A New Framework Architecture for Next Generation e-Health Services

Maria-Anna Fengou, Georgios Mantas, *Member, IEEE*, Dimitrios Lymberopoulos, *Member, IEEE*, Nikos Komninos, *Member, IEEE*, Spyros Fengos, and Nikolaos Lazarou

***Abstract*— The challenge for fast and low-cost deployment of ubiquitous personalized e-Health services has prompted us to propose a new framework architecture for such services. We have studied the operational features and the environment of e-Health services and we led to a framework structure that extends the ETSI/Parlay architecture, which is used for the deployment of standardized services over the next generation IP networks. We expanded the ETSI/Parlay architecture with new service capability features as well as sensor, profiling and security mechanisms. The proposed framework assists the seamless integration, within the e-Health service structure, of diverse facilities provided by both the underlying communication and computing infrastructure as well as the patient's bio and context sensor networks. Finally, we demonstrate the deployment of a tele-monitoring service in smart home environment based on the proposed framework architecture.**

***Index Terms*—ETSI/Parlay architecture, personalized healthcare services, profiling mechanisms, sensor networks mechanisms, security mechanisms.**

I. Introduction

BY its nature, e-Health domain is a multidisciplinary area that is strongly influenced by many different scientific and technology fields. In last decade, many of the key visions of the medical world have taken shape thanks to advances in Information and Communications Technology (ICT). The provision of healthcare services everywhere and at any time, known as ubiquitous healthcare, is becoming a reality, as the ICT concepts of personalized services, service mobility and context awareness have been adopted by the modern medical practice [1], [2]. In many cases, the establishment of ubiquitous healthcare meets the rising demand for personalized healthcare services with low costs and patient's efficient monitoring.

In fact, ubiquitous healthcare has shifted the conventional healthcare provision paradigm to a new one, hereafter referred as Next Generation e-Health (NGeH) paradigm. NGeH emphasizes on the individual's disease prevention, proactive actions, life quality improvement and, under concrete circumstances, on-spot (out-hospital) provision of emergency assistance by delivering personalized healthcare services at the right time, right place and right manner without limitations on time and location [3]. NGeH paradigm encourages individuals to have a normal life regardless of any health problem. For this reason, it encompasses innovative medical practices that are concordant with the real individual's needs, habits, preferences, perspectives, living conditions, or any peculiarity, as they are depicted in individual's profile.

Moving towards such medical practices, it is obvious that conventional frameworks for healthcare provision are not able to support efficiently the whole perspectives of ubiquitous healthcare in NGeH paradigm. Essentially, conventional e-Health framework is a replica of the consolidated healthcare provision framework of the hospitals. It focuses on the creation and delivering of e-Health services applicable within the bounds of the medical units. E-Health framework considers, firstly, that "physician" is the core entity (actor) of the e-Health domain and, secondly, the e-Health services underpin physician to access any medical information and means that could assist him to face the medical situation of the "in-hospital patients". E-Health framework ensures fast and secure access to the patient's electronic Medical Health Record (eMHR) regardless of the physician's location and the technical specifications of the underlay ICT facilities [4].

Instead, the NGeH paradigm considers that the "patient/individual" is the core entity of the e-Health domain. The notion "patient" refers to any individual (elderly, disable, cardiac, etc) that needs temporarily or continuous assistance by other persons, such as physicians, nurses, volunteers, relatives, etc. Hence, according to the NGeH paradigm, an open healthcare domain allowing the seamless

Maria-Anna Fengou is with Wire Communications Laboratory, Electrical & Computer Engineering Department, University of Patras, Rio, Patras, GR-26504, Greece (phone:0030-2610996852; e-mail: afengoum@upatras.gr).

Georgios Mantas is with Wire Communications Laboratory, Electrical & Computer Engineering Department, University of Patras, Rio, Patras, GR-26504, Greece (e-mail: gman@upatras.gr).

Dimitrios Lymberopoulos is with Wire Communications Laboratory, Electrical & Computer Engineering Department, University of Patras, Rio, Patras, GR-26504, Greece (e-mail: dlympero@upatras.gr).

Nikos Komninos is with Wire Communications Laboratory, Electrical & Computer Engineering Department, University of Patras, Rio, Patras, GR-26504, Greece (e-mail: nkom@ieee.org).

Spyros L. Fengos is with the Department of Cardiology, General Hospital "Agia Olga" in Athens, Greece (e-mail: sfengos@gmail.com).

Nikolaos G. Lazarou is with the Department of Emergency Medicine, Rion University Hospital, Greece (e-mail: lazarou.nikolaos@gmail.com).

incorporation of diverse healthcare service components has to be established. For each patient, the combination of the appropriate service components is the formula for the creation of his personalized healthcare service.

In this paper, in the context of NGeH paradigm, we propose a framework architecture for reliable, rapid and cost-efficient deployment of NGeH services over IP-based networks. The proposed framework architecture is based on the ETSI/Parlay architecture used for the deployment of standardized services over next generation IP networks. Particularly, the proposed framework architecture extends the ETSI/Parlay architecture with new service capability features as well as sensor, profiling and security mechanisms in order the complexity and special features (i.e. personalization, context-awareness, security) of these services to be supported. The proposed framework architecture is suggested to be based on the ETSI/Parlay architecture since it allows the interworking between third party client applications and telecommunications capabilities through open and standardized interfaces.

Following the introduction, this paper is organized as follows. In Section II, we give an overview of the NGeH background based on which the ETSI/Parlay architecture is extended leading to the proposed framework architecture. In Section III, we depict the fundamentals of the ETSI/Parlay architecture and its implementation in healthcare domain. In Section IV, we describe the structure of the proposed NGeH framework while in Sections V, VI and VII, its sensor networks mechanisms, profiling mechanisms and security mechanisms, respectively. In Section VIII, we demonstrate how an e-Health tele-monitoring system is constructed in accordance with the NGeH framework and how it is deployed in a Smart Home environment. In Section IX, we discuss about the philosophy and the benefits of the proposed framework. Finally, Section X concludes the paper.

II. The NGeH Background

This Section is focused on the abstract formulation of the NGeH domain. We consider NGeH domain as an operational domain of well defined states and transactions. In this domain the patient interacts with various entities (e.g. doctors, nurses, pharmacists, family members), whose behavior is posed by constructed profiles.

A. The NGeH entities

The NGeH concept distinguishes three types of peer entities that interact each other; subjects, objects and operational domains.

Subjects are all those individuals that are deployed around the patient. They consist of healthcare professionals and aid persons (family members, relatives, friends, volunteers, etc.). At every time and according to the patient's current healthcare condition, a subject's group is self-organized in order to provide sustainable NGeH services to the patient. In this group, every subject manages information and provides service components that are related to their role in the NGeH service. In Section VI, we describe the way these service components are integrated within NGeH services.

Objects are ICT components that are deployed around the patient/subjects. They comprise the monitoring infrastructure of the patient and may consist of bio-sensors, context-aware sensors, GPS, mobile terminals, etc. They yield also the complementary real time information required for the provision of ubiquitous NGeH services.

Finally, the operational domains refer to the places, where the NGeH services are provided, such as hospitals, healthcare units, pharmacies, homes, vehicles, etc.

B. The NGeH domain

We define the NGeH domain as a multi-state, event-driven and multi-operational domain allowing the interaction of the above entities, based upon a set of roles, priorities and capabilities. We consider that the events are related to the patient's health condition described by specific predefined states. At any time, the patient's healthcare condition is set in only one state, in which a concrete NGeH service is provided to the patient by certain types of subjects.

The transition from one state to another is triggered by certain events. Each transition is an event-driven operation. An event can be defined as a significant change in specific bio or contextual information, which is either captured by the objects or imported by the patient himself. The significance of a change is judged through the evaluation of the collected information.

C. The entities profiling model

In NGeH domain, the unified management of bio and contextual information is essential. The eMHR is still the core NGeH tool to organize the implementation and support procedures of NGeH services containing patient's personal information (e.g. name, gender), health history, etc.

Moreover, for each involved entity (mainly for the subjects and the patient) a profile is required. This profile contains detailed information related with the manner the entity participates in the NGeH application and its required actions during the occurrence of any event that is related to the patient's health condition. Especially for the subject's participation, the profile contains information about his/her identification, behavior rules, context, living conditions, time scheduling, educational status and personal requirements, preferences, etc. [5]. The above profile structure, allows the NGeH system to compose multiparty group-working schemes with pre-selected behaviors of all involved entities.

III. ETSI/Parlay in e-Health Domain

A. ETSI/Parlay Fundamentals

European Telecommunications Standards Institute (ETSI), 3rd Generation Partnership Project (3GPP) and

Parlay Group have collaborated and defined jointly the Joint Working Group (JWG) in the context of Open Service Access (OSA). JWG is responsible to further develop and maintain the OSA/Parlay specifications [6]. These specifications enable third party client applications to access transparently the core network functionality and make use of it through a set of open, standardized and technology-independent interfaces, which comprise the Application Programming Interface (API) of OSA/Parlay. This API is called OSA/Parlay API and is essentially the API for the OSA.

The OSA/Parlay specifications were published by ETSI, 3GPP and Parlay Group. However, the Parlay Group was ended around 2007. Thus, today the OSA/Parlay specifications are published only by ETSI and 3GPP. In this paper, we are focused on the corresponding specifications of ETSI resulting in calling them as ETSI/Parlay specifications.

In the context of the ETSI/Parlay, the functionality of the underlying network, which is provided to the client applications, is defined by a set of Service Capability Features (SCFs). The SCFs are considered as abstractions of the network functionalities determined by interfaces, called Service Capability Features Interfaces (SCFs Interfaces).

According to the ETSI/Parlay specifications [7], the ETSI/Parlay API consists of two main sets of interfaces. The first one includes the SCFs Interfaces and the second one contains the Framework Interfaces. Both sets of these interfaces reside in the Service Capability Servers (SCSs) located in the ETSI/Parlay Gateway. The SCFs Interfaces allow any client application to access transparently the network capabilities. The Framework Interfaces provide client applications with the basic mechanisms to discover and use the required network capabilities.

Furthermore, the ETSI/Parlay specifications define an architecture consisting of the following main components: the Client Applications, the Service Capability Servers, the Framework, the Enterprise Operator and the Network Capabilities (i.e. IP-based Network Capabilities). The ETSI/Parlay architecture [7] is shown in Fig. 1.

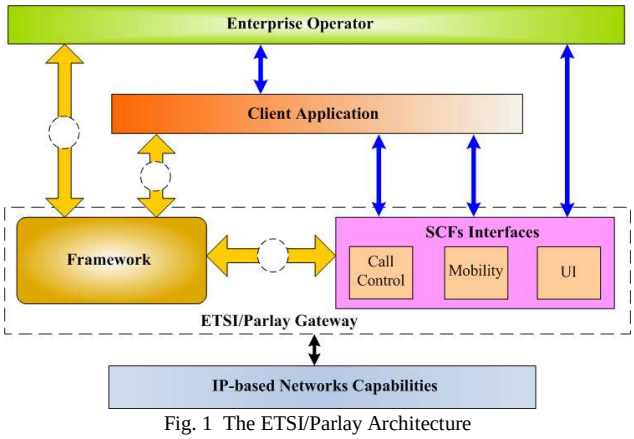

Fig. 1 The ETSI/Parlay Architecture

The Client Applications are deployed on Application Servers and make use of the network capabilities defined into the specifications and provided through the API. The Client Applications represent the client side of API.

The SCSs provide the Client Applications with SCFs through the corresponding SCFs Interfaces. The SCSs are the logical entities implementing the classes of these interfaces. Moreover, the SCSs represent the server side of the API. The communication between a SCS and a Client Application is achieved by standard IT middlewares such as CORBA.

The Framework is located between the Client Applications and the SCS. The Framework incorporates interfaces providing Client Applications with mechanisms which are responsible for enabling Client Applications to discover and use the core network service capabilities. Moreover, the Framework includes interfaces for management mechanisms which are responsible for handling fault and overload situations. Besides, the Framework includes interfaces for mechanisms enabling network operators to authenticate third party Client Applications.

Especially, the Framework incorporates interfaces between the Application Server and the Framework, between the SCS and the Framework, and between the Enterprise Operator and the Framework. These interfaces are represented by the dashed circles in Fig. 1. Thus, the Framework includes the following three distinct sets of interfaces:

- Framework to Application interfaces providing the mechanisms for authentication, authorization, discovery of Framework interfaces and SCFs, establishment of service agreement and access to SCFs
- Framework to SCS interfaces providing the basic mechanism for registration of SCFs
- Framework to Enterprise Operator interfaces providing the basic mechanism for service subscription function

B. E-Health Platforms over ETSI/Parlay Architecture: A Survey

Advanced middleware technologies (e.g. ETSI/Parlay, JAIN SLEE) are not widely exploited by the healthcare sector since there are few e-Health platforms developed over such middlewares. Below, we present a survey on e-Health platforms that have been developed over ETSI/Parlay architecture.

EmerLoc [8] is a location-based system for emergency purposes. Emergency incidents are handled in random locations based on a middleware and network infrastructure. EmerLoc incorporates patient-carried equipment comprised of wireless sensors and his/her portable device that continuously monitors the user's biosignals, a micro-computing unit, which is responsible for processing sensor readings and a central monitoring unit (CMU), which transmits the information to the medical personnel. The authors used existing technologies of wireless networks

(Bluetooth, WLAN/802.11, GPRS) and location-based services (Nibble, GPS). They also used middleware and network application standards such as HTTP, ETSI/Parlay, WAP, RMI and Jini in order to assemble an integrated system. For the location-based platform which is operated in the CMU a location server of the mobile operator is used conforming to ETSI/Parlay standards. With the use of such specifications, it is hidden the complexity and heterogeneity of the operator's equipment and it is achieved a uniform, standardized API for Wireless Service Providers intending to perform functions like charging, billing, messaging and location determination.

In [9], it is proposed the design of an emergency service using ETSI/Parlay APIs for the application to access underlying telecommunication network functionality. ETSI/Parlay APIs allow the improved functionality of the emergency service to be offered anywhere, even in areas that have only a very basic telecommunication network as ETSI/Parlay enables the service to use the core network of whichever telecommunication network it will be implemented on.

The two above mentioned e-Health platforms provide mainly location-based services that are based on the basic mechanisms and the SCFs that the ETSI/Parlay architecture contains.

For the deployment of advanced services, such as the NGeH services, it is essential the extension of the standardized ETSI/Parlay architecture in order the complexity and special properties of these services to be supported. The extension of the standardized ETSI/Parlay architecture should integrate APIs and mechanisms that satisfy the requirements for deployment of secure and personalized context-ware healthcare services. It is important to mention that security, personalization and context awareness are the main properties of the NGeH services.

IV. The Proposed NGeH Framework

Based on the standardized ETSI/Parlay architecture, we propose a generic application framework for reliable, rapid and rapid development of NGeH services. The architecture of the proposed framework is depicted in Fig. 2.

The proposed framework extends the two basic components included into the ETSI/Parlay Gateway. It extends the set of the SCFs Interfaces and the set of mechanisms supported by the ETSI/Parlay Framework.

In the context of the proposed framework architecture, the new set of SCFs Interfaces is called as *Extended Set of SCFs Interfaces* and the new Framework is called as *Extended Framework*.

A. Extended Set of SCFs Interfaces

The *Extended Set of SCFs Interfaces* integrates two categories of SCFs Interfaces. The first one includes the standardized *IP-based Network SCFs Interfaces*, which are defined in the ETSI/Parlay specifications. The second category includes the SCFs interfaces that we introduce in this paper in order to extend the set of the ETSI/Parlay SCFs Interfaces and expand the capabilities of ETSI/Parlay standard for deployment of NGeH services. Especially, the second category involves a number of SCFs Interfaces enabling client applications to access the sensing capabilities provided by sensor networks.

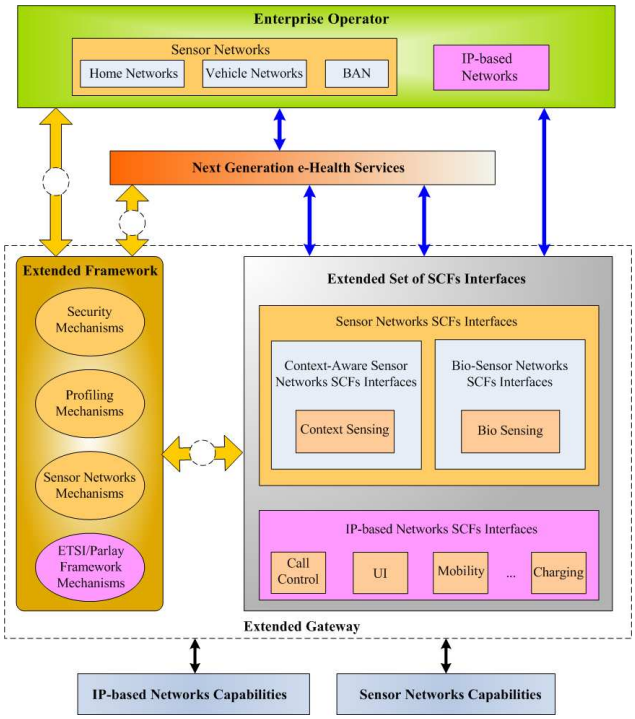

Fig. 2 The Proposed NGeH Framework Architecture

These proposed SCFs Interfaces, called *Sensor Networks SCFs Interfaces*, are classified into the following two subsets based on the type of the information gathered by the corresponding sensor network deployed around the patient: .

- *Context-Aware Sensor Networks SCFs Interfaces* enabling client applications to access the context information sensing capabilities provided by context-aware sensor networks. Context information sensing is the process of collecting context information from the patient's environment. Context information can be collected by many different types of context-aware sensors deployed in different types of networks (e.g. home networks, vehicle networks). These sensors can gather context information ranging from location and time to low-level types of physical context such as temperature, humidity and the concentration of gases (e.g. carbon dioxide). Furthermore, context information sensing can provide information related to patient's activities.
- *Bio-Sensor Networks SCFs Interfaces* enabling client applications to access the biosignals sensing capabilities provided by bio-sensor networks. Biosignals sensing is the process of data acquisition of various vital parameters (e.g. ECG signals, blood

pressure) derived from the patient's body. In the NGeH domain, biosignals are gathered by bio-sensors deployed in the Body Area Network (BANs) located on the patient's body.

The *IP-based Networks SCFs Interfaces* reside in *ETSI/Parlay SCSs* and the *Sensor Networks SCFs Interfaces* reside in *Sensor Networks SCSs*. Both *ETSI/Parlay SCSs* and *Sensor Networks SCSs* are located in the *Extended Gateway*.

Finally, it is worthwhile to mention that the supported capabilities (i.e. IP-based Network capabilities, context sensing capabilities and bio sensing capabilities) by the *Extended Set of SCFs Interfaces* are considered as service components. In the world of service standards, these service components, called service enablers, can be bundled to create independent and reusable niche services targeted at specific markets, such as NGeH applications. Thus, the proposed framework as an extension of the standard ETSI/Parlay architecture [10]:

- Creates a development environment allowing the proliferation of niche services rather than finding the next killer NGeH application.
- Leads to shorter development cycles and decrease the efforts for NGeH application's development.
- Generates considerable revenue to the developers and providers, mainly through economies of scale.

B. Extended Framework

The *Extended Framework* supports four sets of mechanisms in order to enable the ease deployment of NGeH services by third party developers. The first set includes the basic mechanisms of the ETSI/Parlay Framework. The other three sets incorporate mechanisms, through interfaces, that we propose in order the proposed framework to allow third party developers to deploy secure, personalized and context-aware healthcare services. Furthermore, the second set incorporates the proposed *Sensor Networks Mechanisms*. The third set includes the proposed *Profiling Mechanisms* and the fourth set includes the proposed *Security* Mechanisms. The *Extended Framework* is included in the *Extended Gateway* as it is shown in Fig. 2.

V. The Proposed Sensor Networks Mechanisms

The proposed *Sensor Networks Mechanisms* are responsible for the management of the information captured by context-aware sensors and bio-sensor as well as the deployment of context-aware healthcare services. These mechanisms are derived from three well-known context-aware frameworks supporting mechanisms for deployment of context-aware applications. These frameworks are the following: the Context Management Framework (CMF) [11, 12], the Java Context-Awareness Framework (JCAF) [11, 13] and the Context Toolkit [11, 14]. Even though these mechanisms are derived from frameworks processing and managing contextual information, the concept of these mechanisms can also be applied properly on bio information. The proposed *Sensor Networks Mechanisms* supported between the Extended Framework and the Client Application are described below.

- *Context and Bio Information Abstraction*: This mechanism is used for context and bio information interpretation, since NGeH services make use of many different types of sensors to perceive contextual and bio information. The main objective of this mechanism is to hide the heterogeneity of the gathered information providing a higher level of abstraction. Consequently, this mechanism increases the independency of services from the sensors, as well as the reusability of the sensors.
- *Context and Bio Information Storage and Management*: This mechanism is responsible for the storage of contextual and bio information, as well as for the management (e.g. retrieval, search) of the stored information. Additionally, it is responsible for the delivery of the stored information using different types of approaches (e.g. request/response, subscription/notification). Besides, this mechanism is essential for NGeH services that require sensored vital and contextual data to be combined.
- *Reasoning*: In NGeH services the captured information is often unreliable due to the inaccuracy and lack of precision of sensors. Consequently, a reasoning mechanism is essential to address uncertainty of sensors' measurements making deductions for suitable adaptations without an explicit intervention from the user.
- *Devices and Resource Discovery*: This mechanism is responsible to enable devices (e.g. bio-sensors) to be added or removed dynamically from the sensor networks without affecting the entire operation of the sensor networks.
- *Services Discovery*: This mechanism is responsible to inform NGeH services about the available supported services based on their requirements.

In addition to the above mentioned mechanisms, the *Extended Framework* supports the registration mechanism of Sensor Networks SCFs. This mechanism is supported between the *Extended Framework* and the SCSs including the corresponding SCFs [10].

VI. The Proposed Profiling Mechanisms

In the context of the proposed framework, we have defined specific NGeH profiles since they are the main means for deploying personalized NGeH services. In addition to NGeH profiles, we have defined a number of profiling mechanisms for materializing the functionality of the NGeH profiles [15], [16], [17].

A. Profile Functionality

The NGeH framework allows the use of NGeH profiles considered as components for the deployment of personalized delivery of services.

The patient and each subject that participate in NGeH services (e.g. doctor, patient's relative etc.) have their individual profile. The individual profile of the patient contains index to a group profile that is triggered whenever an event is detected. This profile's structure allows NGeH systems to compose multiparty group-working schemes with pre-selected behaviors of all involved subjects. In the group profile, each subject has a specific role with defined activities. The group is formed through certain management, scheduling and notification events [17]. The intention of each subject to participate or not is detected by his current individual profile and is signaled by a notification event [18].

B. Definition of NGeH Profile Classes

The profiles are categorized into five classes:

- Patient's Profile: It contains information about [19]:
  - Context information divided into environmental context information and medical context information. The environmental context information consists of the physical context information (i.e. environmental conditions), the temporal context information (e.g. time, day) and the spatial context information (e.g. location). The medical context information consists of two groups of parameters. The first one is acquired by biosensors that depict the physiological state (e.g. blood pressure, ECG). The second one is self-estimated data explicitly imported by the patient as a subjective estimation of his health condition (e.g. pectoral pain, dyspnea).
  - Healthcare group that treats the patient and consults him and his authorized aid persons.
- Healthcare Professional's Profile. It contains information about [19]:
  - Terminal Capabilities of the different types of terminals (PDA, PC, etc) assuring the user's mobility, uninterrupted network access, and personalized operational settings.
  - Preferences (e.g. the availability). These are choices defined by the user. Complex preferences are expressed in the form of rules that can be used for either defining profile activation criteria or filtering criteria.
- Aid Person's Individual Profile: It contains information about:
  - Terminal capabilities and Preferences, similar to healthcare professional's profile, as well as individualized information concerning his/her participating roles and capabilities in patient's healthcare process.
- Operational Domain's Profile. It contains information about [19]:
  - Identification Information (e.g. name, address)
  - Critical conditions that can be handled (e.g. cardiac arrest, heart attack)
  - Available equipment and facilities
  - Schedule of the on duty hospital.
- Group Profile [17]:
  - The event-driven NGeH model requires the real time collaboration of many subjects as a group for the provision of personalized services to the patient. Thus, the NGeH framework supports the dynamic creation of group profile describing the behavior and roles of all the participating entities in the group for the provision of NGeH services to the patient.

C. Profiling Mechanisms

The NGeH framework provides Profiling Mechanisms that are considered by the developer as simple components that can be integrated to implement personalized delivery of NGeH services. These mechanisms deal with the context information management, as well as the individual and group profile management [17], [20], [21], [22]. Thus, the deployed Profiling Mechanisms are based on the gathered context information, on the presence of organized and structured profiles, and the assignment of roles for the creation of group profiles. Different Profiling Mechanisms are activated according to subject's profile, which changes, as subject's current context changes.

The Profiling Mechanisms supported between the Extended FI and the NGeH Application are described below.

- *Aggregation*: Gathering all the context data from the context providers and processing them. The patient's environmental and medical context, which represents the context information, is collected from multiple context sources (by "context watchers").
- *Reasoning*: Interpreting the sensor-readings in order to capture the high level context. High-level context information is considered, for instance, the current activity of the user. This mechanism uses semantic information defined by an ontology context model or inference rules to form the high level context.
- *Adaptation*: Obtaining the reasoned high level context and combining it with the relevant content of the profile. For that reason, this mechanism compares the context data of the reasoned context with the patient's profile data, applying, for instance, semantic matching. Then, the active context and the actions that should be done are defined. The identified context is exploited by the "Event Handler".
- *Event Handler*: Detecting and handling the events that trigger the creation of the group profile. These events are related to the patient's health condition. These events denote that the patient needs a medical

advice or attention and care due to aggravation of his health condition [17].

- *Individual Profile Creation*: Creation of the individual's profile. Every individual (patient or subject) is considered to have his profile and is added to the system as user. The profile is initially created by fundamental data that then are completed from supplementary sources. Supplementary data of a subject's personal information are used to build the enriched profile of each individual.
- *Individual Profile Update*: Update of the individual profile. Since the individual profile is established, it is continually maintained either manually or automatically with the usage of monitoring components, which enable its update. Moreover, this mechanism supports services and applications to automatically suggest updates to the profile.
- *Role Assignment*: Assigning roles to the actors of the group in order to attain the creation of the group profile. When the event is triggered by the event handler, this mechanism detects the roles that are required and invites them in order to build the group. Each role has its competences as when a session is convened. The patient (i.e. his health condition) and the formed group of eligible subjects correspond to the convene scheme and the participants of the session respectively [17].
- *Group Profile Creation*: Creation of the group profile. The activation of this mechanism is event-driven. When an event is triggered by the event handler, the group profile is created based on the indexes that are stored in the patient's profile. The roles of the group that will be convened are specific. Each role has certain attributes that determine the subjects that meet the conditions in order to participate [17].
- *Group Profile Update*: Update of the group profile. After the creation of the group profile, its dynamic update is considered essential. The attributes of each participant change dynamically over time. Thus, the participants' presence is constantly detected and verified. Moreover, after the activation of group profile, collaboration events may follow such as decision-support events and resource-sharing events depending on the patient's health condition [17].

VII. The Proposed Security Mechanisms

The NGeH framework provides developers with Security Mechanisms for NGeH services. The integration of Security Mechanisms is essential in NGeH services, since these services incorporate extremely sensitive information derived from vital, contextual data as well as profile data. The NGeH framework aims to provide third party developers with Security Mechanisms for NGeH services operating over different types of networks (e.g. sensor networks, IP-based networks). Thus, third party developers are able to properly select those mechanisms that fit well into the provided NGeH services requirements.

The provided Security Mechanisms are considered by the developer as simple components that can be integrated to implement security with multiple lines of defense against both known and unknown security threats. Thus, the deployed Security Mechanisms work well not only in the presence of designated attacks but also under new attacks. The integrated Security Mechanisms are able to address not only malicious attacks but also other network faults arising due to misconfiguration, extreme sensor network overload, or operational failures [23].

The *Extended Framework* intends to integrate a wide spectrum of Security Mechanism to ensure data confidentiality, data integrity, authentication, authorization and non-repudiation. For example, the *Extended Framework* is able to support the Security Mechanisms designed by the authors in [24] and [25].

The "*efficient security mechanism*" proposed in [24], provides authentication and data integrity for the communication among the sensors and the base station of a sensor network. It exploits a low-weight hash function, which is used in combination with a key to produce Message Authentication Codes (MACs), in a group communication model to prevent unauthorized data disclosure, and to ensure that data have not been modified during transmission.

The "*data integrity mechanism*" proposed in [25] can be used by the developer to achieve data integrity in the case of deployment a NGeH tele-monitoring system that operates in a smart home and supports transmission of medical data from the smart home to the healthcare center. In this mechanism, agent technology is proposed to ensure data integrity making use of MACs and cryptographic smart cards connected to the Residential Gateway of the smart home and the PC of the subject. Each smart card stores a pair of secret keys. The one is for encryption/decryption processes executed on the smart card and the other for computing MACs on the smart card. Finally, for computing MACs on sensors and the Body Gateway, each of them uses a secret key, which is the XOR result of its MAC-address and a secret pre-shared key.

VIII. Deployment of an e-Health Tele-monitoring Service in Smart Home Environment Based on the Proposed Framework

In this section, we describe how the proposed framework can be exploited for the deployment of an e-Health tele-monitoring service in smart home environment. This service aims to ensure efficient and high quality care of the patient independent of time, activities and local resources. For this purpose, we consider that the tele-monitoring service is composed of the following service components:

- Continuous bio-sensing for persistent assessment of patient's health situation. This service component acquires real bio information from patient's body and assesses the patient's health condition changes.
- Continuous context-sensing for persistent assessment of patient's living conditions and activities. This service component acquires real context information from patient's living environment and assesses changes on the patient's behavior.
- Dynamic creation of the appropriate group of eligible subjects (e.g. doctor, nurse, relative) to face concrete patient's abnormal situations. This functionality is performed through two successive service components. The first one selects the available eligible subjects using data from patient's profile. The second one sets the telecommunications environment for the group working of the selected subjects.
- Provision of feedback information (e.g. alarm messages) to the eligible subjects related to the patient.

A. E-Health Tele-Monitoring System Architecture

The e-Health tele-monitoring system consists of the following components:

- Smart Home
- Extended Gateway
- Application Server
- Healthcare Center

Smart Home incorporates a heterogeneous network infrastructure including a Body Area Network (BAN), a Wireless Personal Area Network (WPAN) and a Wireless Local Area Network (WLAN). The architecture of the e-Health tele-monitoring system is shown in the Fig. 3.

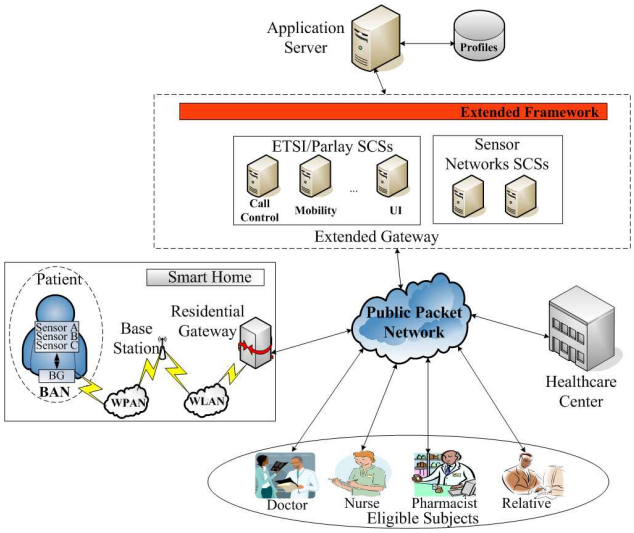

Fig. 3 Architecture of the e-Health Tele-monitoring System

The BAN includes a number of wearable sensors collecting both the essential vital parameters from the patient's body and the appropriate context information from the patient's environment. The BAN integrates also a wearable unit, called Body Gateway (BG), which gathers all the sensing data derived from the wearable sensors and transmits them to the Base Station wirelessly via the WPAN. In other words, the BG plays the role of the bridge between the BAN and the WPAN. Additionally, the WLAN is responsible to connect the Base Station to the Residential Gateway (RG). The RG which is located in the Smart Home, integrates all the different networking technologies used in the internal network of the Smart Home and allows access from the internal network to the Public Packet Network and vice versa. The Public Packet Network infrastructure is used for transferring the sensing data from the RG to the Healthcare Center as well as supporting healthcare delivery from healthcare provider to the patient and provision of feedback information to the eligible subjects.

The *Extended Gateway* integrates *ETSI/Parlay SCSs* and *Sensor Networks SCSs* providing developers of the e-health tele-monitoring service with the appropriate *IP-based Networks SCFs Interfaces* and *Sensor Networks SCFs Interfaces* respectively. In addition to the SCSs, the *Extended Gateway* incorporates the *Extended Framework* providing developers of the e-health tele-monitoring services with:

- the basic mechanisms of the standardized ETSI/Parlay Framework,
- the proposed *Sensor Networks Mechanisms*,
- the proposed *Profiling Mechanisms* and
- the proposed *Security Mechanisms*.

The *Extended Gateway* is essential in order to deploy the tele-monitoring service in a secure, personalized and context-aware manner.

The e-health tele-monitoring service is deployed on the *Application Server*, as it is shown in Fig 3. The *Application Server* is connected with a database, called *Profile Database*, storing patient's profiles and eligible subjects' profiles since profiles are the basic components for achieving personalization. The functionality of the profiles is materialized through the proposed *Profiling Mechanisms*.

B. Achieving Context-Awareness

To achieve context-aware service the e-health tele-monitoring system makes use of the proposed Sensor Mechanisms. Based on many modern context-aware systems, the required functionalities for achieving context-awareness are the following [11], [14]:

- *Modeling of raw bio and context data gathered from wearable sensors*: Creates dynamically abstractions modeling the gathered data. The raw sensory data are modeled in order to be unambiguously interpreted by services and system components. This functionality is implemented by the proposed *Context and Bio Information Abstraction* mechanism.
- *Reasoning of the modeled information*: Increases the abstraction level of the modeled information of the previous functionality. This functionality is implemented by the proposed *Reasoning* mechanism.

- *Storage and management*: Organize, store, manage and deliver the gathered bio and contextual information. The functionality is implemented by the proposed *Context and Bio Information Storage and Management* mechanism.
- *Orchestration and coordination of the previous functionalities*: Provide integrated services to the subjects of the system and enhance the quality of the integrated services. This functionality is implemented by the proposed *Devices and Resource Discovery* mechanism and the *Services Discovery* mechanism.

C. Achieving Personalization

To achieve personalized services, the e-Health tele-monitoring system creates dynamically a group of eligible subjects to face patient's abnormal situations. For the creation of this group the following Profiling Mechanisms are involved [17].

Initially, the *Event Handler* mechanism detects any event that is related to the change of the patient's health condition. When such an event is detected, the *Role Assignment* mechanism is activated in order to define the roles that are essential to be assigned for the current patient's health condition.

Then, the *Group Profile Creation* mechanism assigns the appropriate subject to each role that should participate creating a group of eligible subjects. This mechanism is based on the inputs of the *Event Handler* mechanism and *Role Assignment* mechanism and its access to the profiles of all involved actors in the group (patient and the potential eligible subjects).

After the group is created, the *Group Profile Update* mechanism may update the group during the e-Health service provision. The update may be necessary in two cases: a) if the patient's current health condition is changed requiring the participation of different roles in the group or b) if an eligible subject needs to be replaced by another subject of the same role because he is not available anymore. Thus, for the realization of a potential update, the *Group Profile Update* is based on the inputs from the *Event Handler* mechanism, *Role Assignment* mechanism, *Group Profile Creation* mechanism and the access to the profiles of all the involved actors in the group (patient and eligible subjects) as well as the profiles of the potential subjects.

D. Achieving Security

To achieve security in the e-Health tele-monitoring service a number of Security Mechanisms should be integrated in a multilayer approach. For example, we propose the integration of the two Security Mechanisms that we mentioned in Section VII.

The mechanism proposed in [24] is suitable for providing authentication and data integrity in the BAN consisting of a bio-sensors network. Furthermore, the mechanism proposed in [25] is appropriate for achieving data integrity during the transmission of bio information from the Smart Home to the Healthcare Center.

E. Dependencies of the Extended Framework Mechanisms

There are dependencies between the proposed mechanisms that are integrated in the Extended Framework when a subset or all of them are used for the deployment of the e-Health tele-monitoring service.

We used the Protégé ontology editor and knowledge-acquisition system [26] for the representation of the proposed mechanisms integrated in the Extended Framework and their potential dependencies. The ontology consists of four main concepts (i.e. classes) corresponding to the integrated mechanisms; ETSI/Parlay Framework, Sensor Networks, Profiling and Security mechanisms. In Fig. 4, there are depicted these dependencies named as template slots for the proposed mechanisms.

Mechanisms		Template Slot	
Class		Name	Type: Domain and Allowed Superclasses
Profiling Mechanisms	**Event Handler**	supports:6	Group profile creation
	Pofiling Reasoning	supports:5	Adaptation
	Role Assignment	supports:7	Group profile creation
Sensor Networks Mechanisms	**Context and Bio Information Storage and Management**	supports:1	Confidentiality, Data Integrity, Aggregation, Individual Profile Creation, Individual Profile Update
	Devices and Resource Discovery	supports:2	Sensor Network Authentication, Availability
	Reasoning	supports:4	Context and Bio Information Abstraction
	Services Discovery	supports:3	Availability

Fig. 4 The Template Slots/Dependencies for the Proposed Mechanisms

In Fig. 5, it is depicted the ontology-based representation of the Profiling Mechanisms and Sensor Networks Mechanisms as well as their dependencies. The arrows, named as "supports:i" for i=1,..,7, indicate the template slots that exist between these mechanisms. For instance, the slot "supports: 1" indicates the dependency of the *Aggregation* mechanism, *Individual Profile Creation* mechanism and *Individual Profile Update* mechanism with the *Context and Bio Information Storage and Management* mechanism. The slot "supports: 6" indicates the dependency of the *Group Profile Creation* mechanism with the *Role Assignment* mechanism. Similarly, the slots "supports:4", "supports:5", "supports:7", that are depicted in Fig. 5, are explained.

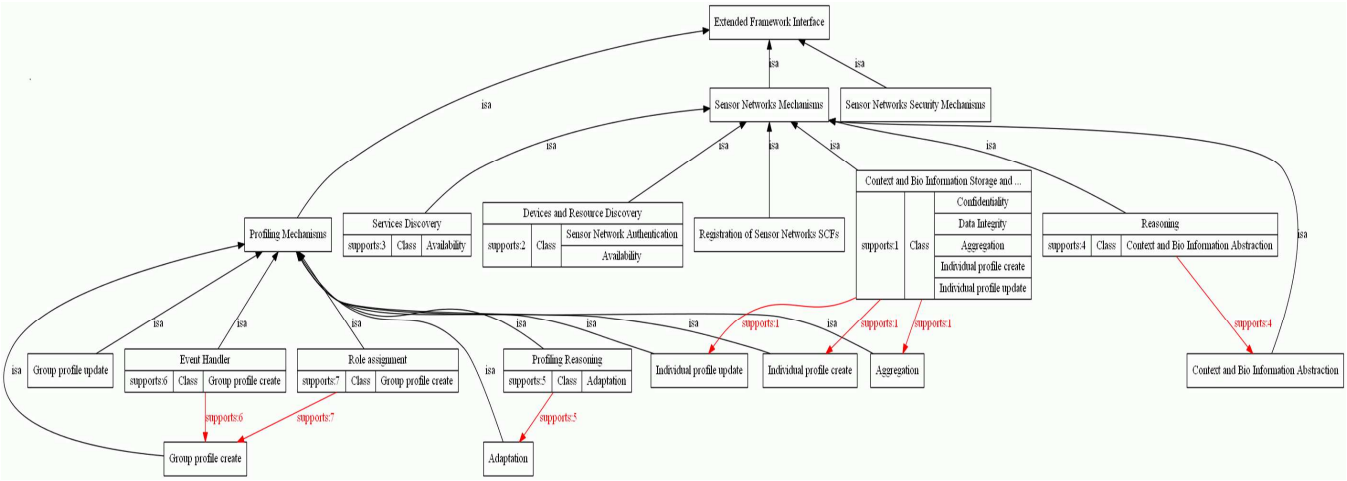

Fig. 5. An Ontology-based Representation of the Profiling Mechanisms and the Sensor Networks Mechanisms

IX. Evaluation - Discussion

In the context of service deployment, ETSI/Parlay standard has enabled the replacement of silo services with services that are constructed by "small" independent service components. So far, ETSI/Parlay has been successfully used for the deployment of telecommunication services, which work either independently or are integrated into other services offered by third party providers.

In Section III, there are provided two examples of telecommunication structured services applied in the e-Health domain. Both examples are mainly location-based systems for emergency purposes. These systems are implemented on the ETSI/Parlay architecture exploiting the provided standardized ETSI/Parlay API.

Based on these implementations, this paper goes one step further and attempts to convey the overall philosophy of the ETSI/Parlay standard in the deployment of e-Health services. In other words, it considers that e-Health services should be built by reusable service components. The deployment of services based on reusable service components leads to the rapid and cost-efficient deployment of e-Health services. Consequently, the interest is shifted from the deployment of silo healthcare services, as it is currently done, to healthcare services built by service components.

This paper not only focuses on the obvious advantages of ETSI/Parlay standard in building e-Health services, but also presents a framework architecture for designing and implementing e-Health services. The service described in Section VIII shows in a clear way how a developer can convert individualized medical practices to operationally efficient e-Health services based on the proposed framework.

The actual evaluation of the proposed framework architecture is possible only through an extensive process of planning and promotion of commercial applications and services from established third party providers. However, it may be noted that only positive results can be expected from the use of such framework in the field of e-Health.

X. Conclusion

In this paper, we propose a new NGeH framework architecture as an extension of the standard ETSI/Parlay architecture. The proposed framework architecture integrates sensor networks mechanisms, profiling mechanisms and security mechanisms with mechanisms that allow the ease exploitation of the core networks' capabilities in order reliable NGeH services to be built. Essentially, the proposed NGeH framework architecture provides third-party developers with the appropriate mechanisms for deployment of such NGeH services. Furthermore, a deployment of an e-Health tele-monitoring service in Smart Home environment is described as an application of the proposed framework architecture. Finally, the benefits of the proposed NGeH framework are discussed.

References

[1] Y. Lee and JL. Lin, "Do patient autonomy preferences matter? Linking patient-centered care to Patient-physician relationships and health outcomes," Social Science & Medicine, Elsevier, vol. 71, no 10, pp. 1811-1818, 2010.

[2] I. Holmström and M. Röing, "The relation between patient-centeredness and patient empowerment: A discussion on concepts," Patient Education and Counseling, Elsevier, vol. 79, no 2, pp. 167-172, 2010.

[3] U. Varshney, "Pervasive Healthcare: Applications, Challenges And Wireless Solutions," Communications of the Association for Information Systems, AIS Electronic Library, vol. 16, no. 1, article 3, pp. 57-72, 2005.

[4] J. Jin, G.-J. Ahn, H. Hu, M. Covington, and X. Zhang, "Patient-centric authorization framework for sharing electronic health records," in Proc. 14th ACM Symposium on Access Control Models and Technologies, Italy, 2009, pp. 125-134.

[5] Draft ETSI ES 202 642 V0.0.28, "Human factors (HF), eHealth; personalization of eHealth systems," 2010.

[6] A.-J. Moerdijk and L. Klostermann, "Opening the networks with parlay/osa: standards and aspects behind the apis," IEEE Network, vol. 17, pp. 58-64, June 2003.

[7] ETSI ES 203 915-3 V1.2.1, "Open Service Access (OSA); Application Programming Interface (API); Part 3: Framework (Parlay 5)," Jan. 2007.

[8] I. Maglogiannis, S. Hadjiefthymiades, "EmerLoc: Location-based services for emergency medical incidents", International Journal of Medical Informatics, Elsevier, vol. 76, no 10, pp. 747-759, 2007.

[9] G. Khayltash and H. Hanrahan, "Emergency Services: The Way Forward," in: Proc. SATNAC: next generation services, 2006, pp. 1-6.
[10] G. Mantas, D. Lymberopoulos, and N. Komninos, "A new framework for ubiquitous context-aware healthcare applications," in Proc. 10th IEEE International Conference on Information Technology and Applications in Biomedicine, Corfu, Greece, 2010.
[11] M. Miraoui, C. Tadj, and C. Ben Amar, "Architectural survey of context-aware systems in pervasive computing environment," *Ubiquitous Computing and Communication J.*, vol. 3, no. 3, 2008.
[12] P. Korpipaa et al., "Managing context information in mobile devices," *IEEE Pervasive Computing*, vol. 2, no. 3, pp. 42-51, Sept. 2003.
[13] J. E. Bardram, "The Java Context Awareness Framework (JCAF) – a service infrastructure and programming framework for context-aware applications," in *Pervasive Computing*, vol. 3468, H. W. Gellersen, R. Want, and A. Schmidt, Eds. Berlin, Germany: Springer-Verlag, 2005, pp. 98-115.
[14] M. Baldauf, S. Dustdar, and F. Rosenberg, "A survey on context-aware systems," *Int. J. of Ad Hoc and Ubiquitous Computing*, vol. 2, no. 4, pp. 263-277, 2007.
[15] ETSI TS 102 747 V0.0.32, "Human Factors (HF); Personalization and User Profile Management; Architectural Framework," 2009.
[16] ETSI ES 202 746 V0.0.16, "Human Factors (HF); Personalization and User Profile Management; User Profile Preferences and Information," 2010.
[17] M.-A. Fengou, G. Mantas, D. Lymberopoulos, "Group Profile Management in Ubiquitous Healthcare Environment", EMBC, 2012, accepted to be published.
[18] R. Etter, P.D. Costa, T. Broens, "A Rule-Based Approach Towards Context-Aware User Notification Services," perser, in *Proc ACS/IEEE International Conference on Pervasive Services*, 2006, pp.281-284.
[19] M.A Fengou, T. Panagiotakopoulos, S Fengos, N. Lazarou and D. Lymberopoulos, "A new telemedicine framework handling the emergency room overload," in *Proc. 10th IEEE International Conference on Information Technology and Applications in Biomedicine*, Corfu, Greece, 2010.
[20] T. Kovacikova, F. Petersen, M. Pluke, G. Bartolomeo, "User Profile Management – Integration with the Universal Communications Identifier Concept," in *Proc 13th WSEAS International Conference on Communications*, Wiskonsin, 2009, pp.117-123.
[21] S.A. Chellouche, J. Arnaud, D. Négru, "Flexible User Profile Management for Context-Aware Ubiquitous Environments," in *7th IEEE conference on Consumer communications and Networking*, Las Vegas, 2010, pp. 980-984.
[22] M. Sutterer, O. Droegehorn, K. David, "User Profile Management on Service Platforms for Ubiquitous Computing Environments," in *65th Vehicular Technology Conference*, Dublin, 2007, pp. 287-291.
[23] N. Komninos, D. Vergados, and C. Douligeris, "Layered security design for mobile ad hoc networks," Computers and Security J., Elsevier, vol. 25, no. 2, pp. 121-130, March 2006.
[24] I. Kolokouris, N. Zarokostas, and N. Komninos, "Integrity and Authenticity Mechanisms in Sensor Networks," *International Journal on Computer Research*, vol. 15, no. 1, pp. 57-72, 2007.
[25] G. Mantas, D. Lymberopoulos, and N. Komninos, "Integrity Mechanism for eHealth Tele-monitoring System in Smart Home Environment," in *Proc. 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Minneapolis, Minnesota, 2009, pp. 3509-3512.
[26] T. Tudorache, N. Noy, S. Tu, M. Musen, "Supporting Collaborative Ontology Development in Protégé," in *Proc. ISWC '08 Proceedings of the 7th International Conference on The Semantic Web*, 2008, pp. 17-32.

Maria-Anna Fengou received her Diploma in electrical and computer engineering from the University of Patras, Patras, Greece, in 2008.

Since 2008, she has been pursuing her PhD in the Department of Electrical and Computer Engineering at the University of Patras. Her current research areas of interest include user profiles, context-aware computing, social networks applied in healthcare sector, ubiquitous healthcare, next generation networks and telecommunication protocols.

Georgios Mantas (M'07) received his Ph.D in electrical and computer engineering from the University of Patras, Patras, Greece, in 2012, his M.Sc. in information networking from Carnegie Mellon University, Pittsburgh, Pennsylvania, in 2008 and his Diploma in electrical and computer engineering from the University of Patras, Patras, Greece, in 2005.

He is currently a Postdoctoral Researcher at the Department of Electrical and Computer Engineering, University of Patras. His main research areas of interest include network security, applied cryptography, e-health security, medical information systems security, smart cards security, ubiquitous healthcare, next generation networks and sensor networks.

Dimitrios Lymberopoulos (M'95) received his Diploma in electrical engineering and his Ph.D. degree from the University of Patras, Patras, Greece, in 1980 and 1988, respectively.

He is currently a Professor in the Department of Electrical and Computer Engineering, University of Patras, where he lectures on communication systems, multimedia communications, and telemedicine services. Since 1982, he has been involved as a Technical Supervisor in various research projects funded by the Greek Government, the European Union, the Greek Telecommunication Organization, and the major Greek Telecommunication industries. He has authored or co-authored over 180 papers in international journals, conferences and technical reports. His research interests include medical communication protocols, telemedicine, context awareness, ontologies in the medical information domain, next generation networks, web multimedia services, data management in medical applications, teleworking (telemedicine) development platforms and medical communication networks.

Prof. Lymberopoulos is a member of the Technical Chamber of Greece and the Greek Society of Electrical and Mechanical Engineers.

Nikos Komninos (M'00) received his Ph.D in information security and cryptography from Lancaster University, Lancaster (UK), in 2003, his M.Sc. in computer communications and networks from Leeds Metropolitan University, Leeds (UK), in 1999 and his B.Sc in computer science and engineering from the American University of Athens, Athens (GR), in 1998.

He has over fifteen years of R&D experience in the academia and industry working on the evaluation, analysis and development of practical secure communication systems. Some of his work includes design/analysis of authentication, key agreement, intrusion detection and response protocols/mechanisms in ad hoc and cellular networks, transport/network layer security, and e-health security. He has written over 50 peer-review journals and conference publications, patents and books in the information security and cryptography research area. He has been invited as international advisor and technical program committee, guest editor in international conferences and journals and speaker with honors in the field. His main technical interests lie in the areas of information security and cryptography for wireless/telecommunication/ad-hoc networks, e-health applications, cryptographic protocols, smart cards and biometrics.

Spyros Fengos graduated in medicine from Medical School of Athens's University in 1983, Greece. In 1991, he completed his specialist training in cardiology in the Evangelismos Hospital of Athens.

He works in N. Ionia's General Hospital "Agia Olga" thereafter. Since 1993, he is Director of the Acute Coronary Unit. He has participated in over a hundred conferences, local and international, with several papers. He has undertaken extensive scientific and research work and has participated in five international studies. His research areas of interest include echocardiography and heart failure.

He is member of Hellenic Cardiological Society (HCS). He is also member of the working groups and heart failure in the HCS.

Nikolaos Lazarou graduated from the Medical School of University of Athens,Greece, in 1975. He was trained in Internal Medicine in the "Evangelismos Hospital" of Athens until 1982.

He worked as a fellow resident in University Hospital of Patras thereafter. Since 1999, he is Director of the Emergency Department at the University Hospital of Patras. As a member of the NGO "Medical Intervention" he participated in the program Development of a System of Wireless Transport of Medical Data for Better Co-Ordination and Control of Emergency Incidents in the Region of South Serbia (2009-2010) funded by the Hellenic Ministry of Foreign Affairs.

He is a member of the facilitation and coordination of the Emergency Department of the Ministry of Health of Greece.