RESHEN, a best practice approach for secure healthcare networks in Europe

Aggelos GEORGOULAS, Athena BOURKA, Alexandros KALIONTZOGLOU, Nineta POLEMI, Dimitris KOUTSOURIS

A. GEORGOULAS is with the National Technical University of Athens in the School of Electrical and Computer Engineering, 9 Iroon Polytechniou, 15773, Athens, Greece (phone: +30 210 7722430; fax: + 30 210 7722431; e-mail: ageorg@biomed.ntua.gr).

A. BOURKA is with the National Technical University of Athens in the School of Electrical and Computer Engineering, 9 Iroon Polytechniou, 15773, Athens, Greece (e-mail: abourka@biomed.ntua.gr).

A. KALIONTZOGLOU is with Expertnet S.A., 1 Achilleos Str. & 244 Kifissias Ave., 15231, Holargos, Athens, Greece (e-mail: Alexandros.Kalionzoglou@expertnet.net.gr).

D. POLEMI is with Expertnet S.A., 1 Achilleos Str. & 244 Kifissias Ave., 15231, Holargos, Athens, Greece (e-mail: Despina.Polemi@expertnet.net.gr).

D. KOUTSOURIS is with the National Technical University of Athens in the School of Electrical and Computer Engineering, 9 Iroon Polytechniou, 15773, Athens, Greece (e-mail: dkoutsou@biomed.ntua.gr).

Abstract: Electronic communication of healthcare related information (in the framework of Regional Healthcare Information Networks), introduces a number of security risks with regard to confidentiality, integrity and availability, which can become quite crucial taking into account its sensitive nature. PKI is acknowledged as an appropriate means for dealing with such risks, as long as all the involved critical factors are first practically assessed. This paper presents a best-practice approach for secure regional healthcare networks in Europe, examining all the identified crucial parameters (technical, organizational, legal/regulatory, medical and business). Our approach is conducted at two levels (the regional and the European), including the integration of PKI-aware security mechanisms (strong authentication, encryption, digital signature, time-stamping) in three regional pilot sites in Greece, Finland and Germany and demonstrating their interconnection in a pan-European architecture. Following the above approach, some major conclusions are excluded, pointing out existing open issues and possible steps forward.

Introduction

Regional healthcare information networks have recently started to grow in Europe, in order to cover local healthcare provision needs more efficiently and timely, especially in isolated regions, where there is often no availability of central general hospitals. The regional networks can fill this gap, connecting local healthcare service providers with central regional and/or peripheral hospitals and thus making possible tele-consultation, tele-diagnosis and exchange of views between remote located doctors in certain patient treatment cases [1].

However, electronic communication introduces a number of security risks with regard to the confidentiality, integrity and availability of the required information, which can become quite crucial taking into account the sensitive nature of healthcare related data. In order to cope with this problem, the application of proper security mechanisms and solutions is mandatory.

Public-Key technology is uniquely qualified to meet the necessary security requirements for several sectors, healthcare being one of them, and it has become the preferred means for providing these capabilities [2][3]. Public-Key Infrastructure (PKI) based on Trusted Third Parties (TTP) is viewed as an essential solution for the safe deployment of healthcare service provision.

Since PKI is a security framework rather than a mere technical solution, PKI-based security involves several parameters that need to be taken into account for a smooth and successful integration within existing healthcare information networks. Such parameters concern: technical integration of the PKI-aware security mechanisms in medical applications, organizational restructuring and policies, legal compliance, medical involvement, as well as business flow reformation [4].

Although the technical PKI services (i.e. Certification, Registration, Directory, Key services, Time-stamping) are being adequately developed, the above-mentioned operational parameters are in most cases underestimated or not explicitly described, thus leading to a lack of really operational and feasible healthcare PKI implementations. This has serious impacts on the healthcare networks reliability and security, reducing the data availability, as well as the quality of the healthcare service provision itself [1] [5] [6].

This paper, which is based on EC RESHEN (IST-2000-25354) project, addresses the above-mentioned problem, by presenting a best-practice approach for secure regional healthcare networks in Europe. This approach is conducted at two levels (regional and European), examining all the identified involved parameters (technical, organizational, legal/regulatory, medical and business).

In particular, the paper describes and assesses the integration of PKI-aware security mechanisms (strong authentication, encryption, digital signature, time-stamping) in three regional pilot sites in Greece, Finland and Germany, and demonstrates their interconnection into a pan-European architecture. Following the above approach, some major conclusions are excluded, pointing out existing open issues and possible steps forward.

In this respect, the paper is organized as follows: Section 1 provides an overview of the specific pilot healthcare business cases, which were addressed, pointing out their specific security needs and measures. Section 2 describes the best practice implementation and assessment performed. In particular, Paragraph 2.1 presents the technical integration at the four pilots, whereas Paragraphs 2.2 and 2.3 describe the underlying organizational and legal frameworks respectively. Paragraph 2.4 is focused on the medical involvement and assessment at the pilot sites, whereas Paragraph 2.5 describes the business perspectives. Finally, Section 3 draws the major conclusions of the paper.

1. Healthcare business cases and security needs

In this Section we describe the healthcare business flows and the applications/services, which were addressed in our work, with the aim of identifying and solving their security problems. This was done in the framework of existing pilot sites in Greece, Germany and Finland.

1.1 Pilot sites and healthcare applications/services

At regional level the pilot sites are operational healthcare information networks in Europe, providing different kind of application –level services to their patients and users [4]. More specifically:

- *Greece*: The network is established in the region of Central Macedonia, comprising of 9 Health Centres within the region, 31 infirmaries that support the health-care services of the Health Centres and a Regional Hospital. The basic application/service offered is electronic communication of healthcare documents (electronic prescriptions and referrals).
- *Finland*: The network is established in the North Karelia Hospital District, covering nineteen (19) remote locations (primary health care centres), which are connected to the central hospital over the Internet. The basic application/service is the e-referral system for electronic documents communication.
- *Germany*: The network is the ONCONET infrastructure, which is dedicated to the exchange of all relevant material requested for optimal treatment of cancer patients in a shared-care approach, covering the region of the northern part of Saxony-Anhalt. Up to 75 clinics directly or indirectly involved in cancer care are linked to the ONCONET.

These networks are interconnected at European level, in order to offer enhanced communication and information exchange between different healthcare professionals across Europe, in the context of a second opinion service for consultation and treatment (with and without patient consent - two cases).

The following figure (Figure 1) presents the overall concept where the three regional pilots are interconnected into a pan-European scheme.

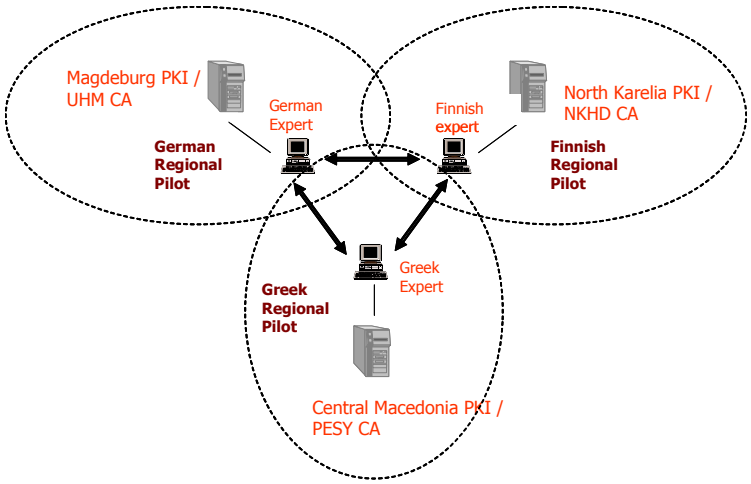

Figure 1. The overall RESHEN architecture

The above-mentioned healthcare networks are facing common security threats at the application level, which are very crucial taking into account the sensitive nature of healthcare related data. This is described in Paragraph 1.2.

1.2 Security needs and measures

The following table (Table 1) summarizes the main security risks as well as the security needs and some indicative measures that need to be taken into account in the three pilots, to protect their information, which in all cases deals with electronic document communication.

Table 1. Security threats, needs and measures in the RESHEN pilots

No	Security Threat	Security Need	Security measure
1	Unauthorized access network resources - unauthorised use of authorised services	Strong authentication	Digital signature mechanisms Smart cards
2	Exposal of confidential/secret healthcare information	Confidentiality	Encryption
3	Unauthorized access to the communication channel	Confidentiality/integrity	Secure Network Protocols, e.g. SSL
4	Modification of healthcare information (e.g. fake prescription document)	Integrity	Digital signature mechanisms
5	Denial of date/time	Proof of date/time	Timestamping mechanisms
6	Concealment of information origin/receipt	Non-repudiation of information origin/receipt	Digital signature Secure e-mail

Following the table, to ensure confidentiality even in case of anonymous data, all transmissions have to be encrypted during time of transmission. Local storage of data can be encrypted but needs an additional policy. The integrity of data needs to be provided as well in order to detect active or passive changes of data items or parts of data items (e.g. destroy medical records). All users have to be identified and authenticated in advance to be sure that only persons with relevant access rights (e.g. medical doctors) can send and receive messages respectively. Last but not least, neither the sender nor the receiver is allowed to repudiate that he has sent or received anything [7] [8]. Most of these measures can be provided by Public Key Cryptography, using a trust framework like PKI and TTPs [9].

In the following we describe how we addressed these issues for the business cases of Paragraph 1.1, in a best practice approach.

2.Security integration and best practice assessment

In the previous paragraphs we described the three regional healthcare networks (regional pilots), as well as the interconnection between them (European pilot), and we identified their specific security threats as well as the required security needs & measures. PKI has already been identified as the appropriate framework for providing the required security measures.

In this Section, we present the establishment of this framework and the integration of the security measures, examining all the technical, as well as the best practice parameters involved (organizational, legal/regulatory, medical, business).

2.1 Technical integration

This part presents the technical integration of security mechanisms in the pilots described in Section1.

The main requirement for technical integration was to address the basic security needs outlined in Table 1 (strong authentication, integrity, non-repudiation, confidentiality, time and date stamping). Moreover, the implementation in all pilots should have the following characteristics:

1. Based on mature and proven technologies.
2. Flexible, extensible and scalable (so as to include additional security services in the future).
3. Standards-based (both for the data representation and the security mechanisms).
4. Interoperable both between the three pilots as well as with similar infrastructures nationally and across Europe.
5. Within the existing mechanisms.

In order to address the above requirements, the following approach was used:

1. *PKI as trust framework*: Three PKI establishments were set-up in the regional pilots, following the relevant national frameworks and activities (accredited CA for Germany, pilot CAs for Greece/Finland). In all cases, well proven products and solutions were utilized, offering a common basic accepted trust framework (including Certification, Registration, Directory, Key services, Time-stamping) [10].
2. *Secure database storage*: As far as data storage is concerned, security was enhanced with the use of specific dedicated database server for secure document storage. This was done in all pilot sites, as a basic technical and organizational requirement for the security of stored information.
3. *XML-based applications*: XML format was used for electronic healthcare documents. XML ensures expendability of the regional applications, in terms of the document types and services applied [11].
4. *XML-based security* (W3C standards): Another important advantage of the XML use is the XML security [12] [13], which is performed at the document type level and is based on internationally accepted standards and processes. Moreover, the XML-based security can provide all the required cryptographic services mentioned in Table 1, in the framework of the local PKI, offering at the same time possibility of extending these services with more advanced ones, like for example the implementation of multiple authorization levels in the healthcare application.
5. *Standards***:** In all pilots we made use of widely adopted standards (W3C Digital Signature and Encryption standards, X.509v3, ITU and ISO Digital Certificate Standard, SSL etc), thus ensuring interoperability with other applications/software at technical level.
6. *Smart cards***:** Smart Cards were used for secure key storage and increased user mobility.

Following the above approach, the next figure (Figure 2) demonstrates the example of the Greek technical integration. Relevant architecture was used in the other pilots as well.

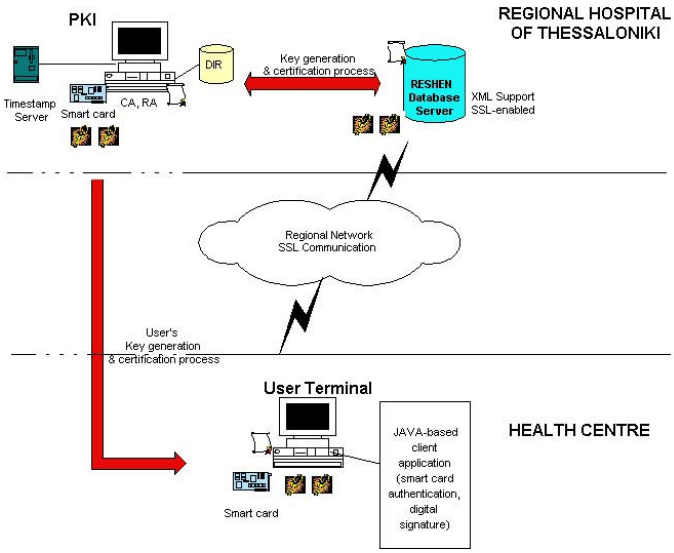

Figure 2. Overall security architecture of the Greek pilot site

Technical integration for the European pilot includes, as a base configuration, the setup of a PKI aware e-mail client supporting S/MIME v3 and crypto cards, the Directories (LDAP) that host practitioners' certificates and a time stamping client. In addition to these, other optional technical tools that have been deployed include Secure FTP clients for the exchange of any type of file (including messages and images), components for the creation and secure exchange of XML documents between clients and a server, and secure videoconference applications operating over SSL. Last but not least, a form of cross certification has been utilized to provide the necessary interoperability framework for the three networks to intercommunicate.

2.2 Organizational structures

In this Section the organizational PKI structure of the three pilots is presented [10]. The organizational structure of the PKI concerns the processes of service provision (e.g. registration of a new user, certificates revocation, etc), the roles of the involved parties as well as the certificate profile which is supported, thus playing a crucial role in the overall network operation.

In order to address these demands, the following steps were taken:

1) The PKI was organized according to the existing structures and use cases of each regional healthcare network.
2) A clear Application Policy was defined for the specific business flows of the each local network.
3) A common application policy was defined for the European level, putting specific points for example for patients consent issues.
4) A very important issue was the definition of Certificate Policy and Certification Practice Statement (CPS) implementing the CPs. Since only in German the accreditation scheme for CAs has been implemented, a CPS was only developed for the German pilot.

In all cases a decentralized model was followed, outsourcing TTP services and keeping healthcare-related services in house.

An additional aspect concerns the administrative framework itself, including education, training and personnel management, which is an important organisational parameter.

2.3 Legal compliance

From a legal perspective, there are two basic requirements: compliance with the national data protection legislation and compliance with the EC directive on electronic signature. All the pilots are taking into account these requirements.

With regard to data protection for example, several security mechanisms are in place like user authentication, access control, encrypted communication, secure storage etc. Concerning e-signature, different situation in terms of legal framework can be found in the three countries. In Germany the digital signature law is in place and operational. In Greece, although there is a national law, the necessary technical and organizational specifications for the set up and operation of CAs, have not been provided yet, thus leading to certain gaps and ambiguities. Finally, in Finland there is no yet national data protection legislation in place. All pilots are prepared to comply with the EC directive, taking into account the relevant national conditions and the experience in the other Member States [14][15].

2.4 Medical involvement

In the previous Sections we described the PKI-based security establishments in the pilot sites, from a technical, organizational and legal point of view. Another very important best practice issue, however, is the involvement of healthcare participants in the security adoption and assessment [16].

In order to address this need, PKI security was integrated in the existing system business flows and extensive user education and training was performed in the three pilots. Education sessions covered basic security concepts, legal issues and policies. The healthcare participants, including medical staff and organizational representatives, were introduced to the security enhanced healthcare applications and trained to their use.

As a measure for the acceptability and usability of the PKI-based security, a user survey was conducted using dedicated evaluation questionnaires. What has been assessed is the acceptance of the healthcare participants towards the medical applications, as well as their awareness on specific aspects of the designed and implemented security mechanisms. However, due to the small sample of medical users participating in the survey, the assessment had more of a qualitative nature than quantitative.

Initially, the survey tried to identify IT use in the medical environment by nurses, physicians and medical research staff. Specific questions evaluated the medical involvement of users into security related operations such as the use of smart cards and strong authentication procedures. The survey also tried to assess the personal experience and expertise of health care participants in their daily use of operating systems and applications, as well as their opinion about typical security related statements considering e.g. trustworthy communication and electronic archives, the role of health organizations in relation to a TTP and the familiarity of the medical

user with specific advantages, disadvantages and risks of electronic communication and secure applications in general.

The user assessment based on the information recorded, showed some interesting results which can only be indicative of what further steps need to be taken in order to promote the medical involvement of users into secure IT environments. Such steps include:

1. Address regionally medical needs, like the secure electronic transactions.
2. Commit all healthcare participants in the processes right from the start.
3. Guarantee medical expertise involvement through consultation procedures and training.
4. Provide a mature and realistic technical and organizational scheme.

2.5 Business perspectives

Since we have examined all the parameters for the implementation, operation and user involvement in PKI-based security, it is now critical to stress the business dimension of the work performed, as this is the main driver for future deployment and extension. This is the purpose of the current Section.

There are two points of view for the business perspectives:

For the Regional Healthcare Networks, the objective is to increase healthcare service quality, thus making the overall network more usable and competitive and attracting more patients (clients), as well as more experienced healthcare professionals.

For the security providers, the objective is the establishment of a feasible and extendable security solution for healthcare, which could be "sold" in other relevant networks and business flows in the country.

In order to fulfil the above requirements, the security implementation should satisfy the following business-related criteria:

1. Integrate security as part of the existing network business flows.
2. Involve all healthcare participants, clearly setting their security-related roles.
3. Define business perspectives in the context of the existing healthcare–related plans and restrictions.
4. Adopt the underlying legal/regulatory framework of the country.

Following the above points, specific business plans were developed both at regional and European level, aiming at further enhancing the research and commercial dimension of the work performed.

3.Conclusions

The paper presents a best-practice approach for secure healthcare networks in Europe, where security is examined towards a number of different parameters, i.e. technical, organizational, legal, medical and business. Some of the main outcomes of the work performed are outlined in the following (including also existing open issues and needs).

As far as technical parameters are concerned, PKI is qualified to cover the security needs of the healthcare sector. The pilots' establishments were based on mature and proven

technologies, thus being flexible, extensible and scalable (so as to include additional security services in the future). Moreover, the use of XML for data representation as well as the use of widely adopted standards ensures the system's interoperability, both between the pilots as well as with similar infrastructures nationally and across Europe.

Regarding the organisational parameters, a decentralized model was followed in our pilots, outsourcing TTP services and keeping healthcare-related services in house. It was recognized that business reengineering is a very difficult task and what is needed is the integration of security mechanisms within the existing healthcare structures and workflows. Also, the development of clear Application Policies as well as Certificate Policies & CPS is essential.

From the legal perspective, the two basic requirements are compliance with the national data protection legislation and compliance with the EC directive on electronic signature. However the legal/regulatory framework is still immature in most countries across Europe.

In terms of healthcare participants involvement, an important issue is the need to raise awareness for secure healthcare. This could be done by developing concrete training procedures and involving high-level healthcare participants, including medical staff and organizational representatives.

Last, from a business point of view, the adopted solution is in line with the current network processes in each regional healthcare network. A basic requirement for successful deployment of such solutions is the development of concrete business plans as well as the definition of financial schemes for the security-enhanced services (healthcare organizations-patients).

4.Acknowledgements

The authors would like to thank the European Commission for supporting the RESHEN project (IST-2000-25354), leading to the work described in this paper. We would also like to thank the RESHEN partners for reviewing this paper.

5.References

[1] A. Bourka, A. Kaliontzoglou, D. Polemi, A.Georgoulas, P. Sklavos, "PKI-based security of electronic healthcare documents", SSGRR 2003w, International Conference on advances in infrastructure for electronic business, science, education, medicine and mobile technology, January 2003, Italy.

[2] *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, IEFT RFC Standard 2459, 1999. Available: http:www.ieft.org/rfc/rfc2459.txt

[3] *Information processing systems – Open Systems Interconnection – Basic Reference Model Part 2: Security Architecture*, ITU-T Rec. X.800 | ISO/IEC Standard 7498-2,1989.

[4] D. Polemi, A. Kaliontzoglou, "Scenarios, organizational issues and services", RESHEN Project, European Commission, Tech. Del. D.3.1, 2001. Available: http://www.biomed.ntua.gr/reshen

[5] A. Bourka, D. Polemi, D. Koutsouris, "An Overview in Healthcare Information Systems Security", presented at the 2001 MEDINFO Conference, London, UK.

[6] P. Heider, H. Nilsson, D. Pinkas, "Evaluation of the European Trusted Services Programme", European Commission, Final Report, 1999.

[7] Healthcare Information and Management Systems Society (HIMSS), 1999 survey (http://www.himss.org/survey/)

[8] A. Bourka, A. Georgoulas, G. Koukoumelis, K. Papadaki, Y. Tollias, B. Blobel, J. Lehtonen, T. Kupiainen, "Survey on current security practices and solutions in the field of regional Healthcare Information Networks", RESHEN Project, European Commission, Tech. Del. D.2.1, 2001. Available: http://www.biomed.ntua.gr/reshen

[9] A. Bourka, A. Kaliontzglou, D. Polemi, A. Georgoulas, P. Sklavos, "Enriching healthcare applications with cryptographic mechanisms and XML-based security services", *IOS Press Journal on Technology and Healthcare*, to be published.
[10] A. Kaliontzoglou, A. Bourka, A. Georgoulas, B. Blobel, P. Pharow, J. Kraemer, J. Lehtonen, "Report on PKI establishment", RESHEN Project, European Commission, Tech. Del. D.4.2, 2002. Available: http://www.biomed.ntua.gr/reshen
[11] *Extensible Markup Language (XML) 1.0*, W3C Recommendation, 1998. Available: http://www.w3.org/TR/1998/REC-xml-19980210
[12] *XML-Signature Syntax and Processing*, IETF RFC Standard 3075, 2001. Available: http://www.ietf.org/rfc/rfc3075.txt
[13] *XML Encryption Syntax and Processing*, W3C Candidate Recommendation, 2002. Available: http://www.w3.org/TR/xmlenc-core/
[14] European Commission, "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures", *Official Journal L 013*, pp.0012–0020, Jan. 2000. Available: http://europa.eu.int/ISPO/ecommerce/legal/digital.html
[15] Z. Kardasiadou, B. Blobel, S. Amberla, "Legal and policy issues of PKI adoption in health telematics applications in Greece, Germany and Finland", RESHEN Project, European Commission, Tech. Del. D.2.2, 2001. Available: http://www.biomed.ntua.gr/reshen
[16] B. Blobel , A. Kaliontzoglou, A. Bourka, A. Georgoulas, "Report on scenarios demonstration and assessment of pilot operation", RESHEN Project, European Commission, Tech. Del. D.5.1, 2002. Available: http://www.biomed.ntua.gr/reshen