

How to Achieve Sustainability in Advanced eHealth Sensor-based Systems

Asbjorn HOVSTO^{a,1}, Peter PHAROW^b, Bernd BLOBEL^b

^a *ITS Norway, Oslo, Norway*

^b *eHealth Competence Center, Regensburg, University Hospital, Regensburg, Germany*

Abstract. A key element for companies is the sustainability of investment. The development of innovative solutions for new markets requires investment might be supported by sensor-based systems. Standards can help guaranteeing long-lasting solutions – they can't guarantee market success. The eHealth domain is a challenging one from the standardization viewpoint as it combines different areas like identity management, security, sensors, safety, ethical and social guidelines, and advanced technologies for bioengineering and biomedical devices. Existing and emerging standards, norms, specifications, technical reports, best practice papers, and policy guidelines need to be known to all stakeholders involved. Awareness, confidence, and acceptance of security solutions in eHealth complete the catalogue of required activities to be performed by major Standards Developing Organizations. The EU project BioHealth aims at increasing the stakeholders' knowledge about existing and emerging security, identity management and sensor standards in eHealth. Awareness for sustainability levels of solutions is the key to acceptance. The article aims at describing how information on applying security, identity management and sensor standardization can be provided to the users and how this awareness activities are structured and performed.

Keywords: eHealth, Sensor, Security, Safety, Standardization, BioHealth, INNOVA

Introduction

Advanced information and communication technology (ICT) is today's backbone of companies, research institutions, and the public sector. The ICT infrastructure is hereby an important part of the organization infrastructure. ICT gets of increasing interest for the society regardless whether users typically just search for reliable information on the Internet, write or receive emails, create documents, or use online shops for different business or personal purposes. Attacking an ICT infrastructure may lead to unauthorized access to, or modification of, data, loss of data, loss of availability of services, and loss of performance. In a standardized manner, those threats must therefore be analyzed, risks must seriously be validated, and countermeasures need to be defined and adequately implemented. Standardized ICT security and related safety and privacy measures are thus of high and even growing importance in virtually any social sector or business area including the eHealth domain [1].

Materials and Methods

Healthcare around the globe in developed countries, developing countries, and countries in transition is turning towards shared and personal care providing an integrated care approach. The underlying paradigm change is bound to an ICT-based communication and cooperation network between different providers involved in patient's care. Challenges of increasing quality and efficiency requirements in the domain need to be met not only by local and regional providers but increasingly by national and European networks of healthcare establishments and health professionals. The application of respective standards increases both technical (functional) and semantic interoperability between all stakeholders that form the domain of eHealth.

eHealth Stakeholder Requirements

The aspect of an active citizen and patient involvement and patient empowerment in the healthcare and welfare processes is an important pre-requisite for achieving the success expected by many developed countries. Health

¹ Corresponding Author: Asbjørn Hovstø, Security and Biometrics, ITS Norway, Grenseveien 92, P.O.Box 6086 Etterstad, N-0601 Oslo, Norway. expert@itsnorway.no. Phone: +47 951 48828. <http://itsnorway.no>.

cards, sensors and other trustworthy and secure (personalized) devices do play an important role in this process. They allow developing an integrated eHealth environment by integrating health informatics, patient integrity, and patient integration. Keywords to foster these processes are -of course- health information systems, public surveillance systems, health card, token, and device-related technology but also the role of these tokens and devices in the process of patient integration, their security functionality for data integrity and patient integrity, the problems concerning access rights, and related data protection and privacy aspects [2].

Security and Safety Requirements

The related security requirements in the medical area are technically not that different from other application domains. Apart from a very demanding and dynamic privilege management and access control policy, medical solutions (hospital information systems, radiology information systems, Lab systems, GP office software, and many other applications) base their security solutions on proper authentication (identification and verification), identity management, confidentiality, integrity as well as availability and accountability [3]. Additionally, aspects of electrical safety, mechanical safety, and especially personal safety play an important role as safety of patients overrules virtually any other legislation in case of emergency.

Technical Requirements

Wireless and contactless identification is a promising technology for applications such as inventory and health supply chain management, logistics, transportation, and access control. Radio Frequency Identification (RFID) has already proven its strengths to efficiently collect, distribute, store, and analyze information on traced objects. EPC Information Systems is the global standard for sharing collectable information in the supply chain. Near Field Communication (NFC) is used in short-range wireless interaction in consumer electronics, mobile devices and PCs. Biometrics is the technology for secure identification and authentication based on methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Major SDOs in the eHealth Domain

Sustainability in applying and using advanced standards requires awareness for, and confidence in, active SDOs in the domain of eHealth and related technical domains. A few of these SDOs shall be mentioned here as they provide liaisons to the project. From the ISO perspective, its ISO TC 215 “Health Informatics”, ISO/IEC JTC1/SC17 “Cards and Personal Identification”, ISO/IEC JTC1/SC27 “IT Security Techniques and Identity management (IdM)”, ISO/IEC JTC 1/SC 31 “Automatic identification and Data Capture Techniques”, and ISO/IEC JTC1/SC37 “Biometrics”. Regarding CEN, its mainly CEN TC 251 “Health Informatics” and CEN TC 224 “Personal Identification, Electronic Signature and Cards and their Related Systems and Operations” as well as CEN/ISSS with different groups. In addition, SDOs like IEC, IEEE, ITU, and ICAO’s “New Technology Working Group (NTWG)” shall be addressed. Recently, ISO/IEC JTC1 decided to establish an expert group for standardization requirements from sensor-based systems.

Strategy and Approaches

Within a project lifetime of just 24 months for the BioHealth project, special aspects need to be addressed. Right from the beginning, BioHealth experienced a well-balanced consortium of people actively involved in different SDOs, and people working in community building and stakeholder formation [4]. Three areas of activities were explicitly identified:

1. Enforce the advanced use of security-related standardization results in eHealth (both existing and emerging ones, both inside and outside the domain);
2. Identify existing gaps in security, safety, privacy, and IdM standardization for eHealth and sensor-based systems to give reasonable feedback to SDOs;
3. Watch critically the introduction of new tools in eHealth safety and security and in related ID management and sensor-based technologies (e.g. biometrics, NFC, RFID)

Strategy and Approaches

Most of the eHealth standards that were identified being important for the BioHealth project aims and goals are ICT based as eHealth is defined as the combination of traditional medicine with means of advanced telecommunication and informatics (health telematics) and telemedicine.

Existing and Emerging Standardization and its Relevance

The major aspect of fact finding and analysis is the adoption and adaptation of existing (and emerging) standards from other domains where respective healthcare policies are applicable. The project has therefore established working collaborations with several SDOs. Some of these liaisons are based on the active work of BioHealth consortium members (e.g. ISO, CEN, ICAO, HL7, and ETSI); some persons actively involved in standardization were contracted. The problem of getting results forwarded to the project-unaware user community is a well-known one. It's thus very important to make the project known and recognized among the stakeholders (e.g. by website, workshops, presentations, newsletters). Additionally, the project goes for the definition of complex scenarios aiming at comprising different standards communities addressed (security, safety, privacy, RFID, NFC, passport, cards) to attract many stakeholders.

During the course of the project it was found that 24 months are certainly enough time to figure out the problems in advanced eHealth standardization but aren't enough to address and solve them properly. That's why the project has started bringing the analyzed and summarized results into an online tool (a repository) with facilities for both an advanced search (based on keywords and categories) and a standards entry functionality which is administered and monitored by the consortium members. The repository is expected to be fully operable by the end of 2007 [4].

Based on the online repository, there's a need for a successor project with longer lifetime that is able to address the supply chain in eHealth including the large and small companies on the market of hospital information systems, health information systems, and departmental systems. Moreover, the favorite strategy in long terms is an initiative supported by European Union, European Commission, and SDOs for keeping the analyzed and summarized stakeholder-focused standards knowledge up and running.

Sustainability of Standardization Efforts

All stakeholders have to take into account that the medical domain is a very traditional domain with roots dating back to ancient times and to the Hippocratic Oath [5]. So medicine considered a complex domain as such. The respective medical domain knowledge heavily influences the medical workflow which does not make it easy to go for alterations, and process updates. Specific health domain requirements must indeed be derived from ethical, organizational, legal, social, religious, and cultural aspects. Medical secrecy, related privacy and the trustworthy doctor-patient-relationship is the very basis for a successful treatment [6]. But technology can be adopted from other domains; medical knowledge and policies shall be provided. An example is the standards family ISO 27000 on "Information Security Management System (ISMS)". Harmonization is not a one-way business, it needs to be a win-win activity [7].

There's no doubt that many purely technical standards from different domains (e.g. IdM, biometrics, RFID, certificates, cryptography, signatures, keys, devices, EMC, etc.) will extensively be used for eHealth applications. Other standards need to be adopted and adapted (e.g. by developing its own healthcare-specific profiles or sets or parameters) for medical purposes. Examples are standards on security infrastructures, cards and tokens, sensors, medical devices, and medical software. The domain knowledge needs to always be incorporated as healthcare certainly is not like any other domain. In reality, just a handful of real eHealth standards do exist. But there are definitely standardization areas within eHealth (messaging, imaging, etc.) with a high potential for fruitful and close collaboration with other areas. It doesn't waste time, but saves it.

Awareness Raising and Community Building

As the project has to address all stakeholders in virtually any activity, it needed to make itself heard. The consortium needed to make the identified stakeholders aware of existing standards and ongoing standardization work. Among others, the project bases its current activities on, e.g., the Berlin eHealth Week Declaration [8] on strengthening European SMEs in the healthcare domain in order to get the political power, and on the current discussions and negotiations for an EU eHealth Directive. The project aims at defining and completely describing use cases and scenarios including all relevant standards that are living scenarios supporting many stakeholders. Direct liaisons with many leading SDOs exist, established either by the project members who are directly involved, by members of partner projects inside and outside the Europe INNOVA, and standardization

partners from other organizations and associations. An International Conference on eHealth in Regensburg, Germany, in the premises of BioHealth partner URMIC in December 2007 has invited the leaders of ISO TC 215, CEN TC 251, HL7, WHO, IMIA, EFMI, and other organizations that are involved in creating standards, norms, technical specifications, technical reports, guidelines, and relevant materials [9]. Last but not least, the European eHealth Week in Slovenia provided a podium for discussing current status and future challenges in eHealth and beyond.

New Technologies and Their Relevance for Advanced Standardization

Complex areas like eHealth need to be modeled in order to achieve comprehensive results. Applying technical standards in eHealth is another challenging task. The US NIST standard, e.g., describes the use of RFID technology in a healthcare environment [10]. Different application fields are identified. "Asset management" in healthcare includes the management of samples, tissues, devices, tools, beds, chairs, operation tables, and much more. All of these items need to have an ID. "Tracking" addresses healthcare-related topics like the location of objects, quality control, and certain aspects of validity of tissues, samples, etc. "Authenticity" is very important not only for RFID-tagged items but for all principals in healthcare. Examples are, e.g., the source of the RFID tag and the respective ID (a person, a device, or an application). "Matching" in this respect is a safety category and covers the aspects of identifying the right person (patient, health professional) for the right sample, tissue, surgery, medication, treatment, and other activities. A "Process control" needs to be performed in order to explicitly know the current status of tools, drugs, and medication as well as their availability whereas the application field "Access control" covers the application of privileges and access rights to information, samples, tools, rooms, beds, devices, results, etc. In this respect, doctors, nurses, patients, social care workers, and relatives have different access rights that can be controlled using RFID tags. So many different domains - applying RFID technology- work together forming a supply chain.

Discussion of Results

Concluding this approach, "Supply chain management" gives an indication how sensors and RFID can help identifying almost all items in healthcare processes and procedures (patients, health professionals, visitors, supportive personnel, tools, samples, tissues, devices, and many other items). The workflow of a blood bank might be a good example to illustrate the complexity of IdM in healthcare as it includes blood giver, health professional, healthcare establishments (red cross, hospital), proper transportation services to and from the blood bank as well as blood receiver and responsible health professional(s) in the receiving healthcare establishment. BioHealth wants to use this scenario for applying all relevant standards to the workflow [4].

But the addressed security level can only be guaranteed in case the responsible parties (systems and application administrator, chief information officer, IT security officer, data protection and privacy ombudsperson, professional user, privateers, etc.) are aware of all threats and risks linked to advanced ICT means, and are thus keen on applying the respective countermeasures. In other words, they need to be aware of the security problems; they need to develop a certain level of confidence, and they start accepting the related security, safety, and privacy measures affecting the system, the application, the device, the infrastructure, and the whole area of their specific working and living environment [1]. Standards play an important role in this respect.

Conclusion and Strategies

Creating awareness, confidence, and acceptance of sustainable standards in Europe and beyond requires a comprehensive roadmap of activities. According to BioHealth's work plan, the project covers less than 40% of this approach as the project lasts 24 months whereas the roadmap itself contains steps covering 60 months. Liaisons with leading SDOs require sustainability not only of addressed standards but especially of liaising organizations. EU projects do typically not fulfill this requirement. All partners interesting in promoting advanced security standards in eHealth and beyond thus need to go for a different strategy – e.g. an institution or a long-lasting project. All identified partners are working on that currently as they have common aims and goals.

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] 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.
- [2] International Alliance of Patients' Organizations (IAPO), <http://www.patientsorganizations.org> (last accessed November 9th, 2007)
- [3] 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
- [4] EU Project “BioHealth”. <http://www.gsf.de/imei/biohealth> (last accessed November 15th, 2007)
- [5] PBS - NOVA Online: Survivor M.D. - Hippocratic Oath – Classical Version. http://www.pbs.org/wgbh/nova/doctors/oath_classical.html (last accessed November 17th, 2007)
- [6] PBS - NOVA Online: Survivor M.D. - Hippocratic Oath – Modern Version. http://www.pbs.org/wgbh/nova/doctors/oath_modern.html (last accessed November 17th, 2007)
- [7] ISO/ITU Standards Family 27000 “Information Security Management System (ISMS)”
- [8] Berlin eHealth Week Conference Declaration (19/04/2007) - Better health care in Europe - Renewed commitment for co-operation on cross-border electronic health services. http://ec.europa.eu/information_society/activities/health/policy_action_plan/ehealth_conf/index_en.htm (last accessed November 17th, 2007)
- [9] “eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge”. International Conference Regensburg 2007. Expert Summit Book and Proceedings Volumes, IOS Press Amsterdam, 2008.
- [10] NIST Special Publication 800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems Recommendations of the National Institute of Standards and Technology, 2007.