BioHealth - Marketing of eID Standards for the eHealth Domain

Tomáš Trpišovský[e], Claudia Hildebrand[a], Rolf Engelbrecht[a], Peter Pharow[b], Hans Demski[a], Mario Savastano[c], Bernd Blobel[b], Asbjørn Hovstø[d]

1

Abstract

The paper addresses various aspects of recent eID technology application in concrete domain - eHealth. It's evident the technology "senso strico" doesn't provide full solution of consumer requirements, at all. Proper treatment of the new technology ought to be adopted on up dated legal regulatory base.

The eHealth eID business seems currently the third growing in Europe, preceded by banking and "telco" only, so achieving sustained eID acceptance is of the utmost importance. Among the recent technologies RFID and biometrics encourage smooth eID implementation. However RFID's public perception in terms of the privacy concerns and lack of understanding of the new technologies seems one of the obstacles in adopting eID within the eHealth domain. The guidance of stakeholders to the eligible treatment is than a must.

In 2006 the EC project BioHealth has been launched in order to provide classification and marketing of relevant standards and to give feedback towards the standardisation bodies. BioHealth aims to create awareness on eHealth standardisation, to inform on security standards and to facilitate their practical implementation. By providing information and expert advice on standardisation and best practices it will raise the acceptance on standards. Furthermore, the project will pave the way for standardised solutions, which are often not sufficiently known, diffused and finally not implemented.

Keywords:

eHealth, electronic identification, standardisation, identification management, RFID

Introduction /Positioning of RFID within eHealth/

Increasing mobility of the citizens, together with patient empowerment, tends to create new requirements related to health care delivery. "Electronification" in that sense mostly -and not exclusively- represented by the patient's electronic health care record requires primarily secure and trustworthy electronic identification of all the stakeholders. Only when based on confidentiality, the healthcare solutions and follow up reimbursement systems may be operated. The RFID technology seems at present the most challenging solution, mainly for its convenience. On top of that, neither RFID identifier nor readers wear out during their operation. This opens space for a more holistic approach and even the conservative banking sector is already offering the contactless provision on their cards (e.g. MasterCard OneSmart PayPass).

Social services are in many European countries being linked to health services. They need to be accessible ubiquitously in real time and also across borders.

The increasing complexity of the medical systems implies a growing need for safety and security. The

[1] [a] *GSF – National Research Centre for Environment and Health, Neuherberg, Germany*
[b] *eHealth Competence Center, University of Regensburg Medical Center, Germany*
[c] *CNR - National Research Council of Italy, Roma, Italy*
[d] *ITS-Norway - Norwegian Association for Multi-modal Transport Services, Rykkinn, Norway*
[e] *IMA-Institut mikroelektronických aplikací s.r.o. (IMA), Praha, Czech Republic*[1]

US Institute of Medicine stated in 2000 in the report "To Err is human, building a safer health system" [1] that up 98.000 deaths / year in the USA were due to medical errors. Electronic identification is the crucial prerequisite to improve the current status.

Exploiting RFID and electronic patient records, eHealth paradigm can contribute to solving these problems. Technical solutions are available. To ensure the necessary benefits, they have to be connected and to work together smoothly and effectively, while, at the same time, ensuring security and privacy.

In 2004 the European Commission set up the eHealth action plan; one of its goals is interoperability in eHealth. In this sense common commitment of health authorities and industry was further emphasized at the eHealth 2006 conference in Malaga, Spain. [2].

Safety and security standards are tightly bounded to the nature of RFID technology. Awareness of it, awareness of related Identity Management and supportive technologies like biometrics, are triggers for rapid deployment of significantly better, standard-based security solutions.

However, the current acceptance, use and implementation of standards do not meet expectations and a lot of stakeholders do not even know of relevant standards and/or standardisation activities.

BioHealth /Future-Proof Liaison to the Practice in eHealth/

BioHealth aims to spread the knowledge on safety and security related standardisation and to enforce the use of the relevant standards in eHealth. In order to analyse the premises on which BioHealth has been proposed, let's briefly review eHealth and its evolution.

eHealth

The term eHealth originated in the 1990s when the boom of the internet set in. In those years eHealth was mainly indicating the change from paper-based records to digital records and the beginning of electronic data transfer from one health professional/health facility to another using electronic media. Electronic communication and digitalized records are, however, only part of eHealth [3], [4].

Let's understand hereinafter eHealth accordingly to the definition by G. Eysenbach [5] "eHealth is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term comprises not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve healthcare locally, regionally, and worldwide by using information and communication technology".

eHealth therefore, means -besides treating a patient in a collaborative effort- that information from other domains, e.g. bio-informatics, will contribute to the patient's treatment. Preventive care will play a larger part and the citizen's role will be changing. Telemedicine, monitoring devices and mobile systems enable the citizens to stay at home, but they ask the patient's active involvement.

eHealth requires the integration of all stakeholders (including educational institutions), a functioning and, at the same time, flexible and adaptable infrastructure and a standardised framework at all levels (from data to application). The privacy and data of those involved has to be protected.

eHealth systems must be secure and privacy compliant at all times. They have to be based on trustworthy and reliable communication and application security services; they have to be failsafe and available at all times [6], [7]. Cross-border solutions have to ensure inter-operable technical solutions, as well as consider the legal and cultural background of each single country.

Standardisation and Standardisation Initiatives

Standards ensure inter-operable solutions. Needless to say nearly each European country has its own national standardisation body issuing its own national standards. In order not to cause inconsistencies within the standardisation domain these standards need to be harmonised with European and international ones. For certain application domains, European standards are mandatory to be followed. For others, international standards are the only ones to be taken into consideration. Harmonising eHealth applications world-wide is thus a real challenge.

The European Commission has been supporting standardisation activities for many years:

CEN TC 251 is the European Standards Developing Organization (SDO) for the Health Informatics domain. Beside other projects such as the revision of CEN ENV "Health Informatics – Security for Health-

care Communication", the main activities are currently directed to the 5-part standard "Health Informatics – EHR communication (EN 13606 rev) including a first approach to EHR-related security services (Part 4) . In addition to that, the CEN ENV 13927 "Health Informatics – Secure User Identification – Strong Authentication Using Micro-processor Cards" is being reviewed and updated.

ISO/TC 215 (Health Informatics) -a Technical Committee of the International Standards Developing Organization ISO - has been focusing on eHealth-related standards activities.

The most relevant working groups from the BioHealth's point of view are security (WG4) and cards (WG5). Their recent activities are "Security Management in Health using ISO 17799" (ISO 27799), "Privilege Management and Access Control" (ISO/TS 22600), "Public Key Infrastructure "(ISO 17090), and "Functional and Structural Roles" (ISO/TS 21298).

CEN/ISSS eHealth Standardisation Focus Group investigated standards' requirements in the area of "eHealth in support of the eEurope 2005 Action Plan [8]. ISO 7816 Identification cards - Integrated circuit(s) cards with contacts provides the basic smart card specification. Its defined parts 1 to 11 and 15 contain all basic functions related to contact card technology.

The **eEurope Smart Card Charter** helped to solve many of the problems hampering the introduction and progress of IT solutions in eHealth. Important standards in this area are ISO 14443 (Identification cards - Contactless integrated circuit(s) cards - Proximity cards) and ISO 15693 Identification cards - Contactless, integrated circuit(s) cards [9]. ISO/DIS 21549 Health informatics - Patient health card data specifies the Patient Health card data and consists of 8 parts.

Other major groups dealing with eHealth security related standards are -amongst others- the International Telecommunication Union (ITU) [10] and ETSI (the European Telecommunications Standards Institute) [11].

Presently one of the main priorities of the European standardisation activities -confirmed also as work items by **CEN TC224**- concerns the harmonisation of identification and authentication of the European citizen.

ISO/IEC JTC1/SC17 Card technology hosts working groups on ePassports, driver license and health.

Challenges

Standards or even information thereof are often not easily accessible; users are not even aware of their existence. **Even being aware SMEs (Small and Medium Enterprises) are simply not able first to buy, next to study and finally to drop a reasonable part of useless standards.** This situation challenges large global industrial stakeholders to set up competitive (and patented = expensive) de facto standards. These are rarely accessible to for public domains.

Many safety and security standards are available at a regional, national or international level, but they often differ and are competing with each other. There are a number of successful national initiatives and implementations in healthcare, which fail when moving to the European level. Reasons are -amongst others- the lack of trust chains at the European level. Digital signatures of healthcare organisations and citizens need to be recognized in all EC countries. Public organisations have to be involved to solve this problem.

Citizen and patients will have to play a major part in the eHealth process. Therefore, awareness - achieved by a respective level of information-, education and training measures, confidence, and acceptance are vital.

BioHealth - Objectives

BioHealth (Security and Identity Management Standards in eHealth including Biometrics-Specific Requirements having an Impact on the European Society and on Standardisation) is a project funded by the European Commission. Initiated in 2006, it aims at promoting, in a European framework, the diffusion of knowledge and the understanding of existing and emerging security standards in the area of eHealth. It will particularly emphasize privacy rules, id management and implementation of biometrics as a Privacy Enhancement Technology. By being actively engaged in the organisation of targeted trials, domain workshops, and by contribution to relevant conferences, the project's achievements and results will be of benefit to a wide range of audience. Ethical issues -especially regarding biometrics and identity management are major issues.

Standards have to reflect the requirements of the stakeholders in eHealth, otherwise they will not be used. Many of the BioHealth partners are actively involved in standardisation. BioHealth is at presence creating a European forum to collect the requirements of the users to be directed to the relevant organisations (Standardisation Bodies, Political

Bodies,) in order to solicit the adoption of new recommendations and standards both at European and at national level.

Identification Management

Many people consider information about their health to be highly sensitive and to deserve the strongest protection under the law. Shared care where various health professionals may be sharing one patient record across different health systems in different institutions requires adequate Identity Management (IdM).

IdM consists of the secure management of identities, of the identification process during which an entity may be authenticated, and of the information associated with the identification of an entity within some context [12]. The entities might be anything that can be uniquely recognized and each individual entity may have multiple identities that may be used in different contexts. In any case IdM comprises the life cycle of identities and identity information as they are established, modified, suspended, terminated or archived.

ISO/IEC 24760 is a standard that aims to provide a framework for the definition of identity and the secure, reliable, and private management of identity information. This framework should be applicable to individuals as well as organisations of all types and sizes, in any environment and regardless of the nature of the activities they are involved in.

Biometrics

Biometrics is an automated method of identifying a person or of verifying his/her identity based on a physiological (face, fingerprints, hand geometry, iris,..) or behavioural characteristic (handwriting, voice,..). Biometric technologies are seen as a key technology for secure identification and for personal verification all over the world. The new portal launched by the European Commission [13] aims to encourage the development of consistent government policies regarding the use of biometrics and the consideration of interoperability and privacy. It is based on open knowledge sharing and calls for contributions from governments, industry and civil society authors.

On the other hand, biometrics raise some concerns. These range from accessibility aspects which can lead to the exclusion of a person because he/she is unable to prove his/her identity to threats posed by a centralisation or even misuse of the data. Differing legal regulations also cause problems. BioHealth will address these issues

Emerging technologies

Emerging technologies like radio frequency identification (RFID) and near field communication (NFC) hold the promise of improving patient care.

RFID tags may be used to follow up a patient in an emergency setting or to monitor and locate patients and enable them to continue living at home and leading an active lifestyle. They make it possible to track medical drugs in hospitals. Other than for an out-of-stock situation the use of RFID may increase the patients' safety in assuming the correct drug in the correct quantity as prescribed by the medical staff and, by means of single-item tagging and temperature-enabled RFID tags, by being certain of the integrity of the drug (e.g. that the drug has not been exposed to temperature higher than allowed).

RFID Standardisation activity in Europe is managed by Task Group 34 (TG 34) of the European Telecommunications Standards Institute (ETSI) and, at the ISO level by JTC1 / SC31 /WG2.

NFC (Near field communication) technology is gaining increased attention through its adoption by the mobile communication industry. It is based on the ISO 18092 standard, evolved from a combination of RFID and short range interconnection technologies.

Tagging raises a number of significant legal, ethical and psychological questions and one of the tasks of BioHealth will be the discussion of a possible prevention of tagging misuses. Particular attention will be paid to involving the stakeholders in the discussion and communicating issues of general interest to the public.

Without a wide perception of RFID as sufficiently safe and secure device, all the technological benefits will be useless. Therefore one of BioHealth priority is educating the users: by means of explaining benefits as well as limitations and threats in order to enable a proper use of RFID tags to private host credentials.

Workplan

BioHealth aims to raise awareness, confidence and acceptance among the users of security technologies primarily concentrating on identity management, including the application of new technologies like biometrics and RFID. It started of by providing information on standardisation activities and related subjects. Next the available standards will be analysed and presented in a form to optimise their use for the stakeholders. BioHealth aims to set up guidelines for their implementation and will

demonstrate best practice examples tailored to the needs of the different stakeholder groups in eHealth.

The BioHealth portal available at http://mirc.gsf.de/biohealth will serve for information exchange, coordination and community-building activities between stakeholders in Europe. It is open to contributions from the various stakeholder groups. The relationship to the citizen will be fostered to encourage patient empowerment.

Informative and awareness sessions will be organised on regional, national and international level. Policy makers will be contacted to get involved in order to advance convergence of the standardisation policies in eHealth on a European level.

One of the major assets of BioHealth is its members' involvement in standardisation bodies. This enables BioHealth to act as a mediator between the stakeholders and the standardisation bodies, at the same time acting as a multiplier for the standardisation bodies' output.

Best Practice Based on Standards?? /Just One Example/

In order to demonstrate the gap between the scientific RFID background and real RFID application let's consider the next example:

IMA (as the system integrator) has Installed a large RFID based system for about 40K credentials (a mixture of tags and cards) and more than 200 readers spread across Praha. On customer request Mifare technology has been used. However, mainly for economic reasons, no difference between Mifare compliant devices and "devices also fitting for Mifare" has been applied. Next to the installation provisional and final tests has been passed and the system had been running smoothly about a year.

The system operation was than taken over by the customer.

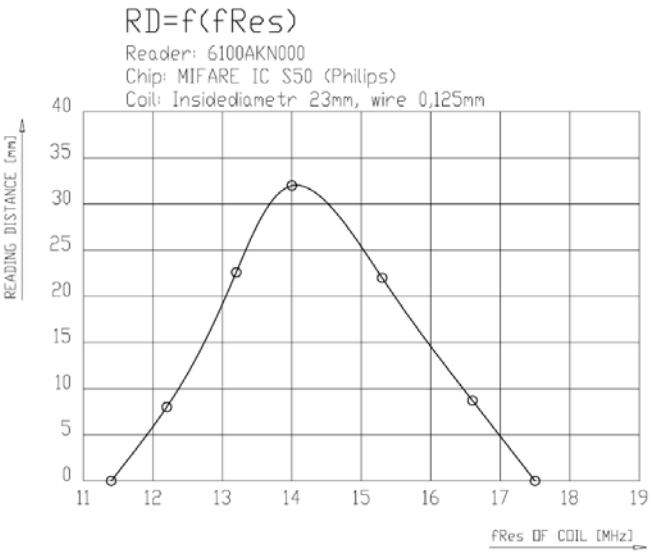
Enlarging the installed system. the customer aimed to benefit from cheap credentials and other system components. Furthermore the purchasing department takes care for new credentials without any test & type verification.

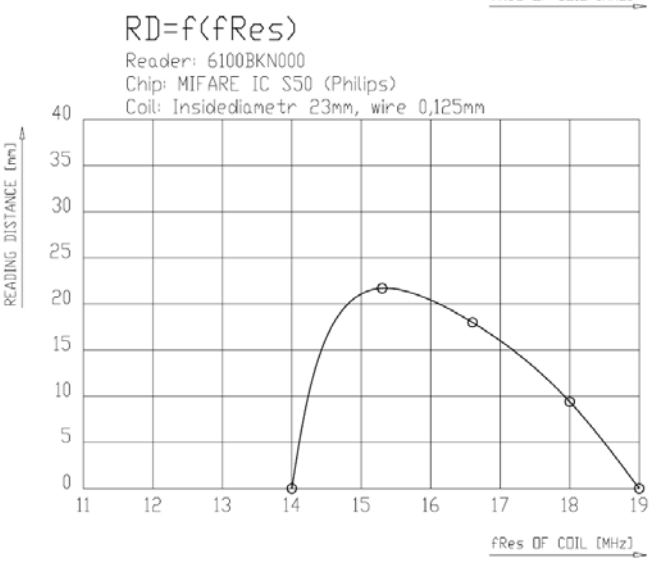
As a result, untested tags have been disseminated while at the same time two types of readers have been applied as shown in the Figures.

It is evident that the proper detection of credentials on 13,56 +- 7KHz causes troubles, reading distance tends to zero (if readable at all) on the second reader and the inconvenience leads to the impeachment of the RFID technology by the users.

Of course the improvement was not that difficult, however, it indicates perfectly the importance of sticking on standards and test & type approval procedures at all the levels of system implementation and follow up operation.

In other words, advanced RFID (smoothly secure, durable, anti-collision, electronic purse, crypto on chip) shall be successfully used only if trusted by the user. And it shall only be trusted if properly implemented and carefully operated.





[Source of Figures: AEG TransID, Czech Republic]

Summary

eHealth is thought to be a necessity to meet the challenges of 21st century healthcare. In order to deliver reliable and widely available applications eHealth requires inter-operability and thus standards on all levels. Though significant work has been done on standardisation in recent years, many of the results are not known to the user nor has the standards' usability been fully evaluated.

In order to help creating the necessary confidentiality and trust in eHealth BioHealth will inform users on security related standardisation in eHealth. The more information citizens and patients have regarding different procedures and processes in healthcare and welfare, the more they will be able to significantly play their dedicated role in the modern healthcare system. BioHealth will address the citizen and provide her/him with information on identity management in eHealth and other related issues, for example the pros and cons of new technologies, like RFID.

The standardisation bodies are urging input from the users; BioHealth will foster the contact between the stakeholders and the standardisation bodies. This Activity is in accordance with the Valencia Declaration on Innovation directed to the European Commission where a closer association of SMEs to the SDOs is claimed [14].

Thus BioHealth aims to offer a sounding contribution to eHealth in Europe.

Acknowledgment

The authors are thanking the European Commission for funding the BioHealth project

References

[1] Institute of Medicine: To Err is human: Building a safer health system (2000). The National Academies Press. URL: http://www.nap.edu/books/0309068371/html/ accessed: 01-12-2006.

[2] Commission of the European Communities, Information Society & Media Connected Health – Quality and Safety for the European Citizen. Luxembourg: Office of Official Publications of the European Communities, 2006.

[3] Weed L. Medical Records, Medical Education and Patient Care. 2nd ed. Cleveland: Case Western Reserve University Press, 1971.

[4] Strunk W, White EB, and Angell R., Elements of Style. 4th ed. New York: Allyn & Bacon, 1999.

[5] University of Chicago Press Staff. The Chicago Manual of tyle. 15th ed. Chicago: University of Chicago Press, 2003.

[6] 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.

[7] P. Ramsaroop, R. Stull, R.J.; Rodrigues, A. Hernandez: Cybercrime, Cyberterrorism, and Cyberwarfare: Critical Issues in Data Protection for Health Services. Information System Technology and Health Services Delivery, Health Services Organization Unit (THS/OS), Pan American Health Organization, Washington, DC, 2003.

[8] CEN/ISSS eHealth Focus Group: Current and future standardisation issues in the eHealth domain: Achieving interoperability. URL: ftp://ftp.cenorm.be/PUBLIC/Reports/eHealth/ - accessed: 01-12-2006.

[9] ISO 15693 Identification cards - Contactless, integrated circuit(s) cards – Vicinity cards. URL: http://en.wikipedia.org/wiki/ISO_15693 - accessed: 01-12-2006.

[10] International Telecommunication Union, ITU. URL: http://www.itu.int - accessed: 01-12-2006.

[11] European Telecommunications Standards Institute. URL: http://www.etsi.org/ - accessed: 27-03-2006.

[12].Windley Phillip J: Digital Identity. 1st ed., Cambridge, O'Reilly,.2005

[13] European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43. URL: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm - accessed: 01-12-2006.

[14]Commission of the European Communities: VALENCIA DECLARATION – Final version: *Innovation policy priorities for Europe, especially for young innovative businesses* http://www.europe-innova.org - accessed: 01-12-2006.

[15]CONSORTIUM AGREEMENT for Coordination Action - FP 6 PROJECT Security and Identity Management Standards in eHealth including Biometrics- Specific Requirements having an Impact on the European Society and on Standardisation (BioHealth), March 1, 2006.

Address for correspondence

Tomáš Trpišovský,
Institut mikroelektronických aplikací s.r.o. (IMA)

Na Valentince 1, 150 00 Praha 5, Czech Republic

Email: tomas.trpisovsky@ima.cz
http://mirc.gsf.de/biohealth
http://standards.eu-innova.org