ETSI TR 102 764 V1.1.1 (2009-02)

Technical Report

eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth

Reference

DTR/eHEALTH-0002

Keywords

interoperability, safety, security

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 Report (TR) has been produced by Advisory Committee Operational Co-ordination Group (OCG) (eHEALTH).

NOTE: ETSI Project eHEALTH has been assisted by STF355 through the ETSI Funded Work Programme in completing this work.

Introduction

eHealth includes the application of information and communications technologies across the whole range of functions that affect the health sector in an international (e.g. cross-border) perspective, from the doctor to the hospital manager, including nurses, data processing specialists, social security administrators and - of course - the patients. eHealth systems include tools for health authorities and professionals as well as personalized health systems for patients (individuals) and citizens (community). Examples include health information networks, electronic health records, telemedicine services, personal wearable and portable communicable systems including those for medical implants, health portals, and many other ICT-based tools assisting disease prevention, diagnosis, treatment, health monitoring and lifestyle management (this description is based on text at the Europe's Information Society eHealth portal [i.1]).

The paper on "Home telehealth-Current state and future trends" presented in the "International Journal of Medical Informatics" [i.2] summarizes the important overall problems regarding healthcare services that most countries are facing such as:

- increased demand of healthcare due to an increased number of elderly and changed life styles leading to an increase in chronic diseases;
- demand for increased accessibility of care outside hospitals, moving health services into the patient's own homes;
- need for increased efficiency, individualization and equity of quality-oriented healthcare within limited financial resources;
- difficulties of recruiting and retaining personnel in the healthcare services in general and in home and elderly care in particular.

It is expected that eHealth will provide partial but significant solutions to the above issues, as it has been recognized as a potential tool to provide access to timely, efficient, and high quality healthcare. Driving forces exist for implementing new solutions such as the migration to self-managed care and allowing increased patient mobility at an international level (e.g. cross border). However, there are numbers of hindrances and restrictions when it comes to practical and sustainable use of eHealth, which include interoperability, security and privacy.

A key ambition of the EU policy is the provision of better care services at the same or lower cost. eHealth is regarded by Europe's Information Society eHealth portal [i.1] as "today's tool for substantial productivity gains, while providing tomorrow's instrument for restructured, citizen-centred health care systems and, at the same time, respecting the diversity of Europe's multi-cultural, multi-lingual health care traditions. There are many examples of successful eHealth developments including health information networks, electronic health records, telemedicine services, wearable and portable monitoring systems, and health portals".

1 Scope

The present document describes the eHealth user service models for the identification of interoperable solutions for healthcare data collection, transmission, storage and interchange. The supporting analysis for this work is found in SR 002 564 [i.3]. The model identifies the requirements for ubiquity, security, privacy and reliability across the eHealth system and the supporting ICT technologies.

The present document may be used in support of the ETSI contribution to mandate M/403 [i.4].

The present document identifies where additional standardization is required in ICT generally and in ETSI in particular to support eHealth.

The present document is intended for the following audience:

- standards developers;
- developers and equipment manufacturers and providers in the eHealth related area;
- developers and providers of eHealth related services.

NOTE: The present document is published as a TR but in the context of being a guide to future standardization may on occasion provide indications of where future standards are required by using the mandate "shall". Such mandates are to be considered only in the guidance for future standardization and not as normative in the scope of the present document.

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.

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.

Not applicable.

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] "Europe's Information Society eHealth portal".

NOTE: Available at: http://europa.eu.int/information_society/activities/health.

[i.2] "Home telehealth-Current state and future trends", Uppsala University, International Journal of Medical Informatics (2006) 75, p. 565-576, Sabine Koch.

[i.3] ETSI SR 002 564: "Applicability of existing ETSI and ETSI/3GPP deliverables to eHealth".

[i.4] Mandate M/403 of the European Commission Enterprise And Industry Directorate-General: "Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies, applied to the domain of eHealth".

[i.5] Freeband homepage.

NOTE: Available at: http://pnp2008.freeband.nl.

[i.6] GRIFS: "Global RFID Interoperability Forum for Standards".

NOTE: Available at: http:// www.grifs-project.eu/.

[i.7] CASAGRAS: "Coordination and Support Action (CSA) for Global RFID-related Activities and Standardisation".

NOTE: Available at: http://www.rfidglobal.eu/.

[i.8] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.9] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

[i.10] EMC list.

NOTE: Available at: http://ec.europa.eu/enterprise/newapproach/standardization/harmstds/reflist/emc.html.

[i.11] "Mobile e-Health monitoring: an agent-based approach", V. Chan, P. Ray, N. Parameswaran, IET Communications, Volume 2, Issue 2, pages 223 - 230, February 2008.

[i.12] "Body Area Network BAN - a Key Infrastructure Element for Patient-Centric Health Services", T. Norgall, Joint ISO TC215/WG7/IEEE 1073 Meeting, Berlin, May 2005.

[i.13] "Body area network (BAN), a key infrastructure element for patient-centered medical applications", R. Shmidt et al. In Biomed Tech (Berl), volume 47, Part I, pages 365-368, 2002.

[i.14] "Human++: from technology to emerging health monitoring concepts", J. Penders et al., 5th International Workshop on Wearable and Implantable Body Sensor Networks, Hong Kong, June 2008.

[i.15] ZigBee homepage.

NOTE: Available at: www.zigbee.org

[i.16] Bluetooth homepage.

NOTE: Available at: www.bluetooth.com

[i.17] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[i.18] IETF RFC 791: "Internet Protocol".

NOTE: Commonly referred to as IPv4.

[i.19] ETSI EG 202 325: "Human Factors (HF); User Profile Management".

[i.20] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[i.21] ETSI TR 102 216: "Smart Cards; Vocabulary for Smart Card Platform specifications".

[i.22] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.23] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.24] IEEE 802.21: "IEEE Standard for Local and metropolitan area networks - Part 21: Media Independent Handover Services".

[i.25] Directive 2006/95/EC: "The Low Voltage Directive (LVD)".

[i.26] Directive 2001/95/EC: "General Product Safety Directive (GPSD)".

[i.27] Directive 2004/108/EC: "The Electromagnetic Compatibility (EMC) Directive".

[i.28] ETSI TR 102 653: "Project MESA; Technical Specification Group - System; System and Network Architecture".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in SR 002 564 [i.3], the eHealth portal [i.1] and the following apply:

Body Area Network (BAN): collection of eHealth devices which are in the body (implants) or in direct contact with it (wearable)

cluster: network of personal devices and nodes located within a limited geographical area (such as a house or a car) which are connected to each other by one or more network technologies and characterized by a common trust relationship between each other.

device: any communicating entity

node: device that implements IPv6 [i.17] and/or IPv4 [i.18]

NOTE: Nodes and devices in a cluster can become members of a PAN when a person with the PAN enters an area where the cluster nodes are located.

Personal Area Network (PAN): dynamic collection of personal nodes and devices around a person

NOTE: The privacy in a PAN is guaranteed by mandating a mutual trust relationship between every node and device in a PAN. A PAN is often referred to as a personal bubble around a person.

personal device: device related to a given user or person with a pre-established trust attribute

NOTE: These devices are typically owned by the user. However, any device exhibiting the trust attribute can be considered as a personal device. The same remarks as those for the personal nodes definition hold for devices.

Personal Network (PN): PAN and a dynamic collection of remote personal nodes, devices and ser in clusters that are connected to each other

personal node: node related to a given user or person with a pre-established trust attribute

PN Federation (PN-F): temporal, ad hoc, opportunity- or purpose-driven secure network of independent PNs

ubiquity: telecommunications or network service is considered as ubiquitous when it is, or seems to be, omnipresent within the scope of its deployment

3.2 Abbreviations

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

ATM	Asynchronous Transfer Mode
BAN	Body Area Network
BRAN	Broadband Radio Access Network
CBR	Constant Bit Rate
CEN	Comité Européen de Normalisation (European Committee for Standardization)
DECT	Digital Enhanced Cordless Telecommunications
ECG	Electro Cardio Graph
ECN	Electronic Communications Network
EMC	Electro Magnetic Compatibility
GoS	Grade of Service
GPRS	General Packet Radio Service
GPSD	General Product Safety Directive
GSM	Global System for Mobile communications
HF	Human Factors
ICC	Integrated Circuit Card
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMS	IP Multimedia System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
LTE	Long Term Evolution
LVD	Low Voltage Directive
NGN	Next Generation Network
OSA	Open Systems Alliance
PAMR	Public Access Mobile Radio
PAN	Personal Area Network
PDA	Personal Digital Assistant
PMR	Private Mobile Radio
PN	Personal Network
PN-F	PN Federation
PSTN	Public Switched Telephone Network
PWLAN	Public Wireless Local Area Network
QoS	Quality of Service
RBAC	Role Based Access Control
RF	Radio Frequency
RFID	Radio-Frequency IDentification
SAP	Service Access Point
SCP	Smart Card Platform
SDO	Standards Development Organization
SMS	Short Message Service
SSID	Service Set IDentifier
TETRA	TErrestrial Trunked RAdio
UICC	Universal Integrated Circuit Cards
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
UWB	Ultra Wide Band

UWB-FM	Ultra Wide Band Frequency Modulation
VBR	Variable Bit Rate
WCDMA	Wideband Code Division Multiple Access

4 Architecture

4.1 Overview

An architecture has two purposes in a technical document:

- to structure requirements;
- to illustrate requirements.

The present document is largely technical and focussed on the technical features of an architecture. However in arriving at such an architecture it is necessary to also consider the users and how they interact with the system and the starting point is shown in figure 4.1.

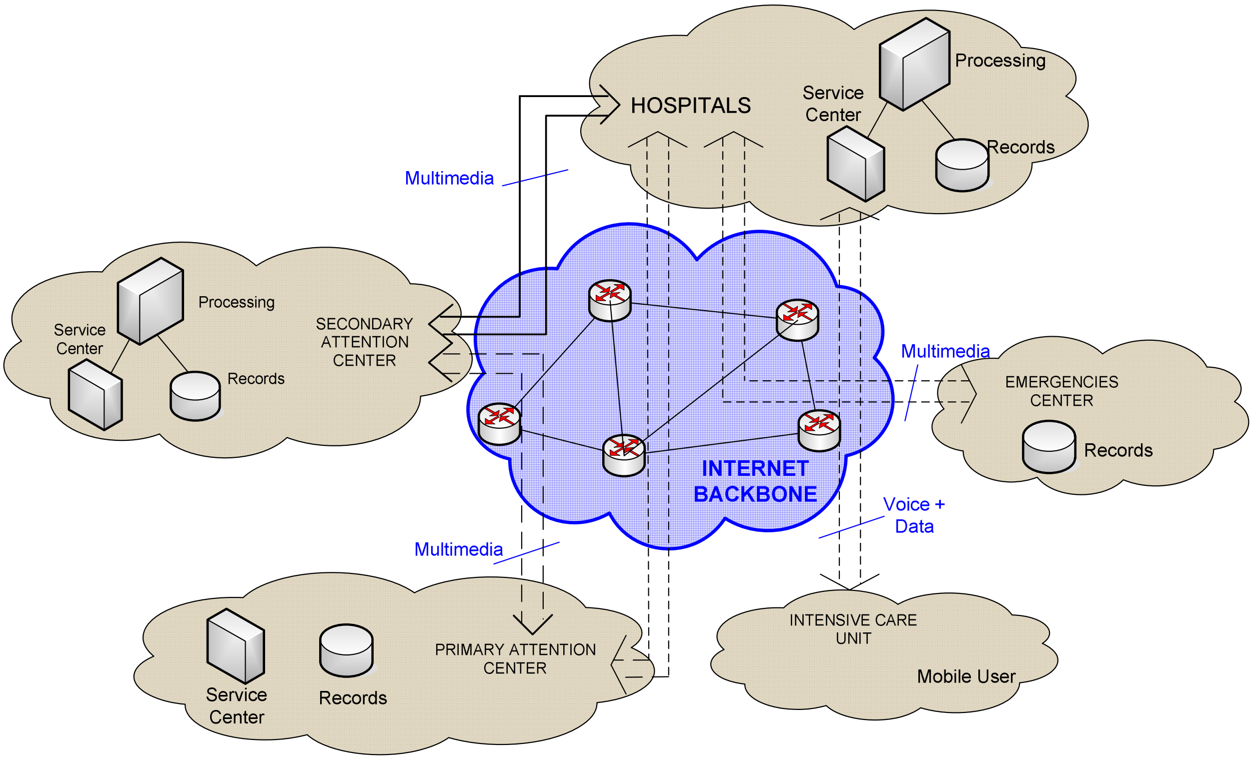


Figure 4.1: The eHealth system illustrating links and users

There are a number of ways to bring the illustration in figure 4.1 to the technical standards developer and the approach followed in the present document has been to propose first a technical eHealth architecture for the purposes of analysis consisting of 3 layers as shown in figure 4.2 and to generate a set of use cases in both text and in UML to capture the relationships of different users to the services and data of the eHealth platform.

4.2 eHealth technical architecture

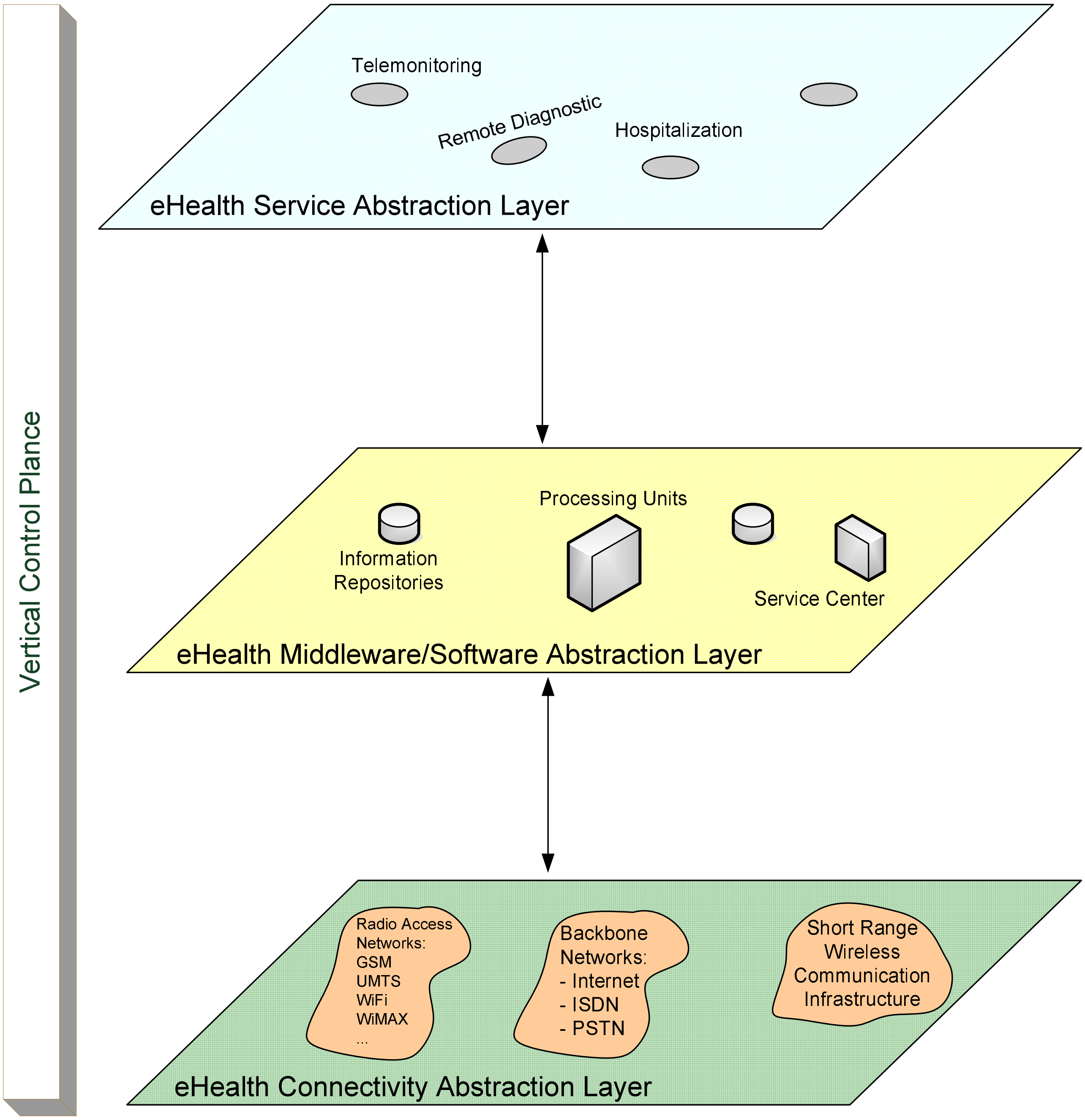


Figure 4.2: Top level eHealth architecture

4.2.1 eHealth service abstraction layer

The eHealth service abstraction layer contains the set of eHealth user services and combines the data and functionality contained in the eHealth platform layer with communications capabilities in the ICT Platform layer.

4.2.2 eHealth middleware abstraction layer

The eHealth middleware abstraction contains the functionality required for eHealth to operate independently of the ICT platform used to transfer data.

The example eHealth user layer services are captured in the present document as use cases in clause 8.

NOTE 1: There is significant ongoing work in the data modelling area in ETSI and in CEN that should be integrated to the eHealth platform in due course.

NOTE 2: The ETSI guide on "User Profile Management" (EG 202 325 [i.19]) provides guidelines for managing user profiles, and serves as background for the ongoing work for User profiles in eHealth. The plans for work on profile management from ETSI expands from EG 202 325 [i.19] to an ETSI Standard (ES) defining objects (including settings, values and operations) related to personalization and user profile management, and a Technical Specification (TS) on architectural issues related to networks, terminals and SmartCards. In parallel to these documents a further ETSI ES is being developed for the specifications of objects, preferences and contexts that are specific for personalization within the eHealth domain.

4.2.3 eHealth connectivity abstraction layer

The connectivity abstraction layer contains the technical measures to connect eHealth components across a network resulting in a managed set of ICT resources defined by the service. The ICT platform requirements or capabilities are characterized as a combination of each of the following classes (see clause 6 for a more detailed analysis and mapping of these classes).

The introduction of real telecom services requires that they are able to provide a mapping to the abstract services. The interface between the layers in the architecture is to be defined in terms of these abstractions.

NOTE: Each layer will offer more detail, i.e. less abstraction as the actual ICT technology is approached from above, and correspondingly less detail as the user service is approached from below.

- Connection capability:
  - Circuit mode, or Continuous Bit Rate (CBR).
  - Packet mode, or Variable Bit Rate (VBR).
- Connection symmetry:
  - Symmetric (i.e. data rate, QoS, GoS, to/from user is identical).
  - Asymmetric (i.e. data rate, QoS, GoS, to/from user is not identical).
- Connection (address) topology:
  - Unicast (i.e. communication is directed to a single endpoint).
  - Multicast (i.e. communication is directed to a distinct group of endpoints).
  - Broadcast (i.e. communication is directed to all endpoints in the network).
- Content type:
  - Data (i.e. in the form of files, e.g. a word document, images information, deferred transmission of sampled information such as ECG and video etc.).
  - Video (e.g. in the form of live casting, and more generally, all real time data streams obtained from real time multidimensional sampled signals).
  - Audio (including speech, ECG, and more generally, all real time data obtained from real time single dimension sampled signals).
  - Image (i.e. a specialist form of data file generally of large size, e.g. high-resolution digital photograph), deferred ECG, deferred video, etc.

EXAMPLE 1: An (short) Message service can be mapped on an SMS call carried on a 2G (GSM) network. This is characterized by message (data), using a connectionless mode, packet mode, unicast, data service.

EXAMPLE 2: A video call from a paramedic to a specialist diagnostic group can be mapped on a TETRA TEDS connection. This is characterized as video (real-time, streaming), packet mode, multicast.

- Higher layer services:
  - Message transfer service, a service where each unit of information is limited in size and stand alone has semantic significance.

4.3 Interoperability and eHealth

Interoperability is the primary goal of the eHealth system in order to ensure that applications can connect and communicate with each other exchanging data in a manner that gives very high levels of assurance of performance, security, understanding and action.

The architecture described in clause 4.2 is a key step in achieving interoperability by enforcing common interfaces between well defined planes.

There is no incentive to provide direct interoperability within the ICT Platform layer as the ICT technologies are designed for a number of different physical environments, therefore within eHealth the aim is to achieve interoperability in the eHealth platform itself and to ensure that this platform can drive the available ICT Platforms.

NOTE: Interworking and interoperability are often confused and the result of eHealth standardization will be interworking between heterogeneous systems by the provision of interface and data definitions that allow the different systems and technologies to interwork.

4.3.1 Device and system considerations

The eHealth system relies upon transfer of data and coexistence of devices. In order to achieve interoperability the data definitions have to be understood by all eHealth enabled devices.

Where radio devices are used the eHealth system requires by default that such devices are able to operate without interference and without restriction on the geographic location. For example an implanted sensor has to be able to operate in all areas and environments that its wearer may reasonably be present and thus there has to be harmonized ability to carry and operate equipment in the areas in which the user may carry the equipment (e.g. a tourist travelling from Lapland to Gibraltar would reasonably expect a sensor to operate at both locations and to not provide any negative impact on his health at either location).

4.4 Security in eHealth

The term security is often misunderstood and more often misapplied in telecommunications. A device is made secure by offering the ability to be immune to some forms of attack and when it presents an acceptable and tolerable level of risk to the user and the system that surrounds it. In telecommunications security is often presented as the ability to conserve or prove a number of attributes of a user and their communication as follows:

- Authenticity:
  - Ensuring that Alice is really Alice and not Bob masquerading as Alice.
- Authority:
  - Ensuring that Alice is allowed to perform the operation requested.
- Integrity:
  - Ensuring that data received is the same as that transmitted.
- Confidentiality:
  - Ensuring that communication between Alice and Bob if seen by Eve does not reveal the actual content of the communication.

In addition it is reasonable in most cases to add other dimensions such as reliability and repeatability to the security term but such things are often outside the scope of technical standardization although there are a number of guides that address such issues, e.g. ISO/IEC 27001 [i.9].

4.4.1 Privacy

Privacy, and the protection of privacy, is not a simple security issue and demands an understanding of the relationship of data to users and the needs of the eHealth professionals. All eHealth patient users have a right to privacy of their data but it is essential that authorized health professional have access to the health records of their patients. This is mostly achieved through the "Authority" security function which requires due care in identity and authentication.

It should be noted that confidentiality is not an essential requirement for privacy but may be enforced if private data is open to the public.

Whilst it is not the role of the present document to define privacy it is important to recognize that many of the threats to privacy can only be partially provided by technology, whereas the bulk of privacy controls are organizational and societal and rely upon a degree of trust between the data provider (e.g. the patient) and the data receiver (e.g. the health professional).

4.4.2 Electronic signature in eHealth

Electronic signature development in Europe has a number of impacts in the eHealth environment and the impact of the eSignature directive on eHealth needs to be explored in the context of proof of ownership and validation of eHealth records.

4.4.3 Non-repudiation in eHealth

One of the key security features in eHealth to protect the clinical audit is the suite of services that make up non-repudiation (the inability to deny sending or receiving a command). For example it is often important to be able to prove the both the delivery and receipt of a prescription and a non-repudiation service will be core in providing that.

4.5 Further work to be undertaken in SDOs (architecture)

In further development of the eHealth architecture the following activities need to be carried out:

- Development of interface definitions between the abstract layers of the eHealth architecture.
- Development of a robust data dictionary to ensure intelligent and comprehensive transfer and operation of data.
- Development of RF co-existence standards to ensure that eHealth devices are able to operate without interference and without restriction on the geographic location.

NOTE: This may require harmonization of frequency allocation and power profiles for devices.

5 Specific eHealth support network architectures

5.1 Body Area Network architectures (BAN)

BAN technology supports communications among implanted/wearable devices as well as communications with a proxy device (typically the gateway) that connects the BAN with external infrastructures (PAN, Internet, etc.).

5.2 Personal Area Networks (PAN)

PAN technology allows supporting transparent, secure and trusty communications among eHealth devices around the person. This set of devices and nodes creates an eHealth environment with both intra and inter-PAN communication capabilities. Remote access to the PAN nodes and devices allows supporting services such as tele-monitoring, tele-diagnosis, remote prescription, etc.

5.3 Personal Networks (PN) and PN-Federation

5.3.1 Personal Networks (PN)

While a PAN connects a person's devices/nodes around him, a PN extends that PAN with other remote eHealth devices and services farther away. Although a PN creates virtual vicinity among the devices, it is more than just overlay connectivity.

5.3.2 Federation of Personal Networks (PN)

Federation allows sharing personal resources, services, and content with others to achieve a common objective that would not be possible by a single PN. An example scenario for Federations of Personal Networks can be the healthcare, where family members and medical professionals federate to allow access to medical sensor information (of specific vital signs) and video images of elderly or sick people living unattended to detect potentially dangerous situations.

Figure 5.1 indicates, using UML as a tool, how the entities identified relate to each other. PN-F consists of two or more PNs which cooperate to achieve a common goal. Just as an example, tuned to the eHealth sector, the doctor's PN can cooperate with the patient's one aiming at downloading the historical report of hearth data stored in a particular PAN device belonging to the patient.

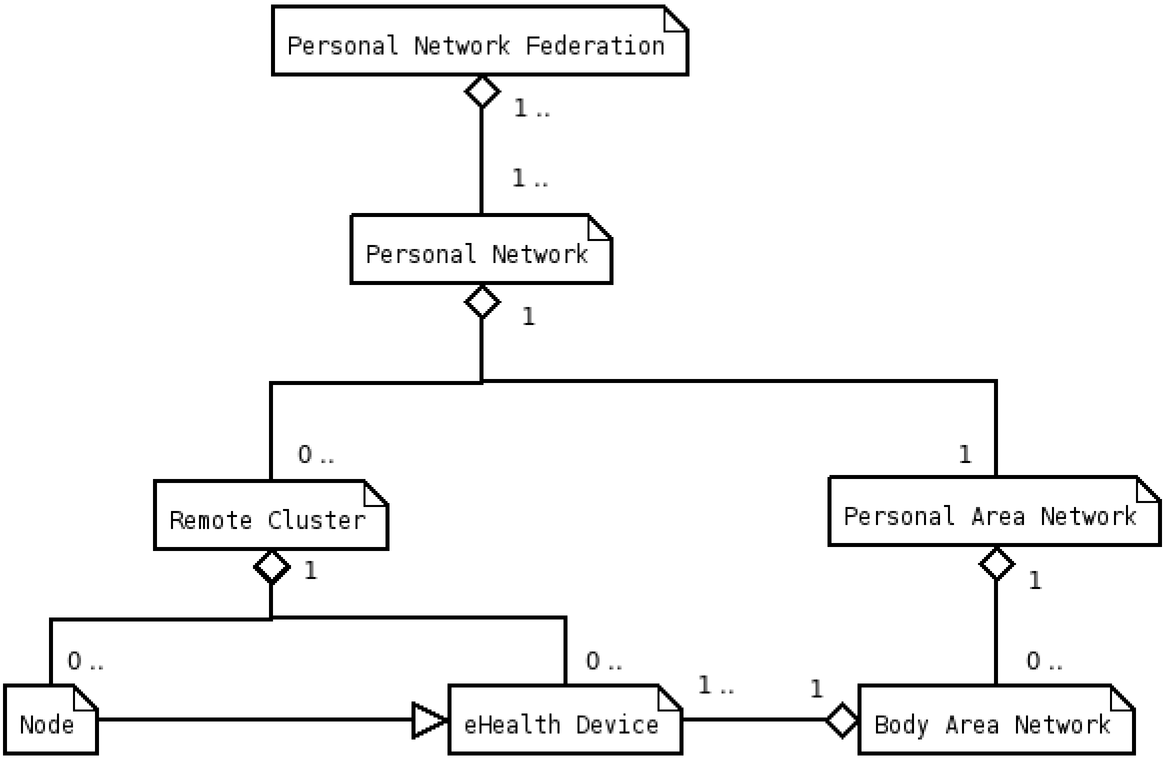


Figure 5.1: UML diagram corresponding to the PN-F and PN

5.4 Infrastructure related network architectures for PN and PN-F

In order to build a PN-F or a PN, heterogeneous communications infrastructures (Internet, TETRA, ISDN, mesh networks, etc.) may have to be used.

5.4.1 Home network infrastructure and architecture

Home network can be assimilated to a cluster.

5.4.2 Vehicle network infrastructure and architecture

Vehicle network is a cluster with mobility.

5.5 Further work to be undertaken in SDOs (specific eHealth support network architectures)

In further development of specific eHealth support network architectures the following activities need to be carried out:

- Integration of PAN, BAN, PN and PN-F to eHealth.

6 Abstract communication services from telecommunications services

6.1 Parameterization of telecommunications services

6.1.1 Ubiquity

A telecommunications or network service is considered as ubiquitous when it is, or seems to be, omnipresent within the scope of its deployment.

6.1.2 Mobility

Mobility within a telecommunications network is used to refer to the ability of a device to change its physical point of attachment to the network without losing its logical connectivity. The obvious example is cellular radio where moving from one cell, the physical point of attachment, to another causes no interruption to the user service (the logical connection).

6.1.3 Security

The security capabilities are identified as follows:

- Station authentication.
- Infrastructure authentication.
- Cryptographic integrity generation and validation.
- Confidentiality provision (link encryption, end to end encryption).
- Service authorization.

In addition key management mechanisms are considered.

6.1.4 Connection capability

In telecommunications there are two distinct modes of operation:

- Circuit mode.
- Packet mode.

A circuit mode call is often considered as traditional telephony where a simple definition may be that for the period of the communication there is a continuous electrical connection between the end points where the order of entry of data is preserved on exit. In practical terms there is not in fact an actual continuous electrical connection.

Packet mode connections treat each packet as discrete and therefore it is possible that each packet takes a different route and thus may arrive out of order. The dominant mode in modern telecommunications is packet mode.

NOTE: The operational mode is distinct from the technology used to implement it, therefore traditional circuit mode services (e.g. voice calls) can be delivered using packet transmission capabilities (e.g. ATM, IP).

6.1.5 Connection (address) topology

The topology of a connection is used to describe much of the physical connection of calls and covers three distinct cases. In each case a communications session may require a topology for each direction of connection:

- Unicast (point to point).
- Multicast (point to multipoint).
- Broadcast (point to all points).

6.1.6 Content type

Whilst in a digital age all content can essentially be represented as a series of binary encoded information there are other characteristics that may be used to assist the ICT platform in carrying the content:

- Data.
- Video.
- Audio (including speech).
- Image, deferred audio, deferred video, etc.

6.1.7 Quality of Service (QoS) and Grade of Service (GoS)

The QoS and GoS offered by a communications service define a number of characteristics where very crudely GoS refers to the ability to access and establish services and includes the time required to establish sessions, system reliability and recovery and system resilience (i.e. how it degrades), and QoS refers to the maintenance of the session once established and covers aspects such as throughput, error recovery/detection.

6.1.7.1 QoS configurability

From an eHealth perspective several parameters of Quality of Service (QoS) may be used to differentiate the suitability of application of technologies to specific eHealth services. Such parameters include latency, jitter, end-to-end delay. In some ICT technologies there are options to offer more than one managed combination of bearer and teleservice, whilst some ICT technologies offer only a single, best effort, QoS capability.

6.2 Existing Standards and standardization efforts application in eHealth ICT platform

NOTE: The material in this clause augments the information provided in SR 002 564 [i.3] although the information in SR 002 564 [i.3] remains valid.

6.2.1 Radio technologies

6.2.1.1 RFID

An RFID tag is an object that can be attached to or incorporated into a product (devices, sensors, etc.), animal, or person for the purpose of identification using radio waves. In essence an RFID tag is a passive device that is powered on receipt of a "significant" RF signal and as this received power is discharged through the device the data on the tag is transmitted (essentially reflected back to the reader). This rather crude description of how the tag works illustrates some of the key characteristics of RFID tags for eHealth and the ICT platform. An RFID system has to split as two components:

- RFID tags.
- RFID readers.

The characteristics of each are different with respect to the ICT platform of eHealth. In particular whilst it may be possible to have RFID readers always present (subject to reliability constraints) as a member of the ICT platform the RFID tags are mostly not visible to the ICT platform.

- Mobility: No.
- Intrinsically secure: No.

NOTE 1: An RFID tag has limited transmission range and is often used as an element in an authentication chain where it forms part of the authentication factor "has", i.e. the person being authenticated is expected to carry an RFID tag acting as (part of) a key. The limited transmission range acts to reinforce authentication in areas such as barrier entry (e.g. transport barriers on underground rail networks) where holders of RFID tags may be discretely identified.

- Standardization bodies: ISO, CEN, ETSI, GS1.

NOTE 2: GS1 is not a formal SDO but acts as an industry registration body for RFID applications.

- Standards activity: EU FP7 projects GRIFS [i.6], CASAGRAS [i.7].
- Connection capability: Packet.
- Connection topology: Unicast (although broadcast prior to activation).
- Content: data.

Whilst RFID devices can be considered ubiquitous there are few standards for the connection of readers and a mass of often incompatible standards for the data content.

6.2.1.2 TErrestrial Trunked RAdio (TETRA)

TETRA is the digital Private Mobile Radio (PMR) and Public Access Mobile Radio (PAMR) technology for police, ambulance and fire services, security services, utilities, military, fleet management, transport services and a host of other communities.

- Mobility: Yes.
- Intrinsically secure: Yes (for Class 3 installations).

NOTE: TETRA offers a number of standardized services for authentication, encryption and key management to counter attacks on the air interface link. As there is no store and forward possible on this link no integrity protection measures are provided.

- Standardization bodies: ETSI, TETRA Association.
- Standards activity: Ongoing maintenance and extension at ETSI.
- Connection capability: Packet, Circuit.

- Connection topology: Unicast, Multicast, Broadcast.
- Content: data, voice, video, image.

TETRA tends to be used in specialist fields and in such fields there is no guarantee of interconnection to other ICT platforms. In public safety environments as an example the networks often are closed with restricted access enforced by national security agencies.

6.2.1.3 WiFi (IEEE 802.11a/b/g/n)

WiFi is the common name applied to the suite of wireless Ethernet standards from the IEEE:

- Mobility: No, although micro mobility may be supported in some implementations (i.e. if the same SSID is used without authentication the station may seamlessly attach to different physical stations).
- Intrinsically secure: No.

NOTE: There are a number of security mechanisms available in WiFi of varying cryptographic strength and with both user selectable key management and selectable provision of encryption. Authentication in WiFi is a function of key management and integrity protection is not provided.

- Standardization bodies: IEEE, ISO, 3GPP, ETSI.
- Standards activity: Intel, IETF and in IEEE with some interest from the GSM OA.
- Connection capability: Packet.
- Connection topology: Unicast (at radio layer).
- Content: data, video, audio, image.

WiFi technologies have become widely available through the growth in the PC market and of ADSL fixed line access, with WiFi acting as a private local access point (equivalent to DECT in the home market).

The other area of growth is the emergence of the "hotspot" business (PWLAN).

6.2.1.4 WiMAX

WiMAX is defined as Worldwide Interoperability for Microwave Access by the WiMAX Forum, formed in June 2001. HIPERMAN stands for High Performance Radio Metropolitan Area Network and is an alternative to the mainly European ETSI Broadband Radio Access Networks (BRAN) standard for Wireless Metropolitan networks.

- Mobility: yes.

NOTE 1: WiMAX Mobile offers this capability.

- Intrinsically secure: No.

NOTE 2: WiMAX offers security functions but they are not deployed by mandate.

- Standardization bodies: IEEE, ETSI (for testing and pre-certification).
- Standards activity: active in WiMAX forum and in ETSI.
- Connection capability: Packet.
- Connection topology: Unicast (at radio layer).
- Content: data, video, audio, image.

The WiMAX forum aims to develop WiMAX as the ubiquitous successor to WiFi (IEEE 802.11a/b/g/n) offering increased security and range. However WiMAX is in the licensed spectrum zone and requires significant development in frequency harmonization to achieve its goal of ubiquity.

6.2.1.5 Ultra-WideBand (UWB)

UWB is a technology for transmitting information spread over a large bandwidth, while allowing sharing the spectrum with other users. This is intended to provide an efficient use of scarce radio bandwidth.

Implementations can be optimized for short range and high data rate, short range and low power (e.g. for Personal-Area Network (PAN) wireless connectivity, for short range, low data rate and very low power (e.g. UWB-FM for sensor networks and sensors in Body Area Networks (BANs)), etc. Other applications areas include radar and imaging systems.

- Mobility: No.
- Intrinsically secure: No.
- Standardization bodies: ETSI.
- Standards activity: ETSI.
- Connection capability: Packet.
- Connection topology: Unicast.
- Content: data, video, audio, image.

UWB is an ongoing development activity being addressed in ETSI and other pre-standards groups.

6.2.1.6 The Global System for Mobile Communications, GSM (original acronym: Groupe Spécial Mobile)

GSM is the most popular standard for mobile phones in the world. GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1 800 MHz bands. Some countries (including the United States and Canada) use the 850 MHz and 1 900 MHz bands because the 900 MHz and 1 800 MHz frequency bands have been allocated to other technologies or services.

- Mobility: Yes.
- Intrinsically secure: Yes (for privacy protection of content).
- Standardization bodies: ETSI and 3GPP.
- Standards activity: active in GSM OA.
- Connection capability: Packet, Circuit.
- Connection topology: Unicast (although broadcast prior to activation).
- Content: data, video, **audio**, image (narrowband best suited and optimized for carriage of voice).

6.2.1.7 Universal Mobile Telecommunications System (UMTS)

UMTS is a third-generation (3G) mobile phone network technology. It uses WCDMA (Wideband Code Division Multiple Access) as the underlying technology, is standardized by 3GPP, and relates to the ITU requirements for 3G cellular radio systems. 3GPP has begun work on Long Term Evolution (LTE) which includes enhanced performance with a new radio access network and evolved system architecture.

- Mobility: Yes.
- Intrinsically secure: Yes for privacy enhancement.
- Standardization bodies: 3GPP, 3GPP2, IEEE, ITU-T, ISO.
- Standards activity: active in GSM/3G Operators Association.

- Connection capability: Packet.
- Connection topology: Unicast, multicast, broadcast.
- Content: data, video, audio, image.

The ongoing deployment networks and sale of 3G terminals will mean that in a short period of time that 3G radio technologies will become ubiquitous.

6.2.1.8 Satellite

Satellite communication and satellite-based Internet services are able to provide service with a wide geographic coverage (the satellite "footprint") at low to medium data rates throughput. Satellites are often used to provide services in locations where terrestrial network access is not available or to locations which frequently change geographic position (e.g. ships). Communication services via satellite are generally available worldwide although individual satellites have restricted geographic coverage (as a function of their beam pattern) with geographic coverage extended by ground based networks (i.e. there is no scheme for satellite to satellite routing of calls or sessions).

6.2.1.9 The PN and PN-F

A Personal Network (PN) connects a person's Personal Nodes together using direct local wired or wireless connections between Personal Nodes as well as infrastructure-based connections and even multi-hop ad-hoc networks to connect geographically dispersed Personal Nodes. Furthermore, network protocols will need to enable communication with other person's Personal Networks as well as independent Foreign Nodes. The most appropriate choice as network protocols is based on the Internet Protocol (IP), both IPv4 and IPv6, in order to work over heterogeneous networks and to facilitate communication with the fixed Internet.

In order to make this a reality, solutions for a large set of problems will need to be specified. There is a need for a good addressing and routing scheme to route packets between Personal Nodes as well as to and from Foreign Nodes. A naming scheme is needed to help the user overcome the difficulty of using IP addresses. Self-configuration and maintenance will need to be supported at the network layer so that non-technical users can operate their Personal Networks in an efficient way. Adaptability to changing conditions is required from all mechanisms, since many of a person's devices will reside in a dynamic environment. To meet these requirements, some concepts have been defined and solutions have been suggested to each of these challenges.

Nodes belonging to the same owner form Clusters of Personal Nodes and they can communicate with any other Personal Node in that Cluster without using Foreign Nodes. In this way, the communication, routing and other self-organizing mechanisms can be protected on a local scale. In this architecture, the home network of a person can be one Cluster, the car network another, the PAN around the person a third and so on.

For the global scale, tunnels are established between a person's Clusters to both accommodate and protect communication between the Clusters. The tunnels can efficiently be maintained by infrastructure-based functionality in a dynamic way. Effective addressing and routing schemes are suggested to route traffic over these tunnels. This is one way of solving the mobility management issue of PN-internal traffic. Other solutions and mobility solutions for communication with Foreign Nodes are also considered.

Finally, the PN-F paradigm is defined as the aggregation of several PNs which cooperate in order to share any kind of service or resource previous agreement of the "owners" around which the corresponding PNs are established.

6.2.2 Fixed network technologies

6.2.2.1 Internet Protocol version 6 (IPv6) / version 4 (Ipv4)

IPv6 [i.17] and IPv4 [i.18] are network layer Internet Protocol (IP) standards used by electronic devices to exchange data in the form of datagrams across packet-switched networks. IPv6 follows IPv4 as the second version of the Internet Protocol to be formally adopted for general use.

- Intrinsically secure: No.

NOTE: There are a wide range of security functions standardized by the IETF for provision of authentication, integrity and confidentiality services. The primary protocol suite, IPsec, has to be supported by all IPv6 deployments but not all deployments will provide IPsec functionality (i.e. mandatory to support, optional to deploy).

- Standardization bodies: IETF, ETSI (for testing and requirements catalogue).
- Standards activity: active in IETF.
- Connection capability: Packet.
- Connection topology: Unicast, multicast, broadcast.
- Content: data, video, audio, image.

Whilst IPv4 has been developed and become ubiquitous IPv6 has had long delays in deployment although it has significant support from 3GPP and the NGN. Some features that are mandatory in IPv6 to support have been deployed in IPv4 thus prolonging the life of IPv4. Such features include IP Security (IPsec), IP mobility and flat address space.

6.2.2.2 NGN and IMS

The core of modern networking technologies is exemplified by the separation of Services and Networks in line with the Framework Directive and the ECN&S architecture it implies. The ECN&S architecture shown in figure 6.1 is closely aligned to the architecture given in clause 4 of the present document.

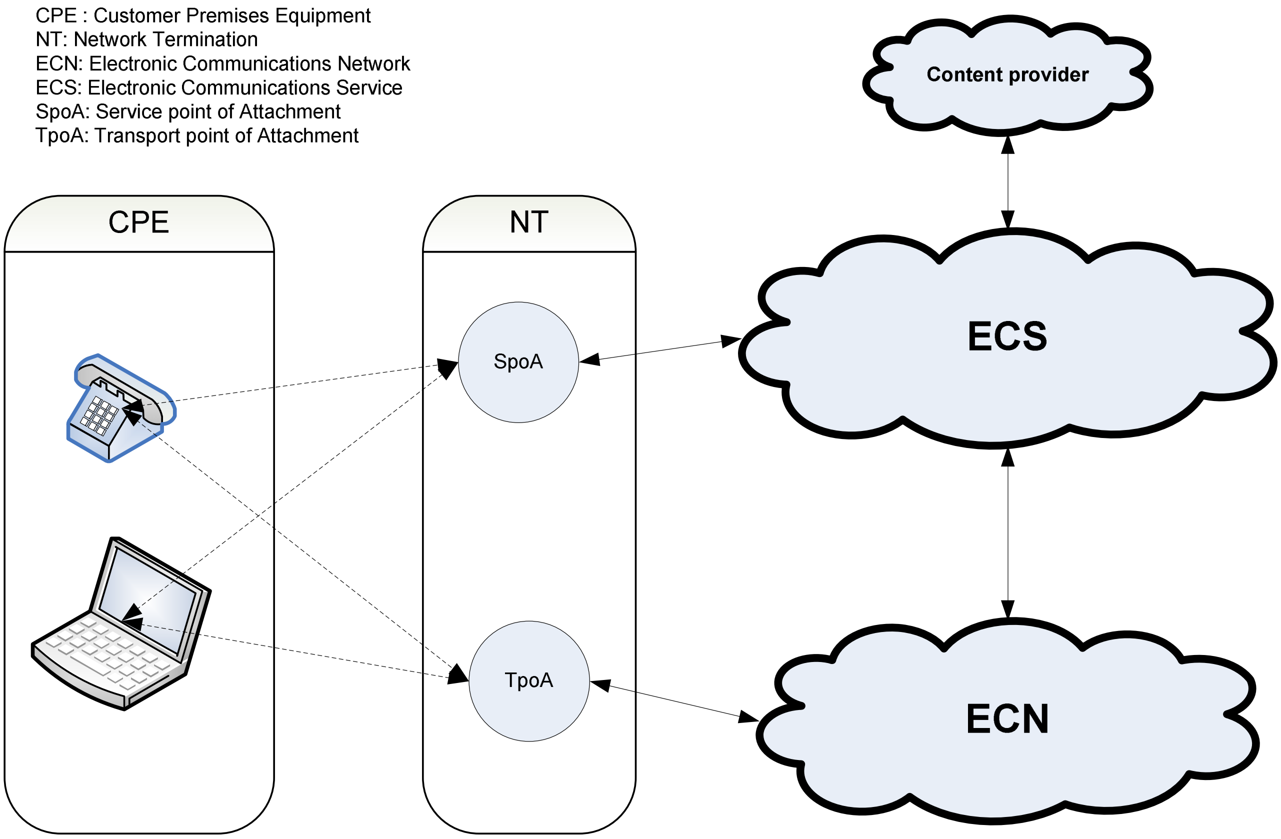

CPE : Customer Premises Equipment
NT: Network Termination
ECN: Electronic Communications Network
ECS: Electronic Communications Service
SpoA: Service point of Attachment
TpoA: Transport point of Attachment
Content provider
CPE
NT
SpoA
TpoA
ECS
ECN

Figure 6.1: The ECN&S architecture from the framework directive

In the context of the Next Generation Network (NGN) developed in TISPAN and 3GPP the IMS serves as the technology platform for the ECS.

6.2.3 Application service technologies

6.2.3.1 eSignature

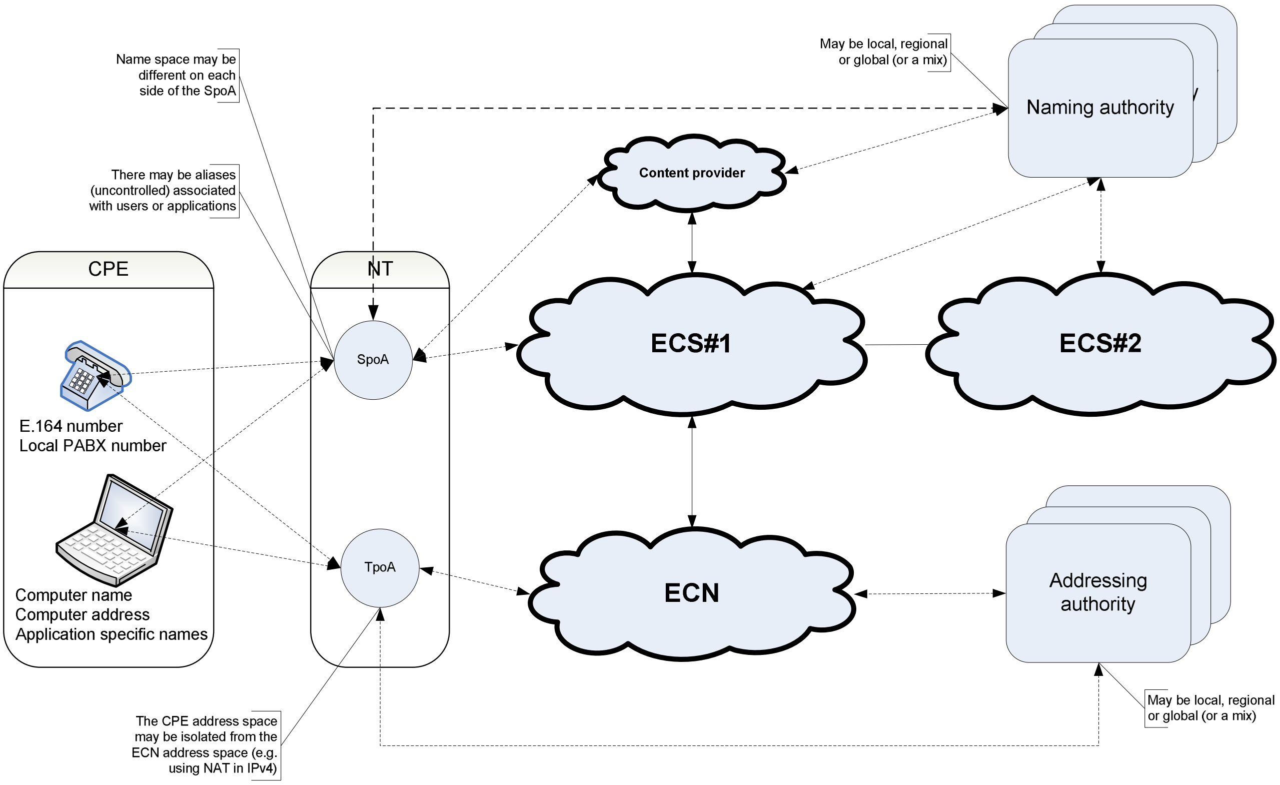
The technology of eSignature builds on public key cryptography to develop a scheme for digest creation and validation that can be validated by a third party such that the following are true:

- the signature is uniquely linked to the signatory;
- the signature is capable of identifying the signatory;
- the signature is created using means that the signatory can maintain under his sole control; and
- the signature is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

In an eHealth environment where documents (sets of data) are moved and where the parties are unlikely to have established in advance a symmetric security association the use of eSignature techniques is likely to prove critical in achieving trust and assurance in the data received.

6.2.3.2 Naming numbering and addressing

A key element in achieving the goals of eHealth is the ability to uniquely identify individuals and to associate them to a location on the physical network. In general individuals and objects will be named and thus subject to naming from a naming authority, whilst the network that links objects will be addressable and thus the location of objects will be subject to addressing from addressing authorities. Figure 6.2 shows some of the concerns raised for NGN networks from the naming and addressing domain.



Name space may be different on each side of the SpoA
There may be aliases (uncontrolled) associated with users or applications
May be local, regional or global (or a mix)
Naming authority
Content provider
CPE
NT
SpoA
ECS#1
ECS#2
E.164 number
Local PABX number
Computer name
Computer address
Application specific names
TpoA
ECN
Addressing authority
May be local, regional or global (or a mix)
The CPE address space may be isolated from the ECN address space (e.g. using NAT in IPv4)

Figure 6.2: The ECN&S architecture and the role of naming and addressing authorities

6.2.3.3 Smart cards

The ETSI technical committee Smart Card Platform (SCP) is working with a wide range of experts from all over the world to ensure that the next generation of Smart cards meets the requirements of the market and at the same time allows the technology available to the platform to develop at a natural rate whilst retaining support to the existing market. A series of ETSI specifications have been established describing Integrated Circuit Cards (ICC) in general, Universal Integrated Circuit Cards (UICC), but also toolkits for creating card-based applications.

- Intrinsically secure: Yes.
- Standardization bodies: ETSI, ISO.
- Standards activity: Banking industry, GSM OA.

Whilst it is not the intent of the present document to list all available standards for smartcards it is useful to note those of most application to eHealth. In particular the means to register applications for telecommunications is addressed in TS 101 220 [i.20] whilst the vocabulary of smartcards is described in TR 102 216 [i.21].

6.2.3.4 Messaging services

Messaging services are characterized in general in their form of connection that allows store and forward networks to carry them. Services that can make use of messaging services have to be delay tolerant.

NOTE: Messaging, store and forward services are analogous to the postal services in that there is no connection between transmitter and recipient.

6.2.3.4.1 Short Messaging Service (SMS)

SMS was developed as an extension to the signalling of GSM cellular networks where the content of the SMS is a package added to a variant of the call setup message. The maximum size of an SMS message is limited by the signalling protocol and by the form of radio link. Most digital networks support a form of SMS (e.g. TETRA, DECT, 3G-UMTS, and the PSTN with ISDN or SIP core capabilities).

A number of applications have been built on SMS that may be extended in the eHealth domain.

SMS is a confirmed service based on "store and forward". However, not all networks support acknowledgement, and the delay may be unbound. This service can also experience delayed delivery under certain circumstances and there are many other aspects of SMS that need to be considered.

6.2.3.4.2 e-mail based messaging service

Email is a more feature rich variant of messaging and for examples based on the IETF (Internet) set of services allow a number of media to be carried. Email is endemic in business and existing eHealth professionals are users of email for document exchange.

6.2.3.5 Telephony services

Telephony refers to the general use of equipment to provide voice communication over distances, specifically by connecting telephones to each. In most modern telecommunications systems there is a distinction of tele-service and bearer-service. There is a mapping of this distinction to the ECN&S framework (see figure 6.1) where tele-services map to the ECS and bearer-services map to the ECN.

6.2.3.6 Location based services

Location based services take a number of forms depending on the technology of the underlying network. There are cell based location services, GPS assisted services (covering satellite location assistance in general and thus including Galileo), fixed line access services and others. In each case the advantage of accurate physical location of the patient, particularly for rescue and first aid missions by providing accurate location data to the emergency services so they can reach victims of accidents, etc. faster and more efficiently cannot be overstated.

6.2.3.7 Application programming and development interfaces

In most layered communications systems a service at layer N is made visible to layer N+1 through a set of standardized (but not necessarily open to test) functions that map to the peer-to-peer protocol visible at layer N. As layer N is providing a set of services to layer N+1 the interface is most often referred to as a Service Access Point (SAP). In a programming environment the set of primitives at a SAP is often made visible in packaged functions of an Application Programming Interface.

EXAMPLE: The Open Systems Alliance (OSA) provide a set of APIs (The OSA specifications) that define an architecture that enables application developers to make use of network functionality through an open standardized interface.

6.2.4 Summary of communications technologies

For the purposes of eHealth the characteristics of ubiquity and security are not met in full by any existing Wide Area Network technologies.

Table 6.1: Summary of classification of wide area communications technologies

	GSM	GPRS	DECT	TETRA	3G	WiFi	WiMAX
Mobility	Yes	Yes	No	Yes	Yes	No	Yes
Intrinsically secure	Privacy enhanced	Privacy enhanced	Privacy enhanced	Yes	Privacy enhanced	No	No
Connection capability	Packet, Circuit	Packet	Packet, Circuit	Packet, Circuit	Packet, Circuit	Packet	Packet
Connection topology	Unicast	Unicast	Unicast	Unicast, Multicast, Broadcast	Unicast, Multicast, Broadcast	Unicast, Multicast, Broadcast	Unicast, Multicast, Broadcast
Content	Audio	Data	Audio	Audio, data	Audio, data, video	Data	Data, Video

6.3 Further work to be undertaken in SDOs (development of existing standards to support eHealth)

In further development of telecommunications for eHealth the following activities need to be carried out:

- Extension of the terms of reference of the Technical Bodies to embrace the eHealth architecture.
- Validation of the abstract parameterization of services.
- Integration of an open interface to the eHealth middleware services.

7 Abstract User Service Model

7.1 Overview

The eHealth system may be simplified to a model of raw data acquisition and from there its transfer and processing to derive eHealth information. The model is also covered by the use cases in clause 8 but may be further illustrated using figure 7.1 as a basis.

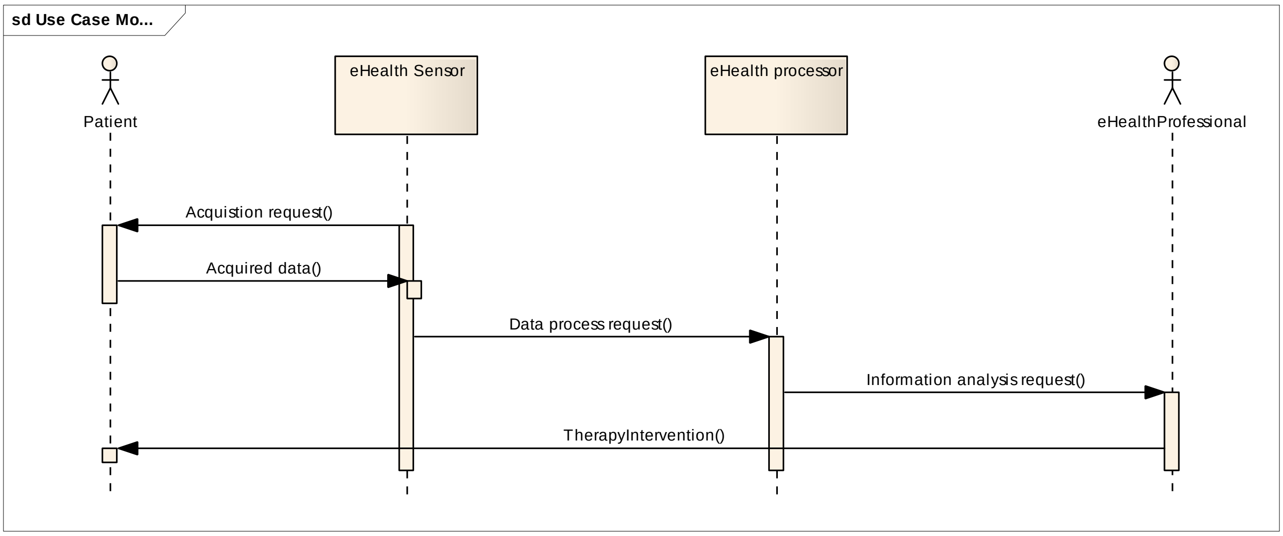


Figure 7.1: User service model interactions

7.2 eHealth Info Acquisition

In eHealth a large element of success is the gathering of data related to the health of a person, termed the acquisition phase. Whilst much of the data will come from direct monitoring of the patient (by means of BANs, PANs, PNs and PN-Fs) much will also come from knowledge of where the patient lives (environmental data), the family health history (genetic factors) and what the patient does (more environmental and contextual factors).

7.3 eHealth Info transfer

Action of transmitting and merging health information.

7.4 eHealth Info processing

Raw data is often poor as the basis of therapeutic intervention and therefore information has to be derived from the data. This action of performing or running intelligent algorithms or logical procedures in order to extract useful information that might help on the decision procedure is referred to here as processing. This phase will try to mimic or ease the task of the doctor while making decisions.

7.5 eHealth Info collation

After examination and comparison of the available information, sensible health information or process results have to be highlighted. eHealth information collation brings together different pieces of data so that the similarities and differences can be seen (i.e. automatically display blood analysis results setting the logical categories but also ordering data based on importance).

7.6 eHealth security services

eHealth security services refers to the set of procedures that assure the authenticity, integrity, confidentiality and reliability during acquisition, manipulation and use of eHealth information processes, in addition to assuring that only authorized parties are able to invoke the suite of eHealth information services. In addition the security services ensure the protection of the actors in the eHealth environment in compliance with existing regulation (e.g. privacy, data protection, law enforcement).

7.7 Imprinting/personalization

Act of automatic configuration of a device so that it is bound to a person (owner). It involves setting the necessary parameters that enables secure and private communication with other personal devices. Besides that the devices are initialized and configured according to the user profile and requirements.

7.8 Synchronizing eHealth Info

Act of updating/upgrading eHealth information of one or more resources so that it causes to indicate or point to the same data. Synchronization enables that similar information is shared on many places and avoids the risk of losing data as the information is replicated.

It can also refer to the act of updating information from the person that is being monitored so that the validity time is renewed.

7.9 Further work to be undertaken in SDOs in support of the abstract user service model

In further development of specific eHealth support to the abstract user service model the following activities need to be carried out:

- Definition of eHealth user profiles (existing work in ETSI TC HF may apply).
- Definition of core processing functionality and data transfer models.

8 Use cases

8.1 Introduction to use cases

The role of use cases in the present document is to illustrate and examine the communications and data requirements for eHealth. The use cases chosen are illustrative and the set of use cases do not represent all the possible uses of the eHealth platform.

The use cases presented try to cover issues of data transfer and analysis of the users involved taking account of relatively simple data transfer and access, through near real time remote patient monitoring, to real time remote surgery.

The use cases in each case consider the originating and terminating parties for the eHealth communication. The following cases are considered:

- Patient originated: Health Professional terminated (noting that the Health Professional could be equipment rather than a person).
- Health Professional originated: Patient terminated.
- Health Professional originated: Health Professional terminated.
- Patient to Health Professional dialogue.
- Health Authority to Citizen.

A second major attribute considered as use cases (in the UML sense) describe the form of eHealth intervention which may invoke each other:

- Telemedicine.
- Remote monitoring.
- Mobile monitoring.

- Therapy intervention.
- Emergency intervention.

Finally in order to assist in classification of the communications requirements the following additional parameters are considered in expansion of the use cases and use case scenarios:

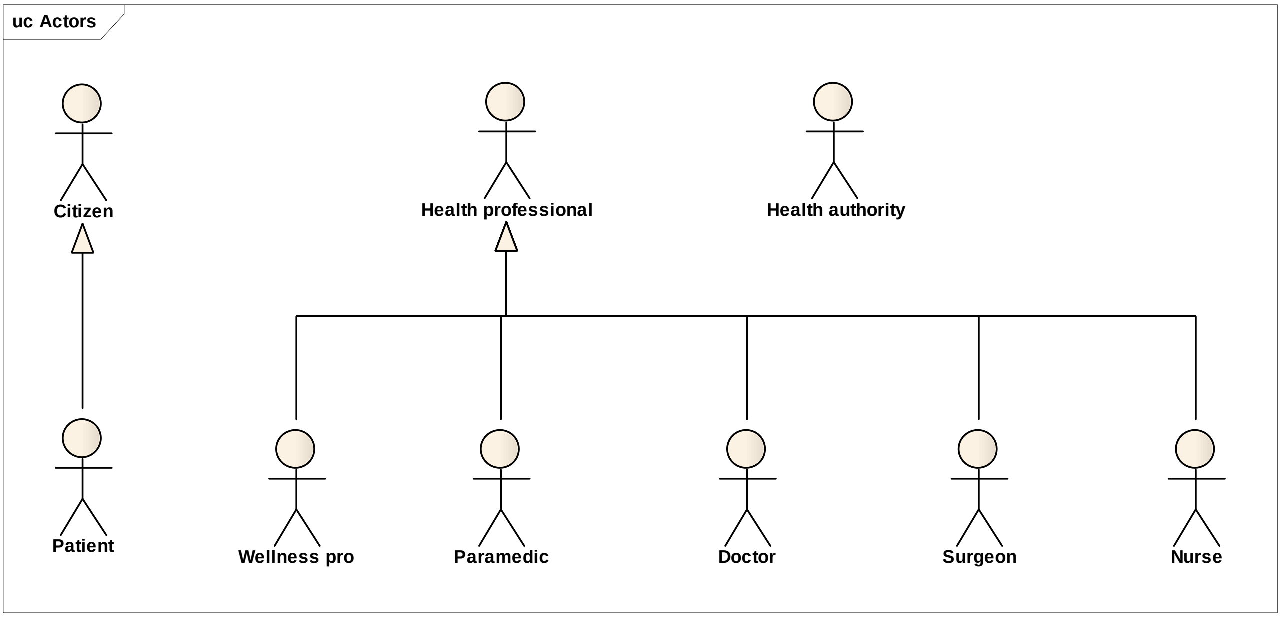
- Unidirectional.
- Acknowledged uni-directional.
- Symmetric bi-directional.
- Asymmetric bi-directional.

In eHealth it is anticipated that a significant proportion of the communication will be between actors where the actor is a machine, for example, between monitoring equipment, e.g. a BAN, and eHealth middleware; the Health professional will receive alarms and will when necessary or convenient access the information (where the distinction between necessary or convenient will be determined in part by the priority of the message and by the pre-processing of the message content).

8.2 eHealth actors

In order to examine use cases in general a number of actors are defined. In the figures that follow there is some consideration of specialist forms of eHealth professional and of patients as citizens.

NOTE: The list of eHealth actors is indicative and is not considered as complete.



NOTE: Each actor may be represented by a machine (i.e. a doctor does not need to be a human being).

Figure 8.1: Actors in use cases for eHealth analysis

In addition to the patient being a simple case of a citizen suggested in figure 8.1 the patient may also be represented by 3rd parties such as carers and sports trainers say. In such cases the authority of the 3rd party to act on behalf of the patient may be represented as shown in figure 8.2.

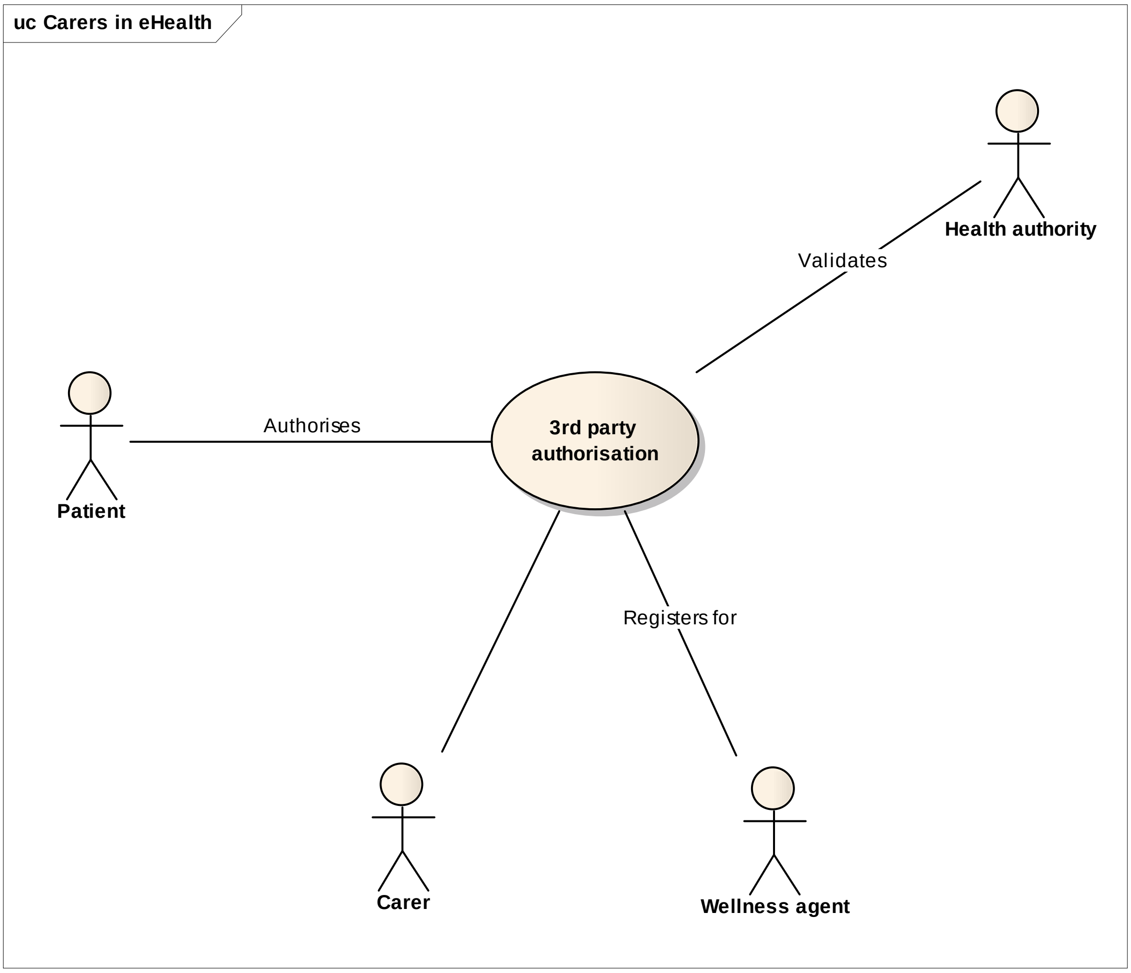


Figure 8.2: Carers and like actors being authorized by patient

8.3 Non-specific eHealth scenarios

In addition to direct health intervention scenarios there are a number of additional use cases that have to be considered as they provide a link to the necessary societal safety and security guards for eHealth in general. The set of use cases and their interaction in figure 8.2 identify a need for the eHealth system to support the registration of eHealth professionals and the ability of patients to validate the registration of an acting eHealth professional. The relationships shown include the identification of a Health Authority to manage the registration of eHealth professionals.

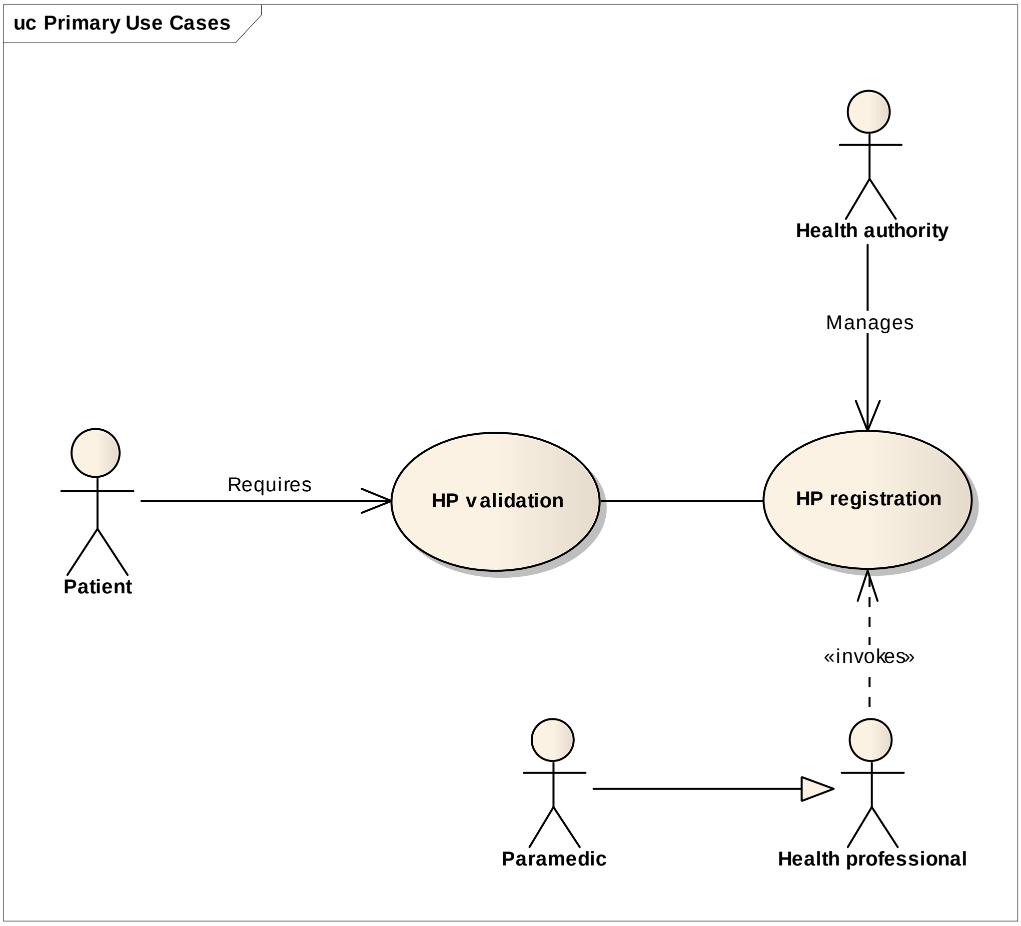


Figure 8.3: eHealth registration and validation use cases

8.4 Generic use cases

The use cases in clause 8.1 are provided pictorially in figure 8.4 and examined in text below.

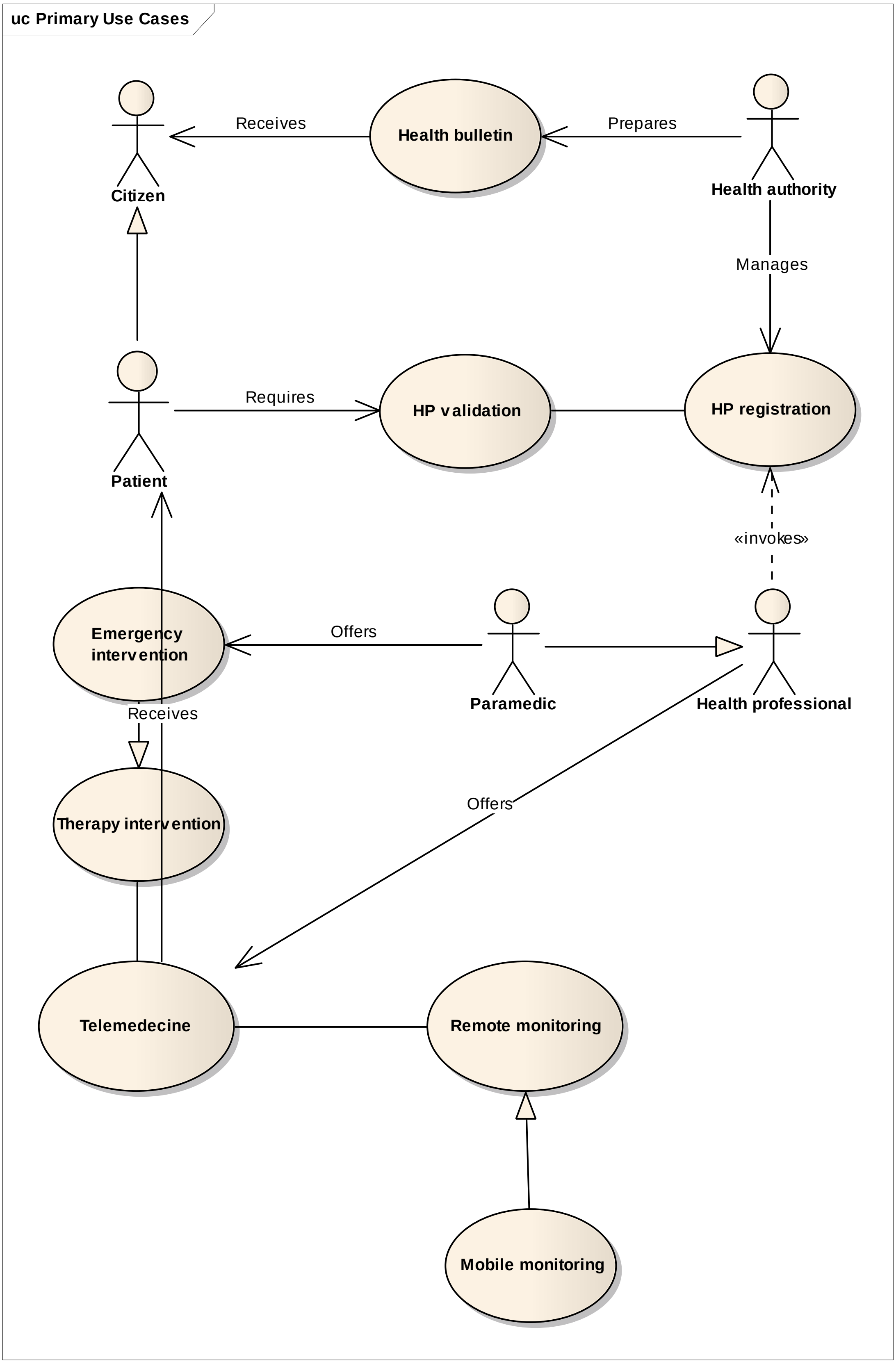


Figure 8.4: Interaction of sample use cases in eHealth

8.4.1 Telemedicine

Telemedicine covers the entire discipline of providing health services with the assistance of telecommunications services.

8.4.1.1 Therapy intervention

A therapy intervention will most often be invoked from health professional to patient, perhaps based on patient to health professional monitoring. As an example a diabetic may have a body mounted or implanted sensor that indicates an insulin injection is required, the sensor will report the problem to the eHealth platform which will respond with a command to provide the insulin injection.

The technology of intervention may evolve without change in the basic use case scenario. Initially in telemedicine the interventions may be by voice conversation between the patient and the health professional, but may evolve to the BAN and the PN-F of which it is a member acting without direct human intervention, but where a record of the intervention is maintained in the PN-F.

8.4.1.2 Emergency intervention

Emergency intervention is a specialism of generic therapy intervention and covers the special case of intervention being administered by a paramedic, or where the urgency of intervention may require that all messages in the sequence are treated with high priority.

An example of an emergency intervention scenario is given in figure 8.5 showing the forms of interaction between the different actors. A characteristic of emergency intervention could be classed as chaos: emergencies happen in inconvenient places (e.g. railway cuttings, mines) or that as a result of the emergency become inconvenient (e.g. a town destroyed by earthquake); emergencies happen at inconvenient times (e.g. late at night, at weekends, at holidays); emergencies happen where communications are difficult (e.g. loss of infrastructure as a result of the emergency, radio communication may be unsafe).

Other characteristics of emergency intervention, particularly in larger scale events, are that the medical services assist the most urgent victims immediately, evaluating the injuries suffered and (as a direct consequence of the eHealth initiative) consulting the patient's health record to apply appropriate first aid. It can be assumed for modelling purposes that some of the patient records will be held in other countries than the one in which the event has occurred.

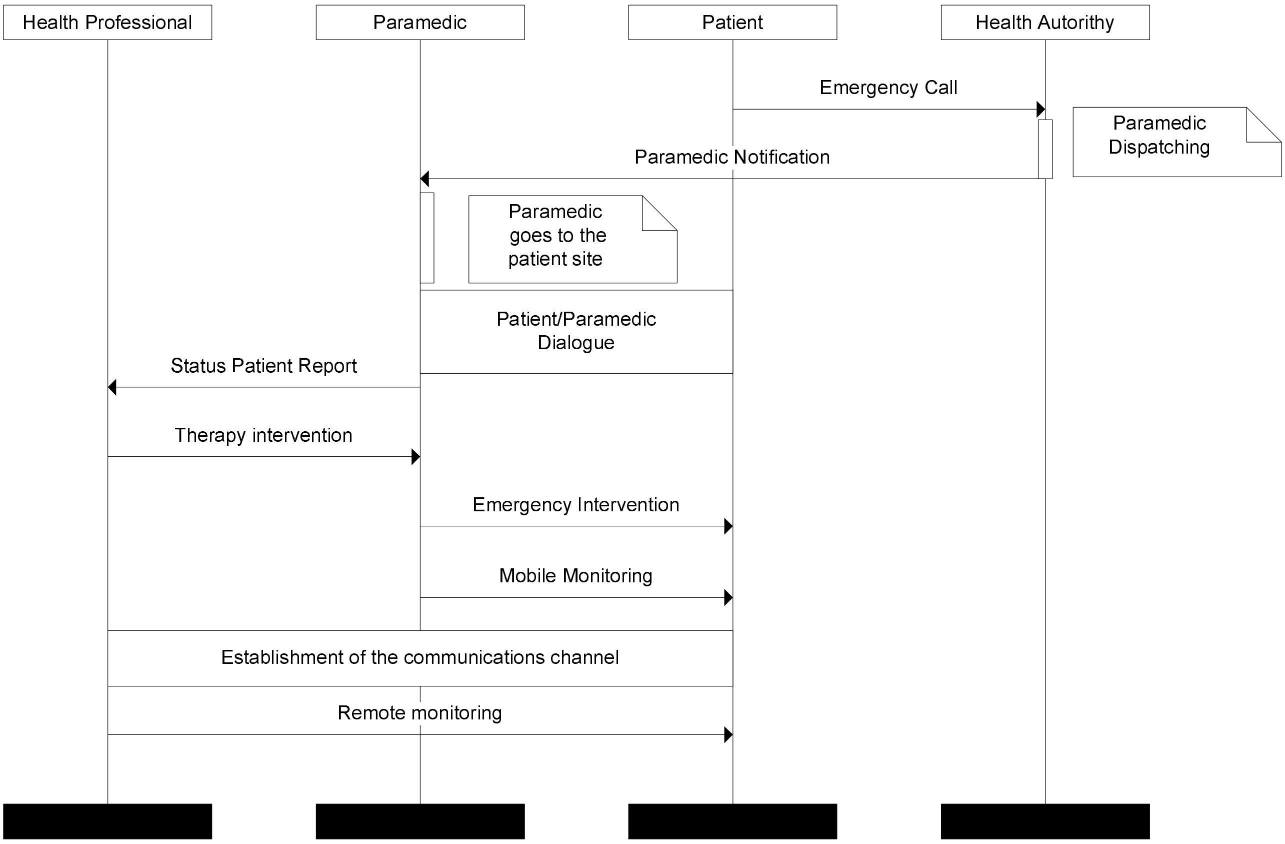


Figure 8.5: Emergency use case interactions

As well as the requirements included in the previous user case, the following can be highlighted:

Ease of deployment of communications infrastructures: Emergencies by definition are unexpected, often in places where either there is no communications network coverage or where the disaster itself has made the network useless. For this reason, it is necessary to make available technologies and techniques enabling the rapid deployment of networks that can be extended as the situation comes under control (e.g. in the first instance a satellite phone may be the only facility available (surface incidents) but drop in cellular base stations may become available using satellite or microwave backhaul pending full network connectivity).

Network federation: In situations such as the ones described, it is habitual to have numerous rescue teams each with its own communications infrastructure coming together in the same area. With the aim of managing all the different resources it is desirable that federations of networks are automatically configured coordinating the distinct resources in order to offer superior qualities of service to those provided by the networks working independently.

Service composition and orchestration: In the same way as with transmission and switching resources, the aggregation in one geographical area of a plethora of services makes it desirable to enable them to be orchestrated suitably by the different agents involved in the emergency.

8.4.2 eHealth monitoring

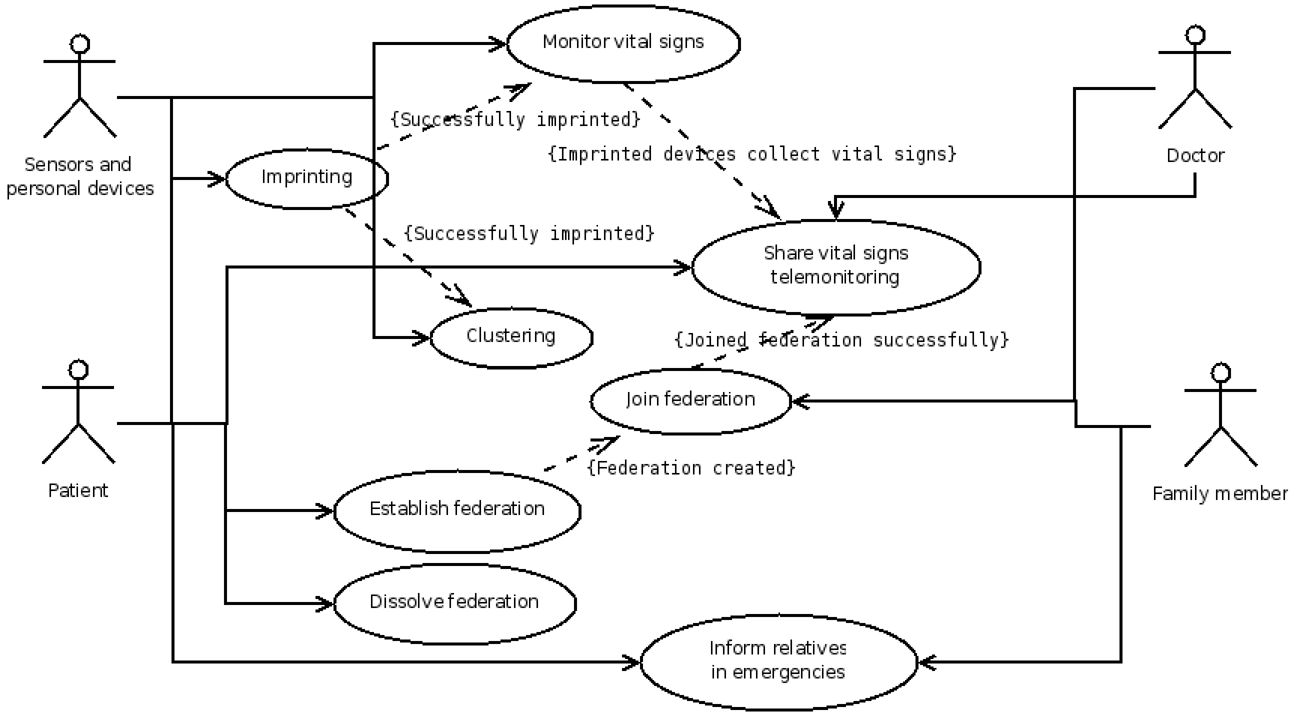


Figure 8.6: Monitoring use-case with body area networks, personal networks and their federations

8.4.2.1 Remote monitoring

Remote monitoring is a practice where the patients, whom are not at the same location as the health care provider, are monitored. A patient is surrounded by a set of sensors and devices (e.g., at home). The recordings of these devices are transmitted to the health care provider via some communication infrastructure. This use-case reduces the time commitment of the care providers.

8.4.2.2 Mobile monitoring

Mobile monitoring can be defined as ubiquitous computing, medical sensor, and communications technologies for monitoring vital signs of patients. The developments in wireless communications along with developments in pervasive and wearable sensor technologies impact future telecare systems. New technologies such as personal networks for eHealth applications provide solutions to the challenges such as eInclusions in terms of eHealth applications, increase in the healthcare costs and uneven distribution of health care quality. A prerequisite for the successful deployment of eHealth application for continuous monitoring of a patient's vital signs is the QoS support (delay, jitter, accuracy, user mobility and number of concurrent users, etc.) by underlying wireless networks. For social acceptance of eHealth application, dependability and reliability are key user requirements. There is a trade-off between the reliability of a system and its performance. The eHealth data of patients consists of various parameters, text, voice as well as video for diverse chronic diseases. These data will need to coexist together as well as with other commercial data such as voice, video (streaming or real), multimedia, and Internet.

The mobile monitoring use-case requires utilization of several short-range body-area network components such as implant/wearable sensors. Such devices will need to provide short-range communication; typically shorter than three meters. From the user perspective, these devices will need to be affordable and comply with international standards to enable cross-border operation. Energy-efficiency is one of key issues for eHealth applications. Since, as in the remote cardiac monitoring use-case, the patients may be mobile, the battery life of the pervasive devices will need to last enough to provide the required service. For example, the battery of an implantable device will need to last for some months whereas a PDA will need to provide service for several days before battery depletion. Energy scavenging is one of the popular research issues for this purpose. Low power, low cost, yet robust and secure short-range solutions are needed for supporting health and wellness applications operating anytime, anywhere.

8.5 Objectives and requirements arising from use cases (general)

In general there are a number of requirements arising from the use cases and their placement into the eHealth architecture proposed in clause 4 of the present document. The requirements are stated in accordance with the recommendations given in TR 187 011 [i.8] in the form of "Precondition - Stimulus - Response".

8.5.1 Objectives arising

- A user should expect ubiquitous network connectivity.
- The user should reasonably that eHealth equipment that requires to be connected through a network should be able to access the network.
- The eHealth system should support the interworking of heterogeneous devices and networks.
- An eHealth device should be able interact securely with the eHealth infrastructure.
- Information held within an eHealth device should be protected from unauthorized access, modification and destruction.
- Services provided within the eHealth infrastructure should be available only to authorized users of the eHealth system.
- Information sent to or from a registered user of the eHealth system should be protected against unauthorized or malicious modification or manipulation during transmission.
- Information sent to or from a registered user of the eHealth system should not be revealed to any unauthorized 3rd party.
- An eHealth user should be able to communicate confidentially with other users within the eHealth network.
- Details relating to the identity of an eHealth user should not be revealed to any unauthorized 3rd party within the eHealth network or in the wider ICT networks.
- Access to and the operation of services by authorized eHealth users should not be prevented by malicious activity within the eHealth network or in the wider ICT networks.
- The eHealth system should be able to collect information relating to the context of any eHealth transaction.
- The eHealth system and the devices used to access it should allow any member of society to be able to use the system.

8.5.2 Requirements arising

The following requirements may be derived from analysis of the objectives stated in clause 8.5.1:

- Ubiquitous network connectivity: The network organization will need to be seamless and ubiquitous by supporting all aspects of communication, including handling mobility of devices. Further, group communication with other networks and third parties will need to also be supported.
- Support heterogeneous devices and networks: An eHealth system may consist of a wide range of different mobile and stationary devices, wireless technologies, and networks. It will need to operate efficiently and seamlessly in heterogeneous environments. It will need to not waste energy unnecessarily in nodes with scarce energy resources.
- QoS and reliability: Some eHealth applications may have high demands for end-to-end quality of service (QoS). It is important that routing and mobility management mechanisms are quick enough so that QoS requirements can be met also when devices are mobile.

- Naming and service management: Technical aspects of the network mechanisms will need to be hidden from the patient and the applications by means of naming solutions as well as service discovery and management. This should also allow a greater amount of self-configuration and adaptation.

- Context-awareness: Today's patients expect their sensory devices and applications to be intelligent, properly predict the users' intentions, and automatically adapt to a changing environment. Hence, context information is valuable since the PN and applications may use such information to better respond to the situation. For example, when monitoring the vital signals, it is important to know whether the patient is walking, running or taking a rest. Such context information will need to be collected without user intervention.

- Security and trust: A security system that protects the monitoring system from unauthorized usage is needed. The system should support controlled sharing of personal resources, services and content with others according to commonly agreed rules.

- Privacy: Sensitive personal information about the vital signal of a patient including the location of the user will need to be protected by the system. Unauthorized access to such information will need to be avoided.

- Usability and form factor: Anyone including children, pensioners, and the physically impaired will need to be able to use such a system. All devices/sensors will need to be self-configured and able to communicate seamlessly with each other without requiring complicated user intervention. Instead, the system will need to support the user in his/her daily activities in an efficient and satisfactory way.

9 Gaps in standardization for eHealth

9.1 Overview of the gaps and filling them

The bulk of the present document analyses the eHealth platform and how technology fits to it. In each clause of the report to this point the core capabilities have been examined of technology and their fit to a proposed architecture. In the course of the analysis a number of "gaps" have been highlighted, where the gap refers to the technology as it exists and its fit to the eHealth platform. The report does not address the political and societal structures that are needed to support eHealth and thus does not address the gaps between the existing political and societal structures and the form that those structures have to take to assure success of eHealth. It is however assumed that in addressing the gaps at the technical level that any gaps in the political and societal structures are also filled.

The priority of filling gaps is addressed in the present clause but is necessarily complex with a number of fixed and conditional dependencies that are identified where known. It is an unfortunate consequence of the gaps though that whilst there are dependencies work has to be started on the assumption that the dependencies are resolved during development rather than only starting development when the dependency is resolved. This is essential to speed up development and will require management of a number of parallel strands of eHealth.

It is also noted that the eHealth platform will coexist with other application platforms (including eGovernment, eSociety, eEntertainment, eCommunication) on a common ICT platform. The priority of all competing platforms on a common infrastructure is not addressed other than by assuring separation of the platforms. However it is noted that a failure in the shared (common) ICT platform will affect all the platforms it supports and therefore the resilience of the ICT platform is not an eHealth specific objective.

It has to be strongly re-asserted that an overriding goal of the eHealth initiative is to give assurance of interoperability of eHealth systems and devices. This is to be achieved in large part by the architecture described in clause 4 and in the remainder of this clause in the form of a gap analysis and identification of future work.

9.2 General eHealth architecture

In further development of the eHealth architecture the following activities need to be carried out:

- Development of interface definitions between the abstract layers of the eHealth architecture.

- Development of a robust data dictionary to ensure intelligent and comprehensive transfer and operation of data.

- Development of RF co-existence standards to ensure that eHealth devices are able to operate without interference and without restriction on the geographic location.

NOTE: This may require harmonization of frequency allocation and power profiles for devices.

In terms of priority and activity to fill the gap the architecture is the single pre-requisite for fitting technology to eHealth.

9.3 Specific eHealth support network architectures

In further development of specific eHealth support network architectures the following activities need to be carried out:

- Integration of PAN, BAN, PN and PN-F to eHealth.

In the bulk of the use cases for eHealth the elements closest to the patient are those that form part of BANs and PANs with their integration to PNs and PN-Fs. However the success of PNs and PN-Fs require significant investment in PAN and BAN standardization. There are a small number of key gaps to fill as outlined below:

- Convergence entities on top of the MAC mechanisms which are able to provide the transparent cooperation between heterogeneous wireless interfaces (extending the work being carried out in IEEE 802.21 [i.24]).
- Addressing and routing schemes to route packets between Personal Nodes as well as to and from Foreign Nodes (dynamic conditions).
- A naming scheme is needed to help the user overcome the difficulty of using IP addresses.
- Service discovery and provision architecture as well as service composition and orchestration.
- Self-configuration and maintenance will need to be supported so that non-technical users can operate their Personal Networks in an efficient way.

9.4 Development of existing standards to support eHealth

In further development of telecommunications for eHealth the following activities need to be carried out:

- Extension of the terms of reference of the Technical Bodies to embrace the eHealth architecture.
- Validation of the abstract parameterization of services.
- Integration of an open interface to the eHealth middleware services.

9.5 Development of support of the abstract user service model

In further development of specific eHealth support to the abstract user service model the following activities need to be carried out:

- Definition of eHealth user profiles (existing work in ETSI TC HF may apply).
- Definition of core processing functionality and data transfer models.

9.6 General

9.6.1 eHealth Device Safety

The eHealth system will include a large number of sensor devices. These devices should also follow the two main European Directives that apply to electrical and electronic equipment with respect to health, safety and performance:

- The Low Voltage Directive (LVD) 2006/95/EC [i.25] lays down the requirements covering all health and safety risks of electrical equipment operating within certain voltage ranges. Consumer goods that are not covered by the LVD are dealt by the General Product Safety Directive (GPSD) 2001/95/EC [i.26].

- The Electromagnetic Compatibility (EMC) Directive 2004/108/EC [i.27] lays down requirements in order to preventing electrical and electronic equipment from generating or being affected by electromagnetic disturbances.

An extensive list of EMC related standards can be found in the EMC List [i.10]. However it is not clear that the considerations for device safety are eHealth aware, in other words are the safety risks congruent with the evolving eHealth device set, in particular for BANs and PANs where many devices subject to the LVD may (or will) be active at the same time across the human body and therefore there may be some influence of the body on the how the devices operate and how they cumulatively impact the body they are reading (assuming the sensors are acting as readers and not as actuators).

9.6.2 Context Awareness

Context-Awareness addresses the need to automatically adapt an application or service to a current situation a user is in. The situation is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves. For example, when monitoring the vital signs of a patient, the context of the patient can be several states such as walking, running or resting. Many projects carry out their work on the assumption that the applications or services are context-aware. This assumption is questionable because provisioning of personal services cannot be implemented without appropriate context. Knowing the context of the patient helps interpreting the collected data better and produces more accurate diagnosis.

Context awareness allows the eHealth servers to take intelligent decisions based on the context in which the vital parameters were taken. Near body area networks or sensor networks can be used to collect context.

Table 9.1: Classification of general eHealth gaps

Gap	Related SDOs	Priorities	Time scale
ehealth service classification	ETSI	H	2 years
Device safety	ETSI	M	2 years
Dependability	ETSI	M	5 years
Context awareness	ETSI, IEEE	L	10 years

9.7 Control Plane

The following gaps apply in the Control Plane for eHealth.

9.7.1 Quality and Grade of Service for eHealth

In eHealth applications, different classes of traffic with different QoS requirements have to be transmitted using the shared infrastructure simultaneously. Optimization of network performance depends on the traffic classification. The communication infrastructure has to satisfy the QoS requirements of different classes of applications. Applications may use the differentiated services from the underlying network with a set of parameters such as delay, jitter, response time, packet loss and priority. The coexistence of various traffic types reduces the manageability. To solve this problem, the QoS parameter sets will need to be associated to different service classes. For example, some applications require high availability whereas some others may require higher priority. A service classification proposed by the Freeband project in The Netherlands [i.5] is:

- Class 0: highest priority requiring real-time communication (e.g., emergency cases).
- Class 1: near real-time communication within a short period (e.g., cardiac monitoring).
- Class 2: periodic messaging (e.g., average heart rate twice per day).
- Class 3: communication from time to time (e.g., arrhythmia evaluation).

The present document recommends that a service classification along the lines above is adopted in eHealth standards.

9.7.2 Security

The role of security technologies in eHealth cannot be understated but cannot be taken as simply a shopping list of capabilities. Security technology has to exist in the context of a risk analysis as recommended in EG 202 387 [i.22] and in TS 102 165-1 [i.23].

- Trust, personalization and imprinting (TC HF is working on eHealth personalization).
- Identity management (ongoing works in ETSI and ITU):
  - Biometrics.
  - Credential management (ongoing works at national levels).
  - Certificate authorities.
  - Revocation.
- Device capability (processing for security algorithms).
- Security tokens for Electronic European Health Insurance Card (ISO Standard).

9.7.3 Personal Networks

A typical eHealth application consists of heterogeneous devices and technologies. Not only devices, but due to the ubiquity the access networks may be heterogeneous, as well. An important issue is to provide the service seamless by abstracting the underlying heterogeneity. For this purpose, personal network concept is an ideal opportunity:

- The process of configuring a node to become part of a PN is called personalization and is a prerequisite to any cluster and PN formation. Personalization has a long-term character, but also needs to be transient to facilitate the change of ownership. It can be achieved by "imprinting" a new node with protected credentials when incorporating it into the PN for the first time. At that time, the node receives valid long-term PN security credentials and is ready to establish secure associations with any other personal node in the same PN. While the personalization step requires user intervention, the subsequent secure associations that the node establishes with each of the other personal nodes are done automatically and transparently to the user. During cluster and PN formation, nodes authenticate each other and establish short-term security associations for the protection of data and control traffic.
- Convergence entities on top of the MAC mechanisms which are able to provide the transparent cooperation between heterogeneous wireless interfaces (extending the work being carried out in IEEE 802.21 [i.24]).
- Addressing and routing schemes to route packets between Personal Nodes as well as to and from Foreign Nodes (dynamic conditions).
- A naming scheme is needed to help the user overcome the difficulty of using IP addresses.
- Service discovery and provision architecture as well as service composition and orchestration.
- Self-configuration and maintenance will need to be supported so that non-technical users can operate their Personal Networks in an efficient way.
- Management functionality that will need to be considered in standardization:
  - How the clusters are formed.
  - Mobility of the patients along with the core cluster and remote clusters.
  - Device capability configuration, calibration and distribution.
  - If the application requires, anonymity of the patients will need to be provided.
- From the networking view point, issues that will need to be considered are:
  - Intra- and inter-cluster routing.

  - Tunnelling among clusters.
  - NAT traversals.
  - How to identify and distribute the capability of the gateway functionality.
  - Application prioritization and QoS provisioning among different classes of eHealth related and other applications.
  - Networking and connectivity layer abstraction and PN application programming interface to enable eHealth middleware development.
  - Interworking with existing technology.
  - Energy-efficient and radiation issues.

9.7.4 Personal Network Federations

A PN is a person-centric (patient) network that provides the user with access to personal resources (e.g., eHealth sensors), services (e.g., vital sign monitoring), and contents (e.g., processed vital signs such as average heart rate) regardless of the location of the user. Sometimes it is also beneficial to share personal resources, services, and content with others to achieve a common objective that would not be possible by a single PN. For instance, to get access to infrastructure networking facilities or to provide access to specific information, such as documents, real-time images, and sensor information, PNs can federate into a group-oriented network. A PN federation (PN-F) is a temporal, ad hoc, opportunity- or purpose-driven secure network of independent PNs. An example scenario for federations of personal networks can be the healthcare, where family members and medical professionals federate to allow access to medical sensor information (of specific vital signs) and video images of elderly or sick people living unattended to detect potentially dangerous situations.

- Regarding the federations of personal networks, the issues that will need to be standardized:
  - Access control.
  - Service and resource discovery.
  - Service subset sharing and goal accomplishment.
  - Federation initiation and establishment protocols.
  - How to locate and identify federations.
  - How to join and leave federations.
  - For emergency situations, how to handle federation establishment in a self-organized fashion.
  - How to integrate personal networks and their federation into existing emergency telecommunications systems such as EMTEL. TR 102 653 [i.28] provides detailed information about the MESA and the interfaces of PANs with ad hoc incident area networks and others.

9.8 Application Layer

The following gap applies for the eHealth application layer.

9.8.1 Actor role and access control

Each actor in the eHealth environment when represented by a real person has to be able to distinguish their role. This leads to a system of authorization based on the Role Based Access Control (RBAC) paradigm. Roles and access control have to be specified and implemented to give strong assurance of the protection of privacy of user data in order to limit the risk of exploit of data. This is particularly important when it is considered that the same person may have different roles in the eHealth environment (say doctor and patient).

Table 9.2: Classification of eHealth application layer gaps

Gap	Related SDOs	Priorities	Time scale
Roles and access control	ETSI, CEN	M	2 years

9.9 Middleware Layer

9.9.1 eHealth System Dependability

For societal acceptance of eHealth applications dependability and reliability are key user requirements. There is a trade-off between the system's reliability and the performance. Measures of dependability quantify the ability of a system to perform its task based on some agreed specification of the desired service. The definition implies that dependability consists of a set of attributes such as availability (readiness to serve), reliability (continuity of failure-free service), safety (avoiding catastrophic failures) and security (in terms of preventing failures because of breaches). In a pervasive eHealth application, patient data accessible almost-everywhere in a ubiquitous way will need to be protected to preserve integrity and confidentiality. The dependability requirements arise not only from the increased scale and complexity of the eHealth system consisting of ubiquitous technology. Some of the issues, like defining/protecting the borders of the network or the confusion due to an unnoticeable malfunctioning part of the system, are direct implications of the ubiquity.

The dependability aims at ensuring that the service is maintained independently of ICT capability (IMS Standards may support this, but not yet covered).

An extensive list of dependability standards can be found in reference [i.10]. However, these standards do not directly deal with eHealth systems. Dependability requirements will need to be identified for eHealth applications.

9.10 Connectivity Layer

The following gaps apply for the connectivity layer in eHealth.

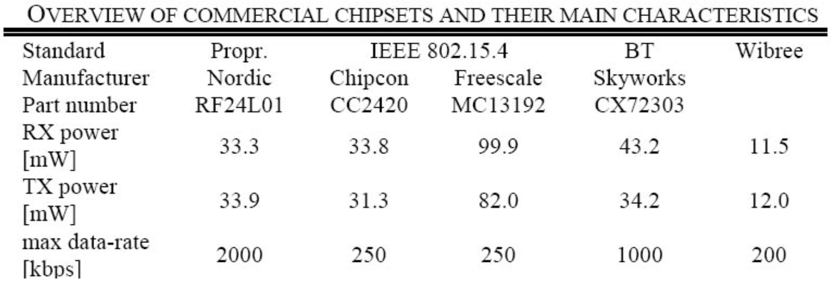
9.10.1 Body Area Networks and Radio Interface

There have been a large number of papers in the academic sphere in recent years that have identified a significant role for the Body Area Network (BAN) in eHealth exemplified by Chan et al [i.11], Norgall [i.12] and Schmidt et al [i.13]. However at the present time few standards exist to allow BANs to become a basic infrastructure element for service-based electronic health assistance. A key consideration is that since every user may carry a series of miniature nodes (acting either as sensors or actuators) which may need to last for a reasonable period, power efficiency is critical when considering the air interface.

In parallel with energy scavenging techniques and future generation of batteries, the radio interface will need to keep certain key features such as ultra low power consumption, robustness (including coexistence with legacy services), low cost, and its capability to produce a front-end topology able to be highly integrated to be compatible with the required form factor.

The evolution from low power to ultra low power will lead to power consumptions in the range of 0,1 mW to 1 mW [i.14], a requirement that currently available air interfaces cannot meet. Besides Zigbee [i.15] and Bluetooth [i.16], the commercial low power consumption chipsets analysed in the overview of [i.14] consume in the order of 10 to 100 mW, still 1 or 2 orders of magnitude over the target for eHealth.

Table 9.3: Overview of commercial chipsets (Source: extracted from [i.14])



OVERVIEW OF COMMERCIAL CHIPSETS AND THEIR MAIN CHARACTERISTICS

Standard	Propr.	IEEE 802.15.4		BT	Wibree
Manufacturer	Nordic	Chipcon	Freescale	Skyworks	
Part number	RF24L01	CC2420	MC13192	CX72303	
RX power [mW]	33.3	33.8	99.9	43.2	11.5
TX power [mW]	33.9	31.3	82.0	34.2	12.0
max data-rate [kbps]	2000	250	250	1000	200

Therefore, it is clear that new air interfaces have to be considered for eHealth applications. Activities devoted to standardization of BAN air interfaces are currently being carried out in IEEE 802.15.6 extending the work done in the past on PAN interfaces in 802.15.1 (basis of Bluetooth [i.16]) and 802.15.4 (basis of ZigBee [i.15]).

For global use of radio in a BAN there are a number of regulatory issues that remain to be resolved including common RF bands for worldwide operation and clearer understanding of interference issues. A large number of research lines are currently open in this area and these need to be collated to support the eHealth standardization requirement specifically to cover power efficient radio interfaces (perhaps based on UWB approaches that may become a suitable solution for BAN applications).

9.10.2 Interworking

The wide range of eHealth applications will undoubtedly lead to a large plethora of different devices, some of which may end up using different air interfaces. For this reason, there should be guaranteed that BAN interworking is assured even at physical layer. The simpler and most economically efficient approach would be allowing BAN nodes with a single radio interface while ensuring the presence of a BAN coordinator/gateway able to communicate to all of them regardless their specific radio interface. Nevertheless, if the evolution of the technologies leads to a cost reduction in the manufacturing process as well as efficient consumption strategies, or the particular application requires it for safety purposes, BAN devices could include dual or multiple air interfaces.

9.10.3 Asymmetric vs. Symmetric links

Flexibility of the links in terms of symmetry would be a valuable feature for the application control and its use in different services. Therefore, the devices should be able to provide information on these capabilities whenever being identified, join a network or being requested.

Since patients are acting as server for some use-cases (e.g., vital sign monitoring), the up- and down-link bandwidths of the access networks and underlying infrastructures should be considered.

Table 9.4: Classification of eHealth connectivity layer gaps

Gap	Related SDOs	Priorities	Time scale
Radio Interface	ETSI, IEEE	H	2 years
Interworking	ETSI, IEEE	M	5 years
A-symmetry	ETSI	L	5 years

Annex A: Summary of M/403

The goal of phase 1 (planning and analysis) of the programme should be to:

- list existing relevant standards and technical reports with short descriptions;
- list relevant needed tasks for achieving the result, it is important that the most needed standards are planned for adoption earlier.

The goal of phase 2 (execution) should be to agree on implementable standards, technical reports, guidelines, methods etc. In the work the European Standardization Organizations shall use quality and project management principles to ensure that content and context within and between the standards are consistent.

In phase 1, the European Standardization Organizations are to further develop the relevant recommendations set by both - but not limited to - the CEN/ISSS Focus Group report on eHealth standardization and the work carried out by DG INFSO and the i2010 Sub -Group on eHealth into a detailed work programme. In addition the European Standardization Organizations are to consider the impact of information appliances (especially those commodity, perhaps unregulated, items for personal use) in the provision of health care and to describe functional boundaries between the eHealth domain and other domains (such as finance, logistics and eGovernment). The work should also take due account of SR 002 564 [i.3] , and to provide the necessary interoperable standards to ensure that eHealth - related data can be transferred correctly and securely, including in a home network environment and/or in a chronic disease management network for older adults . The Report details which of the existing standards may be usefully implemented for eHealth applications, and which ones may have to be prepared or updated. Relevant aspects address in particular transmission aspects, technical interoperability, security, authentication, authorization, data privacy and usability.

The development of testing and verification methods, the drafting of testing standards, as well as the demonstration of interoperability between eHealth services is also key. The experience in this area exists within the European Standardization Organizations (in particular within ETSI with the Protocol and Testing Competence Centre, and the ETSI Plugtest service). The programme will list identified work items, the priority level for each of the tasks, a summary description, the expected deliverables, the lead responsibility, timetables, and approaches for public r elations, publicity and marketing.

The deliverables should include standards and technical reports such as implementation guidelines, methods for conformance testing. The work programme should include (where in scope), items to address the recommendation s of the eHealth Focus Group following on from validation procedures.

One or more open meetings shall be organized with representatives from relevant governmental, healthcare provider, industry, user and domain expert stakeholders to consolidate the draft work programme and to reach broad acceptance for it.

In order to provide optimal technological foundations, infrastructure, safety and regulatory integration in Europe and within global markets the European Standardization Organizations CEN, CENELEC and ETSI are strongly encouraged to collaborate together and with international standards organizations, (notably International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU)) as well as with European and international Standards Development Organizations and their liaisons including relevant standards consortia and organizations (such as IEEE, DICOM,HL7,OASIS,W3C,GSI and WHO). In addition, it is recommended that they see k to work with Information and Communication Technologies (ICT) companies, healthcare authorities, healthcare providers, professional healthcare associations, including large corporations and small and medium sized enterprises, in order to create a basis f or development of interoperability guidelines. Similarly, it is recommended that they seek to work in support of those organizations mandated by their government to work on the specifications for the deployment of interoperable services. This is of utmost importance that the standardization organizations further develops co-operation between experts in the standardization field and involve experts on providing healthcare services, e.g. medical professionals in order to achieve the long-term goal of interoperable health care systems not limited by borders. Furthermore it is of importance that the standardization development work is in coherence with the Government Agencies' priorities on the health care area, e.g. National health care information structure plans and guidance. This co-operation between different parties is a prerequisite for interoperable health care services, delivered in accordance with a predefined quality level and will also assure safety issues for the patients and healthcare professionals.

Another important field that also will need to be taken into account is how standards will be used in research and developmental purposes.

The resulting final work programme will be submitted to the Commission services which will consult the 98/34 Committee prior to the launch of phase 2 covered by this mandate. During phase 2 of the standardization work covered by this mandate CEN, CENELEC, and ETSI (as appropriate and recommended in the agreed work programme) shall develop the European standardization initiatives as listed in the work programme. The European Standardization Organizations shall use work structures (such as workshops, and technical committees) appropriate to the work programme.

Annex B: Bibliography

"Small-size BiTe Thermopiles and a Thermoelectric Generator for Wearable Sensor Nodes", V. Leonov, T. Torfs, N. V. Kukhar, C. Van Hoof, R. J. M. Vullers, , Proc. 5th European Conference on Thermoelectrics (ECT 2007), Odessa, Ukraine, Sep 10-12, 2007, pp. 129-133.

NPR-CEN/TR 15253: "Health informatics - Quality of Service requirements for health information exchange".

IEEE 802.11e: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment: Medium Access Method (MAC) Quality of Service Enhancements".

"Dependability Standards and Supporting Standards".

NOTE: Available at: http://tc56.iec.ch/about/standards0_1.htm.

History

Document history		
V1.1.1	February 2009	Publication