Savastano, Mario

Critical Id-Management factors in eHealth applications

Savastano, M.[1], Hovsto, A[2], Pharow, P.[3], Blobel B.[3]
[1] National Reserarch Council of Italy - Institute of Bio-Structures and Bio-Images (CNR-IBB), Napoli, Italia
[2] ITS Norway, Oslo, Norway
[3] eHealth Competence Center, Regensburg University Hospital, Regensburg, Germany

Abstract

The developing of innovative solutions in eHealth requires a careful consideration of the aspects correlated to identity management, the broad strategic and administrative area which, generically, deals with identification or verification of the individuals' identity other than managing their access to resources by associating rights and restrictions. In several critical contexts, such as eHealth, id management procedures based on the use of traditional credentials such as pins or smart card, may be supported or even replaced by new authentication procedures that implement biometric identifiers. A logical access to the patient records represent a classic case in which biometrics may be used to strengthen the level of confidentiality but also a physical control of the personnel having the right to access to the server room where patients' data are stored may be seen as a procedure supporting the diffusion of eHealth. Nowadays, thanks to the characteristic of "assigning an identity" to objects (or even people), the term "identity management" embraces also the context of the Radio Frequency Identifiers (RFID) and the increase in security, safety and productivity caused by the introduction of such devices is well known to all eHealth stakeholders. It is anyway undoubted that, despite of the advantages offered, both biometrics and RFID are still encountering a certain difficulty in becoming popular in eHealth. Several motivations justify the obstacles and the aim of the present paper is analyzing them other than highlighting the fundamental role played by security, safety and privacy issues. Furthermore, the paper emphasizes the importance of the standardization activity in identity management with particular reference to the EC funded "BioHealth" project [1] targeted to the diffusion of identity management standards in the context of eHealth.

Introduction

The healthcare and welfare domains, in both developed and developing countries, are turning towards an extended interaction among different stakeholders. A significant fraction of the intense communication among them, consists of very sensitive personal information and, 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 that is responsible for the management of the records will keep them secure and confidential they will probably limit the disclosure of data.
In both cases, these limitation of trust lead to an inferior healthcare [2]. With particular reference to the identity management context, which is considered by many expert a key factor in eHealth, other psychological barriers may be caused by the patients' concerns of being harmed by the identification devices. For example, in some particular contexts, despite of the large and growing diffusion, iris recognition may 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.
The correct response to these reasonable instances may consists in a strict verification of the devices' and projects' compliance to safety standard and in a valid communication of this compliance to the users.

The role of security, safety and privacy

Advanced concepts of eHealth place the citizens in the focus of a netcentric architecture in which an important role is played by cards or tokens used in the nodes of the structure. They can bear medical data, improve accessibility to information on services and data or just serve as authentication tools. As anticipated in the previous paragraph, since they enable a high-level healthcare data and services access and provision, the aspects related to security, safety and privacy need to be clearly addressed before establishing a technical solution. Technologies like biometrics, 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 [3], [4], [5].

Security 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].

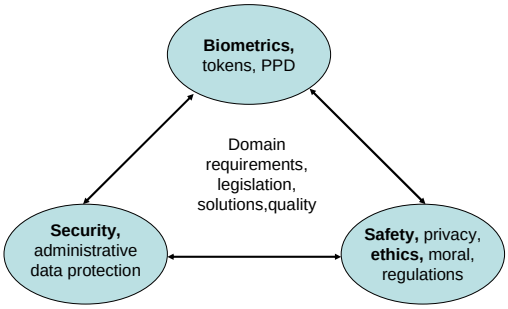

Figure 1. The eHealth "good practices" triangle

In Europe and other parts of the globe, security technologies are frequently used for enabling trustworthy communication and application security services [6]. With reference to Object Management Group (OMG)'s definition of "principal", 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.
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 [3] and [6].

Safety Requirements

Aspects related to safety play a crucial role in eHealth because they overrule virtually any other legislation, both in normal and emergency operations. With reference to the identity management context, a specific interest in eHealth should be paid to some authentication devices such as biometric sensors or RFID.
There are two main sources of concerns for safety in the domain of the biometric authentication. The first one is represented by the possibility of being infected touching the sensor (e.g. hand-geometry devices or fingerprint readers). Even if the possibility of being infected may be considered equivalent to that arising in touching a door knob or a telephone, it is anyway true that health locations should be considered at high-risk. Hospital-acquired infections (HAIs), also known as health-care–associated infections, encompass almost all clinically evident infections that do not originate from a patient's original admitting diagnosis. Nosocomial infections are caused by viral, bacterial, and fungal pathogens and therefore also the use of sensors requiring a contact with a part of the body may give rise to 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 details 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. It should be anyway highlighted that iris recognition devices must be compliant to very strict standard and that their massive use has not evidenced any threat. In particular, as it attains safety standards for iris recognition systems, the following document should be considered:

- ANSI Z136.1 "Safe Use of Lasers"
- American Conference of Government Industrial Hygienists (ACGIH) 'Threshold Limits Values' 1994.
- IEC / EN 60825-1
- International Commission on Non-Ionizing Radiation Protection (ICNIRP), "Guidelines on limits for laser radiation of wavelengths between 180 nm and 1,000 mm.", Health Phys. 71:804–819, 1996
- International Commission on Non-Ionizing Radiation Protection (ICNIRP), "Revision of guidelines on limits for laser radiation of wavelengths between 400 nm and 1,400 nm.", Health Phys, 2000

As anticipated, some concerns may arise because of the electromagnetic pollution caused by RFID implementations. RFID is a relatively new technology, the discussion on potential threats due to pollution is very complex and further investigations on the issue should be carried out.

Privacy requirements

Increasing concern for individuals' privacy and confidentiality coupled with a growing body of legislation and codes of practice governing the use of personal and health data means that sharing health data poses technical, organizational and ethical challenges [7]. A privacy impact assessment process is particularly useful in implementations of new id management technologies such as biometrics or RFID because such analysis, at the design stage of an implementation, can avoid privacy errors and the costs of rectification later.
With particular reference to biometrics, which several eHealth suggest for securely accessing the patients' data, an important guide on privacy issues is provided by the fair information practices (From the OECD Guidelines on the Protection of Privacy). Some already existing applications have anyway highlighted that, apart from a general privacy framework, accessing by means of biometrics to patient data requires a clear assessing of the legal requirements to manage the exceptions. For example, in case that a biometric sample of the patient is required to access the data, he/she has to release a specific authorization to parents or doctors in case of inability to provide the sample.
While biometrics is mainly used for logical or physical access, the tracking of objects or of people is a key functionality of RFID. Applications span from the labeling of products to the identification of the patients' or personnel position and it is clear that in the applications concerning humans a particular attention should be devoted to the privacy aspects. A constantly growing number of documents is dedicated to data protection in RFID applications [8] and a general consideration accepted in several countries is that benefits and privacy should find both a satisfactory level of balance.

Other relevant standardization issues

Health care does not allow any kind of compromise in terms of confidentiality, integrity, availability, accountability, authenticity or reliability since compromising the rating of a hospital's IT assets is very likely to have an unfavorable impact, including the risk of significant financial losses. 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 consisted just in heighten the level of guard, appropriate security solutions may also offer a substantial potential for cost savings and for accomplishing new business opportunities. A particular role in this sense is played by the ISO/IEC 20000 standard since it benchmarks the capability of organizations in delivering managed services, measuring service levels and assessing performance. The implementation of ISO/IEC 20000 reduces operational exposure to risk, meet contractual and tendering requirements, demonstrate service quality and deliver the best possible 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 asset management strategy allowing potential massive savings in license costs and maintenance fees.

The BioHealth Project – Early findings of current implementations of ID management policies in the European countries context

Although experts recognizes the importance of sticking to standards in the design of eHealth applications, it should be recognized that, at least in some contexts, the diffusion of standardization in eHealth is still unsatisfactory. With particular reference to ID management, the general complexity of the context is further increased by other factors. For example, focusing the attention on biometrics and RFID, it appears very clear that their borders with privacy are very vague and that such borders change in time as the public perception changes. Furthermore, the differences from country to country which characterize the context of data protection, add a further element of complexity.
In order to support standardization in eHealth, the European Commission funded the BioHealth project (www.bio-health.eu). Some findings of the initiative were:

- Even if eHealth stakeholders agree on the fact that the electronic medical record offers the promise of improved care and increased efficiency, they generally agree that introducing information technology into health care may create new generalized risks to privacy. The concerns associated to these risks may represent a strong inhibition factor for ID management large scale applications;

- A well targeted promotion of standardization is generally very effective. Finding appropriate eHealth stakeholders who are able to understand the importance of the new ID Management tools may facilitate the proliferation of advanced technologies obtaining a "domino effect";
- The communication concerning the benefits of standardization should be provided at a very user-friendly level. Since the world of standards is often seen, by the majority of the eHealth stakeholders, as a complex and technically sophisticated context, in promoting the benefits of standardization, presentations, videos, animations or simulations concerning practical cases, are much more effective than strictly technical or juridical discussions;
- A European centralized competence hub on identity management issues could be of great benefit to harmonize ID management. Even if specific organizations already provide expert opinion from member state level to the Commission on questions of data protection, the increasing importance of biometrics or RFID would probably require a more specific approach.

As it attains the European ID Management scenario in the eHealth context, a strong message is provided by the Art. 29 Working Party (an independent European advisory body on data protection and privacy) Work Programme 2008-2009. Art. 29 Working Party has considered "Ensuring data protection in relation to new technologies" among the relevant issues. In particular its activity in ID Management will address biometrics (both public and private use – focus on a specific or new application…), RFID and Medical data (e-health patient records).

Conclusions

A reliable identification is the basis for all advanced security and safety concepts. This is particularly true for eHealth information systems and applications which require an empowerment of all parties (principals). They require a secure and trustworthy way of communication and collaboration and depend strongly on common acceptance which, in its turn, is strictly correlated to privacy and ethical issues.
Different technologies including biometrics and RFID allow high-levels of security and safety services in addressing a proper identification of both human beings and goods but, at the same time, the diffusion of standards is still far away from a satisfactory level. Projects like BioHealth may be extremely useful to promote standards but, at the same time, they need 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 as well as other partners and organizations (including ISO, CEN, ISO/IEC JTC1, ICAO, EFMI, CEN/ISSS, and HL7) for permanent support and cooperation.

References

[1] EC funded project BioHealth "Security and Identity Management Standards in eHealth including Biometrics – Specific Requirements having an Impact on the European Society and on Standardization". Scheduled 2006 – 2008. www.helmholtz-muenchen.de/ibmi/biohealth (site last accessed January 2008)

[2] HIMSS Privacy and Security Principles; http://www.himss.org/content/files/CPRIToolkit/version6/v6%20pdf/D02_Privacy_and_Security_Principles.pdf (last accessed November 13th, 2007)

[3] Blobel B: Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems. Series "Studies in Health Technology and Informatics" Vol. 89. IOS Press, Amsterdam 2002.

[4] Kluge EHW: Medical Narratives and Patient Analogs: The Ethical Implications of Electronic Patient Records. Methods of Information in Medicine 1999 38 4: 253-259.

[5] Ball, MJ, Douglas JV: Redefining and Improving Patient Safety. Methods of Information in Medicine 2002 41 4: 271-276.

[6] Blobel B, Pharow P (Eds.): Advanced Health Telematics and Telemedicine. The Magdeburg Expert Summit Textbook, pp. 21-28. Series "Studies in Health Technology and Informatics" Vol. 96. IOS Press, Amsterdam 2003

[7] http://e-hrc.net/research/ethics_privacy.htm (site last accessed January 2008)

[8] http://www.olis.oecd.org/olis/2007doc.nsf/LinkTo/NT00005A7A/$FILE/JT03238682.PDF (site last accessed January 2008)