PKI-based security of electronic healthcare documents

A. Bourka, A. Kaliontzoglou, D. Polemi, *Member IEEE*, A.Georgoulas, P. Sklavos,

***Abstract*—Although electronic documents communication is a growing challenge for healthcare, security risks often pose barriers in its wider adoption. PKI is acknowledged as an appropriate means for dealing with such risks, as long as all the involved technical, medical and business factors are first practically assessed. This paper addresses the above need by presenting a pilot healthcare PKI implementation at regional level in Greece, as framework for secure e-documents communication. The proposed architecture is integrated in the existing infrastructure of a Regional Healthcare Information Network, taking into account all technical, organizational, legal and user-related factors. The security services offered at the application level include digital signature, encryption, time tamping, secure document storage and strong authentication. The final result enhances the healthcare network's service quality, as well as its overall reliability, flexibility and usability, especially in terms of secure e-documents transactions.**

***Index Terms*— best practice assessment, PKI security, Regional Healthcare Networks**

I. Introduction

ELECTRONIC communication of healthcare documents is a growing challenge for the healthcare sector, since it can reduce current paperwork complexity, enhance healthcare service provision with faster and more reliable methods, and support information management and co-operation. On the other hand, electronic communication introduces serious security risks due to the fact that any modification, exposal to unauthorized persons or loss of the healthcare data may even put human life at risk. Therefore, the healthcare data security, in terms of *confidentiality*, *integrity*, *non-repudiation*, *availability* and *accountability* is an essential requirement [1][2][3].

Over the last years *Public Key Infrastructures (PKI)*, based on *Trusted Third Party (TTP) services* [4][5] have been qualified as an appropriate framework for covering the above healthcare security needs, which can be utilized at the application level (in conjunction with Internet technologies like Java, XML, SSL) for the provision of cryptographic security mechanisms. Such mechanisms include e.g. strong authentication, encryption, digital signature and time-stamping [3].

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 both new and existing medical applications, organizational restructuring and roles definition, policy development, network liability, medical involvement, as well as reformation of the existing business flows and perspectives with regard to the new security requirements [6].

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. So, for example, we have a number of certification products and tools, but still there are no specific PKI model architectures for healthcare. 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 [7] [8].

The current paper, which is based on work performed within the RESHEN project (Regional Secure Healthcare Networks, IST-25354), addresses the above problem by presenting a success story of PKI-based security for electronic healthcare documents within a specific Regional Healthcare Information Network (RHIN) [9][10].

In particular, the paper describes and assesses the integration of PKI-aware security mechanisms (strong authentication, encryption, digital signature, time-stamping) in

This manuscript was submitted on November 20, 2002. This work was supported in part by the European Commission under the Reshen project (IST-25354).

A. Bourka is with the National Technical University of Athens in the Department of Electrical and Computer Engineering, , 9 Iroon Polytechniou, 15773, Athens, Greece (phone: +30 210 7722429; fax: + 30 210 7722431; e-mail: abourka@biomed.ntua.gr).

A. Kaliontzoglou, is with the National Technical University of Athens in the Department of Electrical and Computer Engineering, , 9 Iroon Polytechniou, 15773, Athens, Greece (e-mail: akalion@softlab.ntua.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).

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

P. Sklavos is with the National Technical University of Athens in the Department of Electrical and Computer Engineering, , 9 Iroon Polytechniou, 15773, Athens, Greece (e-mail: psklavos@softlab.ntua.gr).

an electronic referral and prescription application (e-referral, e-prescription), taking into account all different PKI-related perspectives, i.e. technical, organizational, legal/regulatory, medical and business. The final aim is to use the results as best practice guidelines for PKI-based security in healthcare, which can add value and quality in existing RHIN, in a feasible and applicable way.

The paper is organized as follows: Section II provides an overview of the e-referral / e-prescription business case, functionality and security risks, in the framework of a Regional Healthcare Information Network (RHIN). Section III describes and assesses the security solution, which was adopted, examining all the relevant best-practice areas (technical, legal, organizational, medical, business). Open issues and recommendations are also identified for each case. Last, Section IV summarizes the results and draws the major conclusions, outlining also possible future enhancements.

II. Security Needs and Measures for E-Documents Communication

This Section presents the specific business flow of a Regional Healthcare Information Network (RHIN), the security risks that are identified in this flow, as well as the security measures that should be taken for encountering them.

More specifically, we focus on the case of an e-referral / e-prescription application within the regional network of Central Macedonia (Greece), where all participants make use of central system resources in producing, accessing and sharing electronic patient referral and prescription documents (e-referrals /e-prescriptions).

A. *E-referral/e-prescription business flow*

The Regional Healthcare Information Network (RHIN) that we examine comprises of one Regional Hospital and a number of Health Centres (HC), Infirmaries and Pharmacies within the Region, as shown in Fig. 1 [9].

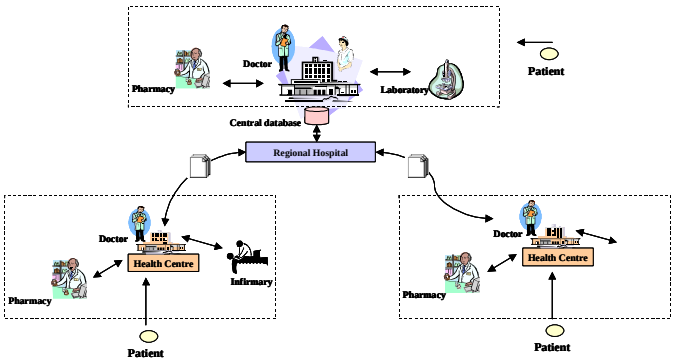

Fig. 1. E-referral/e-prescription communication in Regional Healthcare Information Network.

The Hospital hosts a central database for referral and prescription documents, which can be accessed by client applications, installed at users' terminals in all the network nodes. Users of the system are considered all persons authorized to create and sign, read and act on referral and prescription documents. Users with document signing rights are normally only the doctors of several specialties.

The client applications enable users to create new e-referrals and e-prescriptions (e-documents), deposit them to the central database or store them locally in their local PCs, as well as open existing e-documents from the database (created by them or another healthcare professional) and provide treatment and medication to the patient, based on the document's content. The business flow of the e-referral / e-prescription is captured in the use case diagram of Fig. 2:

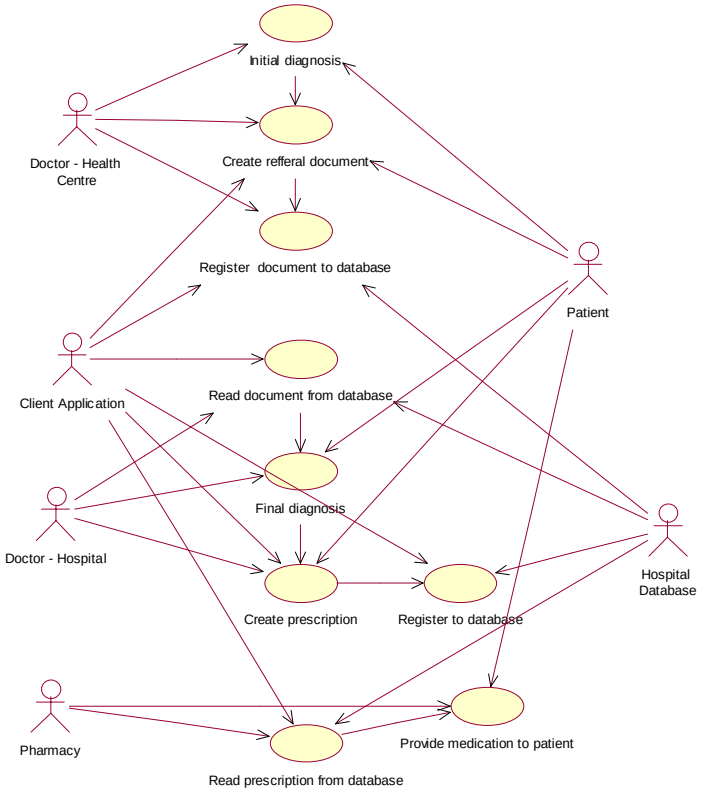

Fig. 2. Use case diagram for e-referral / e-prescription application.

Based on Fig. 2, a possible scenario of use of the e-referral / e-prescription application is as follows:

1) A patient visits one of the Region's Health Centres due to a sudden healthcare problem or disorder. The local doctor examines the symptoms, makes a first diagnosis and suggests that the patient visits the Regional Hospital for extra medical tests.
2) The HC doctor compiles a new e-referral registering the patient's personal information, the Hospital's department where the referral must be addressed, as well as the initial diagnosis, proposed therapy and required tests. Additional information may be retrieved by a patient medical record application, if available. The e-referral is automatically registered in the network's database, for use by the Hospital's doctors.

3) At the Hospital, the doctor opens the referral at the patient's arrival, reads the diagnosis formed by his/her colleague in the Health Centre and acts accordingly.
4) When a final diagnosis is made, the Hospital doctor compiles a new e-prescription document for the patient and deposits it in the database, for use by the pharmacies. If the patient wishes, the doctor may store the e-prescription on his/her PC and send it by e-mail to a specific pharmacy.
5) At the Pharmacy, the pharmacist may open the document upon the patient's request and provide the required medication.

B. *Security risks and measures*

Despite the flexibility and openness of the above scenario, electronic documents communication introduces some serious security risks, which should be fulfilled in order for this healthcare application to reach the required level of user acceptance. Table I summarizes the main risks, together with the relevant security needs and measures that must be taken for facing them [11].

TABLE I
SECURITY RISKS, NEEDS AND MEASURES FOR THE E-REFERRAL /E-PRESCRIPTION BUSINESS FLOW

No	Security risks	Security needs	Security measures
1	Unauthorized access to e-referral/prescription documents	Strong authentication	Digital signature mechanisms Smart cards
2	Forgery of e-referrals /prescriptions documents	Integrity Non-repudiation	Digital signature mechanisms
3	Exposal of confidential/secret information	Confidentiality	Encryption mechanisms
4	Unauthorized access to the communication channel	Confidentiality Integrity	Secure network protocols (SSL)
5	Denial of date/time of e-documents creation/sending	Proof of date/time	Time-stamping mechanisms

As shown in Table I, access to the client applications should be restricted only to the authorized persons. Usernames and passwords are not sufficient for such an operation, since they can easily be broken, revealed or lost. Strong authentication is thus required with the use of cryptographic mechanisms and secure private tokens like smart cards.

Moreover, there must be a clear proof that a document was actually created by the specified doctor; otherwise it would be possible for unauthorized persons to create invalid referrals and fake drug prescriptions using the doctor's name. Therefore, digital signature mechanisms should be incorporated into the client applications to ensure document integrity and non-repudiation.

In certain cases, confidential information may need to be transferred between two network users (like for example information about an AIDS patient). For this reason, there must be a possibility to encrypt the document's data using cryptographic mechanisms, so that no one else except the receiver is able to read it.

The network communication should be encrypted as well, so as to disable eavesdroppers to get in the channel and destroy, modify or read data without authorization. Therefore, encryption of network channels using secure protocols like SSL is essential.

Last, it is necessary to register the date and time of the document's creation, as the doctor's proof of in-time diagnosis and treatment for a certain patient. Data time stamping is thus required.

Following Table I, all the security needs can be covered at the application level using cryptographic modules, like digital signature and encryption. In order to support these modules, however, the required PKI framework should be available, offering the underlying TTP services like registration, certification, directory and time-stamping.

The setup of the above PKI framework must be in line with the existing e-referral/e-prescription business flow and, therefore, the security integration must be done in accordance with all the technical, organizational, legal/regulatory, medical and business parameters involved in the RHIN operation. In other words, the PKI–based security of electronic documents communication must follow a best practice approach, driven by the technical characteristics, as well as the existing organizational structures and user needs of the network. This process is explicitly described in the next Section.

III. SECURITY INTEGRATION AND BEST PRACTICE ASSESSMENT

In the previous Sections we described the security needs of the e-referral/e-prescription business flow in Central Macedonia and we identified PKI as the appropriate framework for providing the required security measures.

Therefore, in the current 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). In each case, the adopted solution is described, together with its assessment, as well as relevant open issues and recommendations that should be taken into account in the future.

A. *Technical Implementation*

This part presents the technical integration of security mechanisms in the e-referral/e-prescription communication flow described in Section II, which provides PKI-aware functionality in the overall healthcare network.

1) *Needs and requirements*

The technical solution for the e-referral/e-prescription business case should address the basic security needs outlined in Section II.B (strong authentication, integrity, non-repudiation, confidentiality, time and date stamping). Moreover, the implementation should have the following characteristics:

1) Based on mature and proven technologies.
2) Extensible and scalable (so as to include additional document types or security services in the future).
3) Standards-based (both for the data representation and the security mechanisms).
4) Interoperable with similar infrastructures nationally and across Europe.

The next paragraph presents the adopted technical solution, explaining how the above requirements were fulfilled.

2) Adopted solution and assessment

Fig. 3 depicts the RHIN security architecture, which comprises three main components [9]:

1) The regional PKI, offering Registration, Certification, Directory and Time stamping services [12]. The organizational structure of this PKI is described in paragraph Section III.B.
2) The security enhanced Database server in the regional Hospital for storage of XML digitally signed and time-stamped documents (referrals and prescriptions) over SSL.
3) PKI-aware JAVA clients at the application level (e-referral /e-prescription clients), running at each user terminal in the network nodes (Hospital, Health Centres, Infirmaries, Pharmacies) and providing secure referral and prescription documents communication with the central database. XML technology is at the core of the security services integration. Smart cards are used for secure key storage and increased user mobility [13][14][15].

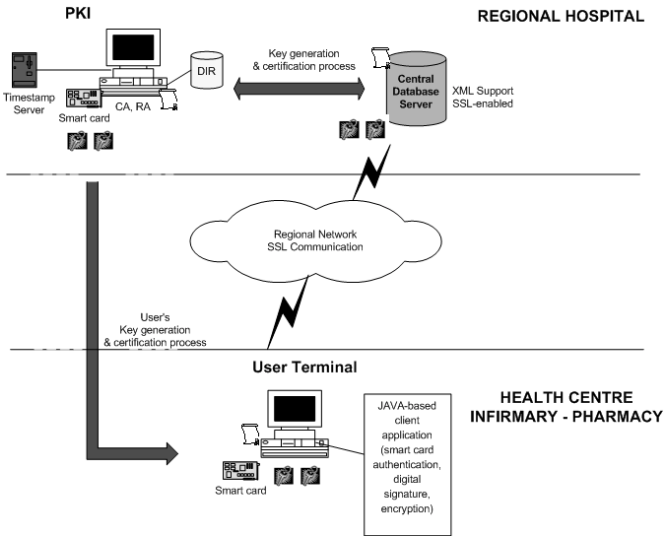

Fig. 3. Overall security architecture for the e-referral/e-prescription business case.

The PKI-aware client applications include functionality of composition/storage – retrieval/view of e-referrals and e-prescriptions, as described in Section II. However, now the clients have embedded security functionality in the existing process, based on the security measures of Section II.B. In particular, the security functionality includes:

1) Strong user authentication, document integrity and non-repudiation using digital signature mechanisms and smart cards.
2) Confidentiality of document content using asymmetric and symmetric encryption mechanisms and smart cards.
3) Document time stamping.
4) Valid transfer of (digitally signed, time-stamped and encrypted) documents.
5) Secure data transfer over the SSL protocol for mutual client/server authentication and encryption.
6) Secure data storage / documentation.
7) Secure key storage and enhanced portability and flexibility using smart cards.

All security mechanisms are implemented at the XML level, using relevant standards like the W3C Digital Signature and Encryption standards [16][17][18].

The above PKI-aware technical solution was evaluated against pre-defined test cases and found smoothly integrated within the existing network infrastructure [11].

In general terms, the proposed security architecture and service provision are based on a flexible, standards based and extensible technical scheme, applicable for several different healthcare document types besides referrals and prescriptions, or any other type of healthcare information, which can be described in a structured way (like electronic patient records). Moreover, the use of XML enables easy integration of additional security services in the same application, like for example role based authorization to network resources through the definition of distinct authorization levels (doctors, nurses, healthcare personnel, etc).

In terms of interoperability, the XML open structure enables inter operation between different healthcare networks and applications, since secure information is communicated via standard based representation formats, rather than dedicated systems and mechanisms. Furthermore, the security-enhanced application itself has been designed in JAVA, so it is platform independent and can easily be transformed into an Internet application or applet to be used by broader user communities.

3) Technical problems and recommendations

Smart card integration was initially hard to implement due to lack of relevant cryptographic service providers and APIs supporting the Java language. Other technical problems were the Greek language representation in XML, as well as the conflicts between the different cryptographic providers in JAVA.

Some areas for further implementations, which were identified, include the integration of new types of healthcare documents in the application, the implementation of new security services like role based authorization using XML based schemes, as well as the transformation of the application to an Internet based solution, in order to include more users and get the patients actively involved in the healthcare electronic communication process [9][11].

B. Organizational structure

So far we have described the technical PKI integration within the e-referral/e-prescription business flow. In this Section the organizational PKI structure is presented, since this forms the basic prerequisite for the application of the overall security solution.

1) Needs and requirements

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.

For a flexible PKI establishment, the organizational structure should:

1) Built according to the existing structures and use cases of the RHIN, which in our case form the business flows of the e-referral/e-prescription application.
2) Distribute the several PKI-related roles in a feasible and pragmatic way.
3) Define a clear organizational tree with specific rights and obligations for all participants.
4) Define a clear Application Policy for the specific business flows of the network (e-referral/e-prescription application).
5) Define one or more Certificate Policies (CP), according to the healthcare users needs, as well as a concrete Certification Practice Statement (CPS) implementing the CPs.

Following the above requirements, the PKI organizational structure for the RHIN of Central Macedonia was adopted.

2) Adopted solution and assessment

The organizational structure for the RHIN we are examining is shown in the Fig. 4.

The proposed PKI structured is based on a distributed approach, where all PKI services except Registration (i.e. Certification, Directory, Time-stamping) are outsourced to an external accredited Trusted Third Party, whereas Registration is managed by the Regional Hospital. Key generation is done locally at the users terminals, in co-operation with the external Certification Authority (CA), as well as a Smart Card Issuing System [9].

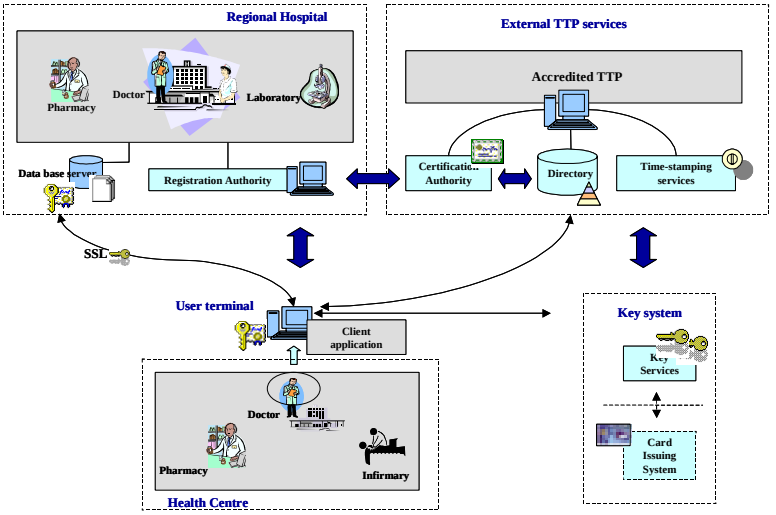

Fig. 4. Organizational structure for the Regional Healthcare Information Network.

The reason for selecting the above approach is that it avoids loading the healthcare network with dedicated TTP services, which require much expertise, efforts and costs, keeping at the same time balance with the users though the Hospital-based Registration service. In this way, the existing RHIN structure is followed, involving the PKI processes as part of the e-referral/e-prescription business flow for the healthcare participants.

More specifically, the network users now are aware that, in order to use the e-referral/e-prescription application, they must first go through the Registration process with the Regional Hospital, obtain a key pair and certificate and install them in their PC for the security measures implementation. All the PKI-related and security-related procedures are described in detail in e-referral/e-prescription Application Policy, which should be accepted and followed by all the involved healthcare participants [9].

With regard to the Certification service itself, a CPS should be defined based on one or more CPs with specific user requirements for the certificate profile. In the proposed scheme, CPS should be provided as a service of the external (accredited) CA, including specific provisions for the Hospital Registration Authority. This, however, is still an open issue for Greece, due to regulatory restrictions, which are described in more detail in the next paragraph. In any case, for the CPS development we support the IEFT RFC2527 Standard [19], taking also into account dedicated healthcare –related attributes, e.g. ISO 17090 Standard or other relevant specifications [20][21].

3) Open issues and recommendations

The main organizational open issue in the Central Macedonia healthcare network is the lack of accredited CAs in Greece for the implementation of the external TTP services, which are thus provided as pilot implementation with the support of research institutions. This is, however, expected to change soon, through the establishment of the necessary

regulatory framework from the National Authority of Telecommunications and Post, which is appointed as the Supervisory Authority under the Presidential Decree on Electronic Signatures [22]. Similar situations exist today in other European countries as well [23].

Additionally, although not always an open issue, the political support for the PKI integration in the healthcare network must be assured, since this is the basic driver for any important organizational change.

C. Legal compliance

Liability of healthcare networks is of major importance, since personal information is involved. In the following paragraphs, we describe how legal issues were addressed in the specific e-referral/e-prescription security business case.

1) Needs and requirements

Greece has already transposed the EC Directives on data protection into national law, as well as the EC Directive on electronic signatures. Therefore, from a legal perspective, the basic requirements for PKI integration concern the provision of all the required measures for compliance with the above basic laws.

2) Adopted solution and assessment

The technical solution and the organizational structure described in Sections III.A and III.B are completely aware of the requirements laid down by the Data Protection legislation, as well as the e-signature law provisions.

With regard to data protection, for instance, access to patient data is granted after prior patient consent, whereas only medical personnel may have access to the medical data, as well as the system administrator employed by the Regional Hospital and thus subject to confidentiality rules, according to the rules for civil servants. These issues are clearly set in the e-referral/e-prescription Application Policy. Moreover, the communication of data is encrypted in order to ensure data confidentiality, availability, integrity and non-repudiation and to prevent the telecommunication service provider from getting in the line [10].

Concerning e-signature, the relevant Presidential Decree was released in Greece 2001, but still, as mentioned in section III.B.3, the necessary technical and organizational specifications for the set up and operation of CAs have not been provided, thus leading to certain gaps and ambiguities. Nevertheless, the current implementation is prepared to comply with the requirements of the Directive on Electronic Signatures as soon as they are explicitly set, taking also into account the experience in the other Member States, like for example in Germany [22][23].

3) Open issues and recommendations

The main open legal issue is the elaboration of the existing Presidential Decree on Electronic Signature by the relevant Greek Regulatory Authority (as mentioned in Section II.C). Moreover, additional legal requirements for healthcare data security may be set.

Last, the proposed security solution grants access to patient entire medical record and, thus, is not health professional role aware. This does not affect the current e-referral/e-prescription business flow, but could be considered at a later step.

D. Healthcare participants involvement

In the previous Sections we described the e-referral/e-prescription PKI-based security solution, 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. In the following we show how this was performed in the RHIN of Central Macedonia

1) Needs and requirements

The basic needs for an accepted and feasible PKI establishment, in terms of medical involvement are to:

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) User involvement and assessment

In order to address the above –mentioned needs, PKI security was integrated in the existing system business flows and extensive user education and training was performed. 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 e-referral/e-prescription application and trained to its use [10].

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 has 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. Last, the survey assessed the security-enhanced e-referral/e-prescription application as part of the regular document communication process in the Regional Healthcare Information Network.

Some of the main outcomes of the medical user survey are outlined as follows [10]:

1) There are three major IT related tasks performed by the medical practitioners and these are input of self-recorded data, external and internal data transfer and evaluation and analysis of medical data. Therefore, security is basically considered around these operations.
2) In general the Greek healthcare participants have very little experience with security related features, but they are very positive towards integrating such functionality in their everyday work. Nevertheless, upper level management user groups also gave indications that they consider security-enhanced telemedicine applications make working with computers more complicated.

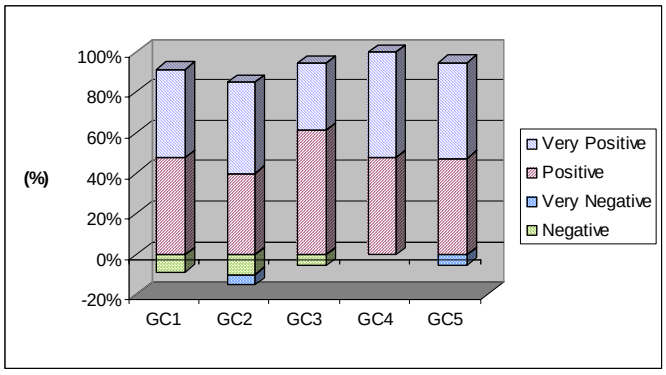

Fig. 5. Assessment results for IT and Security Mechanisms
The horizontal ax in represents categories of IT and security mechanisms in the following way:
GC1: Computers and networks in general;
GC2: Computer security and electronic medical data;
GC3: Patient rights consolidation;
GC4: Digital signatures and cryptography;
GC5: Smart card use

Figure 5 shows the attitude of healthcare participants towards different categories of IT and security mechanisms (the results are qualitative in terms of percentages). So, for example, the opinion on smart card is very positive for over 50% of the medical users, whereas there is still as small percentage considering them inappropriate for healthcare related work.

3) Another important point is that medical practitioners do not get frequently informed about security related policies and legal issues involved, much less for PKI, and their importance. This has an impact on their confidence towards security related operations and therefore limits their involvement. An example that supports this conclusion is that a large percentage of users do not have a problem to share their password or PIN.
4) The acceptance of the security enhanced e-referral/e-prescription business case was generally good as far as the concept and security mechanisms are concerned, but there were still comments on the characteristics of the application itself (more user friendly operations). Fig. 6 presents the opinion of medical staff towards different aspects of the security-enhanced system (the results are qualitative in terms of percentages).

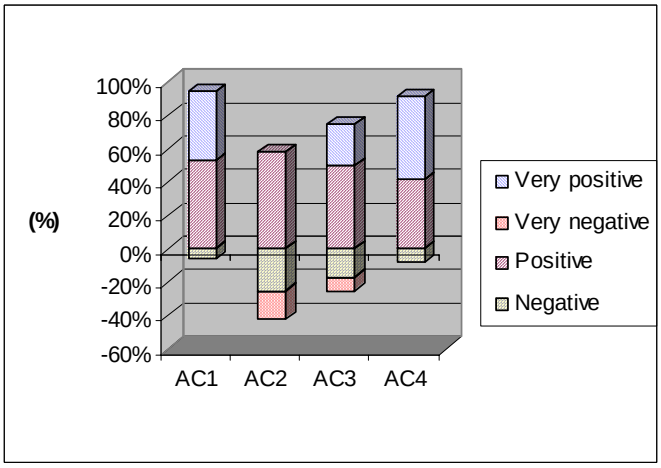

Fig. 6. Assessment results for the security enhanced e-referral/e-prescription application. The horizontal ax represents different aspects of the application in the following way:
AC1: Application idea and general concept;
AC2: Generic application functionality;
AC3: Application functionality in terms of security (digital signatures, cryptography etc.);
AC4: Smart cards integration.

It should be mentioned that both Fig. 5 and 6 represent generalizations of the actual survey findings and their purpose is to give the overall impression for categories of interest, for example the attitude towards smart cards.

3) Open issues and recommendations

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) Regular education of the medical personnel in security aspects, policies and legal issues addressed.
2) Involvement of the healthcare participants in all stages of the implementation process.
3) Commitment of the healthcare participants via clearly defined Application policies.

Especially in Greece the current status still is far behind progress, and therefore the effort has to increase.

E. Business perspective

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.

1) Needs and requirements

For the Regional Healthcare Network the PKI business-related issues concern the increase of healthcare service quality (due to security enhanced operations), 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 (technical developers, PKI providers), the main business case 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 fulfill 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.

As shown in the next paragraph, the current implementation is aware of most of the above criteria.

2) Business positioning and assessment

The PKI-based security for e-referrals/e-prescriptions, as described in 3.3, is integrated in the RHIN of Central Macedonia as part of the existing business processes, whereas the dedicated TTP services are outsourced. This provides a feasible implementation, which does not interact with the existing medical services and at the same time it is strongly engaging all involved healthcare participants via a concrete Application Policy.

Moreover, the PKI organization follows the structure of the Greek Regional Healthcare Systems, which is based on a decentralized approach of healthcare service provision in the country, as well as the current Greek market trends for secure XML, digital signature, time stamping and TTPs [24].

In this way, the proposed technical and organizational solution is within the existing plans and perspectives of the Greek market and thus further extension to other regional networks in the country can be expected.

Despite this fact, however, there are still bottlenecks and open issues with regard to the business plan formation, due to the lack of legal framework, as well as the lack of security-related education in the Greek healthcare sector. This is further described in the next paragraph.

3) Open issues and recommendations

Some important open issues/recommendations arising for the business assessment in Central Macedonia are outlined as follows:

1) Security is generally deemed necessary but in certain cases the upper management of regional healthcare networks is considering it as a deterring factor due to extra costs. Therefore, threat analysis and risk assessment need to be integrated as business factors like for example book keeping, taxation etc.
2) Another setback in security adoption is the competition of security services for resources currently distributed among other kinds of business requirements such as workflow, performance, efficiency etc. This is sometimes considered as threat to regular business processes and, therefore, all the required recourses like hardware, internet access and e-mail have to be available before the adoption of the PKI based security solution.
3) Training of healthcare participants and involvement in the process is very important, in order to setup successfully the new infrastructure procedures.
4) Analyzing the costs for setting up and maintaining either a PKI-based security solution for a healthcare organization needs to take into account certain specifications for the accreditation scheme that will be adopted in the Greek law. As already mentioned, the full set of specs has not been provided yet and, thus, there is still gap in the formation of security-oriented business plans.

The above points are expected to be covered in the future through the elaboration of the Greek Digital Signature law, as well as the identification of security as a major infrastructure need of the electronic healthcare communication.

IV. Conclusions and Further Actions

The paper presents a best-practice application and assessment of PKI-based security within the business process of an existing Regional Healthcare Information in Greece. More specifically, the security integration is examined for the electronic communication of patient referrals and prescription documents, through a specific healthcare application, namely the e-referral/e-prescription application.

Due to the best practice nature of the work performed, security is examined towards a number of different parameters, i.e. technical, organizational, legal, medical and business. Table II presents the needs, adopted solution and assessment per each different parameter, including also existing open issues and/or recommendations.

TABLE II
BEST PRACTICE APPLICATION AND ASSESSMENT OF PKI-BASED SECURITY

Best practice parameters	PKI-based security			
	Needs	Adopted solution	Assessment	Open issues
Technical	• PKI-aware. • Mature and proven technologies. • Extensible and scalable. • Standards-based. • Interoperable.	• JAVA security • XML data representation and security (W3C). • SSL communication.	• Smooth RHIN integration. • Applicable for any structured h/c data. • Easy integration of new security services. • Open structure, web compliant, standard based.	• Smart card integration in JAVA. • Compatibility of crypto-providers.
Organiza-tional	• Feasible PKI scheme & roles definition. • Application Policy. • CP and CPS.	• Distributed PKI scheme. • External accredited CA • User-driven key services • CP according to RFC2527.	• Flexible and feasible solution. • Organization follows the existing RHIN operations.	• Lack of regulatory framework for accredited CAs. • Need for political support.
Legal	Compliance with existing Data Protection E-signature laws.	• Aware of Data Protection law (patient consent, information confidentiality, rights definition). • Prepared to comply with e-signature law.		• Gaps in e-signature law. • Healthcare prof. roles integration.
Medical	• Address real medical needs. • Commit users from start. • Guarantee medical involvement. • Mature & realistic scheme.	• User training and education. • . • User survey based on questionnaires	• Very little user experience but positive attitude towards security (e.g. smart cards). • Lack of security-related information (legal issues, policies). • Good acceptance of the PKI enhanced business flow.	• User education and training. • Involvement of users in the development process. • Clear application policy.
Business	• Integrate security in existing business flows. • Define business perspectives within healthcare plans. • Adopt the underlying legal/regulatory framework.	• PKI establishment was done according to the e-referral/e-prescription business case. • Follows the Greek Regional Healthcare Systems concept. • Follows the plans of the National Healthcare System.	• Integrate security as real business factor. • Provide all the required recourses. • Training and education of healthcare participants. • Lack of regulatory framework for CA accreditation	• Integrate security in existing business flows. • Define business perspectives within healthcare plans. • Adopt the underlying legal/regulatory framework.

As shown in the Table, the technical solution is based on XML security and is characterized as flexible, standards-based, extensible and interoperable.

With regard to the organizational PKI structure, the distributed approach was selected, outsourcing all the TTP services except Registration to an external authority and keeping user Registration within the Regional Hospital. An Application Policy is setting the main use cases for the security enhanced e-referral/e-prescription application. Moreover, from a legal perspective, the adopted solution is aware of both the Data Protection and Electronic Signature Laws.

In terms of healthcare participants involvement extensive training took place, together with a detailed user survey. According to this assessment, medical users have very little experience and law education on security, but still they are very positive towards the security concepts and are interested in integrating them in their everyday work. In this respect, there is also a positive attitude towards the security –enhanced e-referral/e-prescription business flow.

Last, from a business point of view, the adopted solution is in line with the current network processes, as well as with the overall Greek Regional Healthcare Systems concept and, thus, it has many possibilities of success in other Regions of the country.

As far as further actions are concerned, an important issue for the deployment of PKI-based security is the technical and organizational elaboration of the Greek Electronic Signature law, which is expected to come soon from the relevant Regulatory Authority. Moreover, user education and training is essential, as well as the integration of security as a new mandatory part of the business processes in new and existing Regional Healthcare Information Networks.

ACKNOWLEDGMENT

The authors would like to thank the RESHEN partners for reviewing this paper.

REFERENCES

[1] *Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*, CCITT Rec. X.509 | ISO/IEC Standard 9594-8, 1994.

[2] *Information Technology – Security techniques – Non repudiation – Part 1: General*, JTC1/SC27 | ISO/IEC Standard 13888-1, 1997.

[3] B. Blobel, *Analysis, Design and Implementation of secure and Interoperable Distributed Health Information Systems*. Amsterdam, NL: IOS Press, 2002.

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

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

[6] 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

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

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

[9] 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

[10] 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

[11] 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.

[12] *UNICERT 3.5.1 Documentation*, BALTIMORE TECHNOLOGIES, Dublin, IE, 2002. Available: http://www.baltimore.com.

[13] *Extensible Markup Language (XML) 1.0*, W3C Recommendation, 1998. Available: http://www.w3.org/TR/1998/REC-xml-19980210

[14] *JBUILDER 5 Documentation*, BORLAND, Scotts Valley, US, 2000. Available: http://www.borland.com

[15] *IBM XML SECURITY SUITE*, IBM, New York, US, 2002. Available: http://www.alphaworks.ibm.com

[16] *XML-Signature Syntax and Processing*, IETF RFC Standard 3075, 2001. Available: http://www.ietf.org/rfc/rfc3075.txt

[17] *XML Encryption Syntax and Processing*, W3C Candidate Recommendation, 2002. Available: http://www.w3.org/TR/xmlenc-core/

[18] *IAIK JCE 3.0*, Graz University of Technology, Graz, AT, 2002. Available: http://jcewww.iaik.tu-graz.ac.at/products/jce

[19] *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, IEFT RFC Standard 2527, 1999. Available: http://www.ieft.org/rfc/rfc2527.txt

[20] *Healthcare Informatics – Public Key Infrastructure*, ISO TS 17090 Parts 1-3, 2001.

[21] A. Bourka, "Advanced Public Key Infrastructure services for Healthcare: Development of secure application for e-healthcare documents communication – Implementation of prototype method for automated Certificate Policies compatibility assessment", Ph.D. dissertation, Department of Electrical and Computer Engineering, National Technical University of Athens, Athens, GR, 2002. Available: http://www.biomed.ntua.gr

[22] 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

[23] 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

[24] Greek Government, "Improvement and modernization of the National Health System, Chapter A: Regional Healthcare Systems, *Official Journal of the Government of the Greek Democracy*, Journal No. 37, 2001.