of node B in node A's coordinate system. Node B knows α_C-α_B and β_C-β_A from the triangle A B C. Node B also knows β_A through A's coordinates in C's system. Node C has all information to rotate and possibly mirror its coordinate system to align it with node A's. Finally, node B translates its coordinate system by the coordinates supplied by node A, thus, making its coordinate system equal to node A's.

D.1.4 The anchor and the seed

In self-organizing networks, e.g. sensor networks, it is usually sufficient to know the relative location of the individual nodes, no relation to any defined grid, e.g. the World Geodetic System (WGS84), is required. On the other hand, the UE's position is valuable for emergency sessions especially if a wireless path exists between the customer premises network and the UE.

If the UE is connected to a wall socket, the location of this wall socket, maintained by the customer premises network infrastructure is sufficient for emergency sessions.

Wireless paths are based on equipment that is called "access point", "base station", etc.; this equipment must participate in the Self-Positioning Algorithm. The access point is a natural anchor for the self-organization of the network by providing its known location.

The algorithm requires a numeric location for the access point, e.g. the World Geodetic System (WGS84) or regional numeric coordinate system.

Unfortunately, having just one anchor point provides not enough information to the Self-Positioning Algorithm to allow the network coordinate system to be congruent with the numeric coordinates of the access point (see figure 34 where node N could be anywhere on a circle/sphere around the access point). Further equipment is required to provide additional known points (one to three). This equipment does not need the functionality of an access point, it suffices that it is at a known location and that it participates in the Self-Positioning Algorithm to act as a seed for the establishment of a congruent network coordinate system.

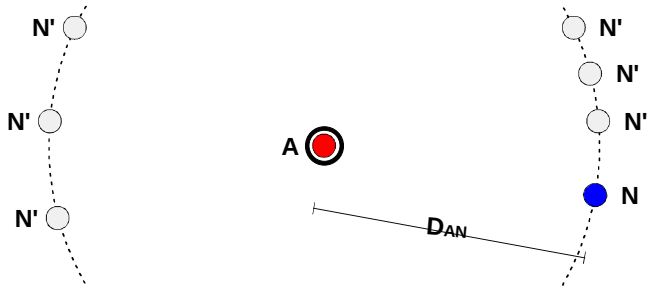


Figure 34: Distance to one node with known coordinates

NOTE 1: One seed (in addition to the anchor) is sufficient if all UEs are on one side of the "access point - seed" axis and no height component is required (see figure 35).

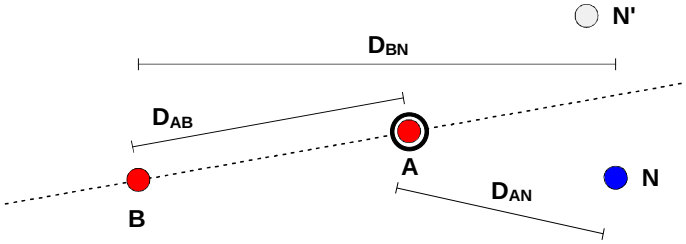


Figure 35: Distance to two nodes with known coordinates

NOTE 2: Two seeds are sufficient for determination of the location if no height component is required (see figure 36). It is further required that the access point and the two seeds do not lie in a line.

NOTE 3: If height is an essential element for emergency locations, three seeds are required. It is further required that the access point and the three seeds do not lie in a plane.

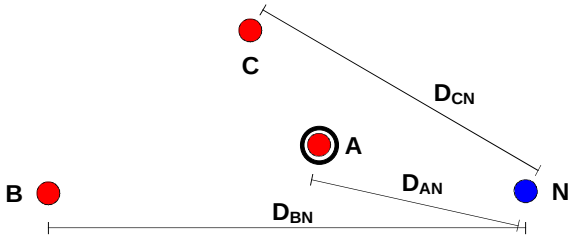


Figure 36: Distance to three nodes with known coordinates

With an anchor and three seeds, a node can receive four different position messages and measure the four distances. This is done by solving (for p and δ) the following system of four equations

$$\textbf{for } i=(A,B,C,D) \left(\; d_i = | L_i - p | + c \cdot \delta \; \right)$$

where each equation corresponds to one distance d_i measured by N to nodes A, B, C, and D. Therefore, the node can determine its location p and the synchronization offset δ and therefore synchronizes to anchor and seeds. The correct time then trickles from the nodes close to the anchor and the seeds to the outer reaches of the anchor's service area.

The algorithm to solve the four equations above is identical to the algorithm used for determining GPS locations.

D.1.5 Bibliography for annex D

For additional information on self-organizing location determination in ad-hoc networks see [i.1], [i.2], [i.3], and [i.4].

D.2 WLAN Positioning System

WLAN (or Wi-Fi) Access Points have become ubiquitous over the last few years such that at many locations in urban areas it is possible to receive signals from several stations. Since WLAN access points are uniquely identified by their Media Access Control address; these signals can potentially be used for location determination by establishing a database of their known positions and comparing the data with present position of a nomadic device equipped with suitable software.

One company working in this field claims to have collected information on more than 23 million access points in more than 2 800 towns, covering more than 70 % of the population of the USA, Canada, and Australia. They are planning to map the 50 largest towns in Europe and more than half the population of Great Britain, France, and Germany by the end of March 2008, with an accuracy of 20 metres to 40 metres. Apple intends to make this system available to users of the iPod, the iPhone and other devices.

D.2.1 System Operation

On notebook computers, PDAs and mobile phones already equipped with WLAN receivers the WLAN Positioning System (WPS) can be realized in software alone, though with GPS receivers having become so small and cheap many mobile phones now include them for location purposes. A symbiosis of GPS and WPS makes sense as WPS works best in urban areas where GPS systems may be problematic. Chipsets combining the two systems, combining the advantages of WPS and GPS are becoming available, enabling robust location determination in rural areas, in dense urban areas and inside buildings and tunnels. Figure 37 shows the comparative performance of WPS, GPS and XPS (the combined system) across variety of environments.

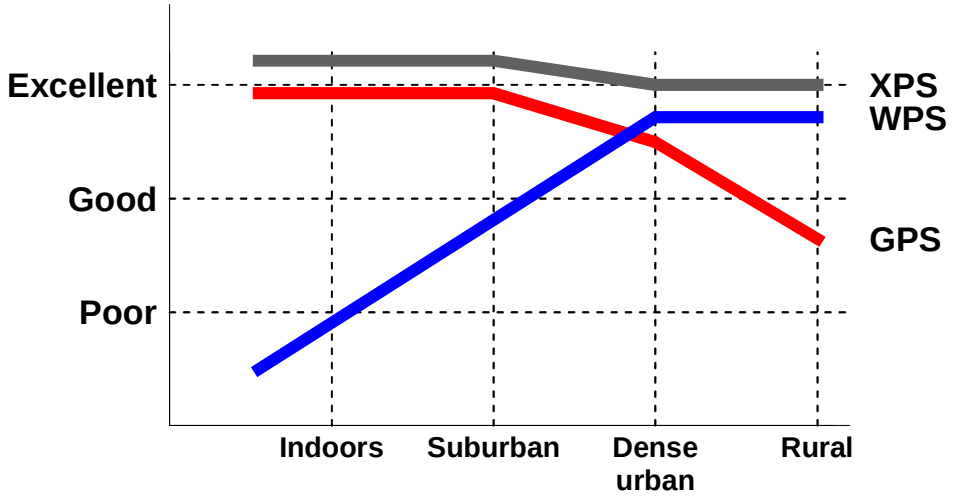


Figure 37: Comparative performance of location technologies GPS and WPS

This will overcome the deficiencies of existing location technologies such as GPS, cell tower triangulation and IP location which can lack accuracy, speed and reliability particularly in urban areas and indoors, thus limiting the wider adoption of Location based Services (LBS). WPS is software based system that can be implemented on almost all of the hundreds of millions of Wi-Fi enabled devices presently in service. This can dramatically reduce the cost and time associated with deploying location based applications or services in comparison with other positioning technologies providing a system that works indoors and outdoors, giving location information to an accuracy of 20 metres almost instantly, thus is more accurate than all other positioning technologies indoors and in metropolitan areas.

Every Wi-Fi base station repeatedly broadcasts a beacon signal announcing their existence to the surrounding area. These beacons typically travel 150-200 metres in all directions, many of them overlapping to create a natural reference system for determining location. The WPS location client identifies these signals and calculates its current location using special positioning algorithms and a knowledge of the geographic location of individual access points. Where there are more people, there are more Wi-Fi signals. So WPS performs best in areas of highest population density.

Wi-Fi access points are deployed for private and public use to provide high speed wireless coverage inside buildings, ensuring that WPS has excellent coverage and performance indoors distinguishing it from other positioning systems in urban and indoor environments. Consumers spend most of their time in these locations, thus WPS is the ideal system on which to base any consumer targeted Location Based Service. The number and proximity of access points means that within a coverage area, WPS quickly and accurately identifies nearby access points and almost instantly determines its position, usually in under one second.

The coverage area for WPS is critically dependent on maintenance of the reference database; the owners claim that they repeatedly re-calibrate the reference data in order to maintain the level of performance over time. In addition, the WPS location client is claimed to fix and expand the coverage area, and address the continuously changing nature of the network in real-time as users calculate their own location, though it is hard to see how this is accomplished without compromising user privacy.

D.2.2 Application

In operation, the mobile device user runs a location application which triggers the WPS client to execute a wireless scan of the area. WPS receives all the nearby WLAN beacons that include the unique MAC address; typically, WPS will receive more than five signals from any given scan. The results of this scan are compared either against the local cache of reference data or the central reference database via a network connection. The resulting list of reference points is fed into a suite of positioning algorithms and the user's current location is determined to within 20 metres, a process taking 50 milliseconds to 100 milliseconds. The location result can be fed directly to the end-user's application or combined with other positioning information, such as GPS, for a hybrid location result.

The two major components to the WPS system are the Mobile Location Client (MLC) and the WPS Location Server. The Location Server supports the MLC by ensuring that the client has up-to-date reference data and can also execute positioning algorithms should the user prefer a network-centric approach. It also includes the subscriber management and billing systems, and can run within a network operator's infrastructure; alternatively, a public Location Server is available for providers who want to minimize their cost and complexity.

D.2.3 Key Differences

The key differences which make WPS unique from other positioning technologies available, as highlighted by the system designers are:

D.2.3.1 Cost and Simplicity

WPS is a software only system that removes the need for new hardware. Operators can add LBS applications to existing hardware and unlike any other positioning system, WPS can be installed at production time or downloaded over-the-air.

D.2.3.2 Availability

Satellite based positioning systems such as GPS require direct line-of-sight to the sky in order to produce a reliable location fix. Since it relies on Wi-Fi access points, WPS works equally well indoors and outdoors and provides a consistent coverage area.

D.2.3.3 Reliability

Time-of-arrival systems suffer performance issues from multi-path signals in congested environments. Network-based systems often do not work outside of home areas - a problem as users become roam across networks undermining user confidence since they cannot be sure when to trust the system information. WPS produces accurate positioning data at all times, freeing users from worry.

D.2.3.4 Accuracy

Across large metropolitan areas WPS is claimed to be the most accurate positioning system available, with no other positioning system able to match its sub-20 metre accuracy indoors or in urban areas.

D.2.3.5 Speed

No other system produces an accurate location from a cold start as fast as WPS which can determine a user's exact location within seconds even without network assistance.

D.2.3.6 Hybrid Operation

WPS can be integrated with other location system to provide a single location source to applications and services while leveraging the strengths of each of the underlying system. Hybrid offerings combining WPS with GPS, IP Location, Cell Tower ID or WiMax are possible. The latter has a great deal of similarity with Wi-Fi, particularly in the area of base station identification, thus combining these two technologies provides the precision of WPS with the potential for wider coverage with WiMax, whilst in combination with GPS, WPS can provide near universal coverage,

D.2.4 Note of Caution!

The information in this anex (including figure 37) has largely been derived from the website of Skyhook Wireless Corp. at www.skyhookwireless.com and is uncorroborated. Whilst the system appears, in principle, to offer a viable solution to location problems, especially indoors and in urban areas, readers are cautioned that the system is critically dependent upon the establishment and maintenance of the database covering the concerned area. Whilst this is a dynamic operation relying to some extent on user feedback it, the database and the associated IPR appear to be owned and operated by a single company whose credentials have not been investigated during the preparation of the present document. There would also seem to be serious privacy concerns regarding both the ownership of the Wi-Fi base stations and end-user tracking.

In addition, a research team at the ETHZ in Zürich led by Prof. Srdjan Čapkun has demonstrated that it is possible to mislead terminals implementing WPS, for example an iPod or iPhone. Setting up a radio spoofing system with falsified MAC addresses made an iPod believe itself to be in New York City, 6 300 kilometres distant from its actual position in a laboratory in Zürich.

Annex E (informative): Bibliography

The following documents contain additional information for the present document.

3GPP2, 'IP Based Emergency Calls', IETF/3GPP Hosted SDO Emergency Services Coordination Workshop, Columbia University, New York, 5-6 October, 2006.

ATIS-XXXXXX (Draft), "Location Acquisition and Location Parameter Conveyance for Internet Access Location Acquisition and Location Parameter Conveyance for Internet Access Networks in Support of Emergency Services".

Australian Industry Specification ACIF G629:2006, "Interim VoIP Location Indicator for Emergency Services Signalling Specification".

IST-2001-34061 - E-MERGE, "Specifications of the European In Vehicle Emergency Call Vers1.5".

draft-ietf-ecrit-framework-05 (http://tools.ietf.org/id/draft-ietf-ecrit-framework-05.txt), "Framework for Emergency Calling using Internet Multimedia".

draft-ietf-ecrit-phonebcp-04 (http://tools.ietf.org/id/draft-ietf-ecrit-phonebcp-04.txt), "Best Current Practice for Communications Services in support of Emergency Calling".

draft-ietf-geopriv-policy-15 (http://tools.ietf.org/id/draft-ietf-geopriv-policy-15.txt), "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information".

draft-winterbottom-geopriv-lis2lis-req-01 (http://tools.ietf.org/html/draft-winterbottom-geopriv-lis2lis-req-01), "LIS to LIS Protocol Requirements".

Consumer & Governmental Affairs Bureau, "Wireless 911 Services", FCC - Consumer Facts, http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html.

History

Document history		
V1.1.1	July 2008	Publication