Security, Safety, and Related Technology – The Triangle of eHealth Service Provision

Mario SAVASTANO a,1, Asbjorn HOVSTO b, Peter PHAROW c and Bernd BLOBEL c

a IBB, National Research Council of Italy (IBB-CNR)
b ITS Norway, Oslo, Norway
c eHealth Competence Center, Regensburg University Hospital, Regensburg, Germany

Abstract. The developing of innovative solutions in the emerging eHealth market requires strong economic efforts which may be justified only in presence of particularly suitable boundary conditions. Among the factors retained of primary importance for the development of eHealth, a correct approach to id-management is unanimously considered fundamental. Three keywords in the id-management context appear particularly important: standardization, security and safety. Standardization may contribute to increase the size and duration of the eHealth market, while security and safety may encourage all the stakeholders to trust in an appropriate and safe management of all the very sensitive personal data involved in the eHealth applications. The aim of the present paper is analyzing some security and safety issues in eHealth from the particular prospective of the identity management and standardization. The paper highlights the mission of the EU funded “BioHealth” project whose mission is to increase the stakeholders’ knowledge about existing and emerging standards in eHealth with particular reference to identity management [1].

Keywords: eHealth, Security, Safety, Ethics, Biometrics, RFID, Standardization

Introduction

The healthcare and welfare domains, in both developed and developing countries, are turning towards an extended interaction among different stakeholders. A significant part of this intense communication consists of very sensitive personal information and, therefore, appropriate measures have to be adopted to protect data. If patients are not confident that their data will be acquired, transmitted and stored in a secure and confidential way, they will not be forthright and reveal accurate and complete information. On the other side, if healthcare providers themselves are not confident that the organization responsible for the management of the records will keep them secure and confidential, they will probably limit the disclosure of data. Having assessed that security and privacy represent two fundamental factors in eHealth, there are other issues that play important roles, with particular reference to id-management procedures which represent one of highest level key factors of eHealth.

1 Corresponding Author: Mario Savastano, IBB-CNR, c/o Department of Electrical Engineering of the Federico II University of Napoli, Via Claudio 21, 80125, Napoli, Italia; E-mail: mario.savastano@unina.it
Many experts suggest that biometrics and RFID (Radio Frequency Identifiers), will find always more a proactive integration with eHealth but, on the other way, some concerns regarding the safety these technologies are raised. For example, in some particular contexts, despite of the large and growing diffusion, iris recognition give sometimes rise to suspects for a potential damage of the eyes and the same RFID identifiers are under investigation because of the electromagnetic pollution. Sticking to the existing safety standards and informing the users of a perfect compliance may represent a valid answer to the concerns.

1. Materials and methods

Advanced concepts of eHealth place the citizens in the focus of a net-centric architecture in which the peripheral is represented by cards and tokens that can bear medical data, improve accessibility to information on services and data, or just serve as authentication token. Since they enable a high-level healthcare data and services access and provision, aspects like security, safety, ethics as well as underlying and supporting technologies need to be clearly addressed before establishing a technical solution. The preferred way to deal with the future challenges of modern healthcare requirements shall be a well-balanced combination of mobile personalized security devices and advanced health networks for both information and services provision. The identity management for all principals (persons, systems, applications, devices, components, etc.) is the key for all further security and safety services. Thus, concepts of security, safety, privacy, quality, and ethics play an important role in the framework of advanced health services. Technologies like biometrics, Radio Frequency Identification (RFID) and Near Field Communication (NFC) are able to technically support the legal, political, and social requirements for such advanced healthcare and welfare service provision [2], [3], [4].

2. Security and safety requirements

The security requirements in the medical area, technically speaking, are not particularly different from those required in other domains. Apart from a very demanding and dynamic privilege management and access control policy, medical and health applications (like in hospital, diagnostic images, laboratory information systems, General Practitioners office software and many other software solutions) base their security functions’ provision on available proper mechanism and algorithms for authentication (identification and verification), identity management, confidentiality, integrity as well as availability and accountability [5], [6]. Additionally, aspects related to mechanical, electrical and electromagnetic safety, and play a crucial role in eHealth because safety of patients overrules virtually any other legislation, both in normal and emergency operations. Every technology applied in healthcare needs to strictly and comprehensively address these security and safety requirements derived, e.g., from respective legislation and ethical rules [4].
2.1. Security requirements towards advanced technologies

Security technologies are frequently used for enabling trustworthy communication and application security services [5]. With reference to Object Management Group (OMG)’s definition of “principal” [7] a basic security principle reflects a certified binding of a principal to its electronic unique identifier or assigned properties, rights and duties, also called attributes of that principal. Application security services deal with authorization and access control to data and functions. Besides, they also cover accountability of principals, audit track and auditing of these principals and services ensuring integrity, confidentiality of data and functions. Communication security services concern the identification, authentication, and verification of communicating principals. In an end-to-end secure communication environment (object security), these services are used for authentication and control of access rights of principals communicating as well as integrity, authenticity, confidentiality, and accountability including non-repudiation of origin, receipt, and information exchanged. For such security objects, security-aware principals are needed [2], [5].

Integrity and confidentiality of communicated data may also be provided at a system level transparent to the application and to the user following, but not requiring, the user’s awareness for those security measures (channel security). Another important requirement for both communication and application security concerns the availability of information and services. More information regarding the different security categories, services, and underlying mechanisms can be found in [5], [6].

2.2. Safety Requirements towards Advanced Technologies

In the development of advanced technologies particular attention should be paid to safety requirements. With reference to the e-health context a specific interest is represented by some authentication devices such as biometric sensors or RFID.

2.3. Safety Requirements in Identity Management

There are two main sources of concerns for safety in the domain of the biometric authentication. The first is represented by the possibility of being infected touching the sensors (e.g. hand-geometry or even fingerprint readers). Even if this possibility may be considered equivalent to that arising in touching a door knob or a telephone, it is anyway true that hospitals represent high-risk locations. Hospital-acquired infections (HAIs), also known as healthcare associated infections, encompass almost all clinically
evident infections that do not originate from a patient's original admitting diagnosis [8]. Nosocomial infections are caused by viral, bacterial, and fungal pathogens. Therefore also the use of a sensor may result in a potential exposure to risk.

Other concerns may arise from the use of biometric sensors which use the eye as a source of information. Iris recognition systems use LED (Light Emitting diodes) which diffuse near-infrared light (NIR) to improve iris detail with dark irises. Unlike UV, IR does not have the energy to produce photochemical damage but NIR illuminators may pose safety issues since the eye does not respond to NIR and does not protect itself as with visible light by means of pupil contraction, avoidance or blinking.

As it attains safety standards or iris recognition systems, LED Eye Safety Standards apply and therefore the following standards and regulations (for references see the respective organizations’ homepages):
- ANSI Z136.1 “Safe Use of Lasers”
- American Conference of Government Industrial Hygienists (ACGIH) 'Threshold Limits Values', 1994
- ICNIRP (1996) laser guidelines for exposure limits (ELs)
- IEC / EN 60825-1

While biometrics is used for persons, RFIDs have a primary role in e-health since they improve dramatically the identifications and traceability of materials. Some concerns because of the pollution induced and some documents highlight the necessity of further investigation. Main safety standards for RFID are:
- EN55022 Class A equipment (EN61000-6-3:2001) for emissions
- EN61000-6-2:2001 for industrial immunity
- EN60950:2000 safety standard for Information Technology Equipment

3. Technical Challenges and Solutions for Security and Quality

Healthcare does not allow any kind of compromise in terms of confidentiality, integrity, availability, accountability, authenticity or reliability and therefore require an particularly safe management of data since, compromising the rating of a hospital’s IT assets, is very likely to have an unfavorable impact, including the risk of a significant financial loss. Consequently, there is an increasing and critical need to protect information and to manage the security of information and communication systems.

While the original motivation for introducing IT security measures has often been security enhancements, appropriate security solutions also offer substantial potential for cost savings and for accomplishing new business opportunities. The ISO/IEC 20000 standard benchmarks the capability of organizations in delivering managed services, measuring service levels and assessing performance. The implementation of ISO/IEC 20000 will reduce operational exposure to risk, meet contractual and tendering requirements, demonstrate service quality and deliver the best possible service. Accordingly it can result in cost savings for users, large or small organizations as well as increased productivity and improved customer service. Regarding software asset management, the implementation of “ISO/IEC 19770-1:2006, Information technology
Software asset management – Part 1: Processes”, enables organizations to benchmark their capability in delivering services, measuring service levels and assessing performance. Until now the application of these business processes has been arbitrary, and relatively few organizations have been able to implement a comprehensive software asset management strategy with the potential of massive savings in license costs and maintenance fees.

4. Discussion of Results and Strategies

Although everyone recognizes the importance of sticking to standards in the design of eHealth applications, its intrinsic interdisciplinarity represents an evident factor of complexity. Moreover, even if all stakeholders of a project have a sufficient knowledge of the technical and standardization domains, some aspects, such as privacy related or ethical issues are difficult to approach both due to their uncertain boundaries both because of the different perception at the international level. In the course of the BioHealth project, such aspects have been clearly individuated but, at the same time a certain difficulty has emerged in promoting standards in eHealth. Three major issues seem to have priority: (i) make a selection in the domain of stakeholders to find the most appropriate ones for the relevant application, (ii) adopt user-friendly approach, such a as multimedia (video, animation, simulation, etc.) to highlight the benefits of standardization, and (iii) propose a centralized approach, at a EU level, to manage the identity management problems concerning technical and ethical issues [3], [4], [5].

5. Conclusion and outlook

A reliable and secure identification is the basis for all advanced security and safety concepts. This is particularly true for health information systems and applications which require an empowerment of all parties (principals) requiring a secure and trustworthy way of communication and collaboration. Moreover they depend strongly on common acceptance which, in its turn, is strictly correlated to privacy and ethical issues [8], [9], [10].

Different technologies including biometrics and RFID, allow for guaranteeing high-level security and safety services addressing proper identification of both human beings and goods but diffusion of standards in these fields is still away from a satisfactory level. Projects such as BioHealth, promoting the knowledge and dissemination of standards, may be extremely useful in supporting eHealth applications but, at the same time, they often require a time frame that exceeds the duration of the project.

Acknowledgement

The authors are in debt to the European Commission for supporting and funding the “BioHealth” project within Europe INNOVA Platform Initiative as well as many other partners and organizations (including ISO TC 215, ISO / IEC JTC1 SC 37, CEN TC 251, CEN TC 224, EFMI, ICAO, CEN/ISSS, IEC, ITU, and HL7) for their permanent support and cooperation in all areas of security, safety, and privacy standardization and policies [1].
References


