MEDINFO 2001
V. Patel et al. (Eds)
Amsterdam: IOS Press

An Overview in Healthcare Information Systems Security

Athena Bourka [a], Nineta Polemi [b], Dimitris Koutsouris [a]

[a] *Biomedical Engineering Laboratory, Department of Electrical and Computer Engineering, NTUA, Athens, Greece.*
[b] *Institute of Communication and Computer Systems (ICCS), NTUA, Athens, Greece*

Abstract

The scope of this paper is to present the current needs and trends in the field of healthcare systems security. The approach applied within the described review was based on three major steps. The first step was to define the point and ways of penetration and integration of security services in current healthcare related applications addressing technical, organisational and legal/regulatory issues. The second step was to specify and evaluate common security technologies applied in healthcare information systems pointing out gaps and efficient solutions, whereas the third was to draw conclusions for the present conditions and identify the future trends of healthcare information security. A number of EU RTD Projects were selected, categorised, analysed and comparatively evaluated in terms of security. The technical focus was on key security technologies, like Public Key Infrastructures (PKIs) based on Trusted Third Parties (TTPs) in conjunction with other state-of-the-art security components (programming tools, data representation formats, security standards & protocols, security policies and risk assessment techniques). The experience gained within this review will provide valuable input for future security applications in the healthcare sector, solving existing problems and addressing real user needs.

Keywords:

Security; PKI; TTP; Healthcare information systems

Introduction

Healthcare information systems are constantly growing in Europe, since they significantly enhance healthcare information exchange, thus making easier the provision of healthcare services to the citizens in a more timely, efficient and cost effective way. However, electronic communication introduces some serious security problems, which, due to the complexity, sensitivity and criticality of the healthcare related data, should be handled appropriately at all possible levels. Under the term "security" in a healthcare information system, the following concepts are implied: data confidentiality, data integrity, authentication, non–repudiation, availability of information. Furthermore, the above concepts can appear in several different ways in a healthcare information system, in terms of data security (within the healthcare information system or during transmission between different systems), network security (communication channels), as well as security of applications used for data creation, presentation, maintenance and processing. During the last years Public Key Infrastructures (PKI) based on the Trusted Third Party services (TTPs) have been qualified as an appropriate means for dealing with healthcare information systems security risks, in conjunction with a variety of security components, tools and architectural schemes, especially for operation over INTERNET.

The current paper, which is based on work conducted under the HARP (Harmonization for the Security of Web Technologies and Applications) IST project [1], presents a state-of-the-art review in the field of security in the healthcare sector. The major objective of this review was to define the point and ways of penetration and integration of security services in current healthcare related applications, at technical, organisational and legal/regulatory levels, specifying and evaluating the security solutions most usually applied. Furthermore, the review aimed at identifying existing gaps and reusable security components and practices, setting the basis and providing guidance to future developments in healthcare security, driven by real user needs.

Materials and Methods

Trusted Third Party services and security technologies

Following the overall review objectives, particular focus was given on the application of proven technologies in healthcare, which have been tested and used in other sectors, as well as in emerging technologies, leading future developments. In this respect, Public Key Infrastructure technologies and INTERNET security were of considerable interest.

A TTP has been defined by ISO/IEC as a security authority or its agent trusted by users with respect to security-related activities, e.g. to support the use of digital signatures and

confidentiality services. TTPs are usually established within a Public Key Infrastructure (PKI) scheme, which operates under the public key technology principles. The core PKI security services are four: Registration, Certification, Key and Directory. In addition, some prospective value-added components of a PKI-based organisational structure are key recovery, date/time-stamping and cross-certification.

INTERNET security is comprised of a number of components, found separately or inter-related in different applications. Such components include: data representation formats and standards (e.g. XML, security-specific formats like PKCS, X.509, PGP, SPKI), application level protocols (generic protocols like LDAP, HTTP, FTP and security protocols like IPSec, SSL/TLS, SHTTP), smart cards, e-mail security (PGP/MIME, S-MIME), programming environment and JAVA security, distributed environments & platforms (CORBA, Mobile Agents, DCOM, telemedicine digital libraries).

The above issues were examined in the review together other with aspects, like security policy and legal framework in healthcare, standardisation and risk assessment.

Outcome of EU projects

The review was conducted through selection, analysis and comparative evaluation of EU RTD projects and relevant applications. First, a list with criteria for the projects' evaluation was defined. These criteria were then used for the selection, categorisation and review of a number of healthcare projects. In addition, other general TTP & security projects were also examined, aiming at the identification of common components and tools, valuable for the healthcare sector. The results of both parts of the review were summarised in tables and comparative conclusions were drawn.

Designation of specific criteria for the projects review

The following criteria were used for the projects' review, taking into account different aspects of security solutions in the healthcare sector [1]:

Technical criteria: This group concerned the technical security solutions proposed and /or implemented within each project, which in some cases are provided in terms of certain security architectures (TTP models, Hardware and Software security implementations), whereas in others they are related to technical surveys, security recommendations and requirements, risk assessment methods, etc.

Organisational criteria: This group concerned organisational structures and relevant recommendations for setting-up a PKI infrastructure, especially at a cross-border level. Aspects of CA hierarchies and cross-certification models are included.

Legal and regulatory criteria: This group concerned legal issues related to security in the healthcare sector and especially in telemedicine applications. Besides, security policy and accompanying measures were considered, as well as relevant standards developments.

Financial criteria: This group was addressed only in cases examining costs for TTP implementation and operation.

Selection, categorisation and review of healthcare projects

The projects examined in this part of the review were all dealing with security issues in the healthcare sector. Although the most specific area of interest was TTP solutions in telemedicine and INTERNET applications, other more general findings and solutions with regard to security and healthcare were provided, in order to have an overall picture of the state of the art in the above sector. As shown in the following, fifteen projects in total were finally selected for review, which were all found representative of their sector in the terms defined above. The projects were grouped in five sub-categories, according to their specific security objectives: a) TTPs in Healthcare: THIS [2], TRUSTHEALTH [3], EUROMED-ETS [4], OPARATE [11], EUROTRUST [11] and TRUSTWEB [11], b) Security in healthcare information networks: INTRACLINIC [5] and NETLINK [6], c) Horizontal healthcare & security aspects: ISHTAR [7], SEISMED, SIREN, MEDSEC, d) Risk assessment in telemedicine applications: VITAL-HOME [8], e) Secure communication of medical information: SEMRIC [9] and VIRTUOSO [10]. The comparative description of the above projects is shown in Table 1.

Outcomes from healthcare projects review

A first conclusion in the area of healthcare oriented TTPs is that research and application development remains rather limited and becomes even more limited when the WWW is chosen as the communication means. Only three projects were found directly focused on TTPs in the healthcare sector (THIS, TRUSTHEALTH, EUROMED-ETS) and only EUROMED-ETS developed TTPs over the WWW.

TRUSTHEALTH [3], using the outcomes of THIS [2] study, defined quite clearly the general architecture for secure communication of Healthcare Professionals (HCP) within a healthcare information network. Special attention was given to the aspects of professional registration, authorisation and certification, providing also a proposal for professional certificate based on the X.509v3 Certificate (extension of subject directory attributes). Personal HCP smart cards were a key element in the whole model. The class authentication of HCP was also examined, especially for interaction with the patients' cards. Last, the naming scheme for HCPs and the Directory structure were analysed and described. In general, the healthcare oriented TTP model proposed by TRUSTHEALTH (and THIS) is quite clearly defined and could be applied in any healthcare environment where the professional authentication and certification is a key issue. However, TRUSTHEALTH did not provide any reference to the secure exchange of medical information or to issues of TTPs inter-connection.

Table 1- Healthcare projects review

Projects General description	Key Technical issues	Organisational issues	Legal/ Regulatory Financial issues
1 - THIS Requirements for ES & TTPs in healthcare.	a) Use of HCP cards b) Electronic HCP authorisation c) Class authentication for HCP, d) Directory	Hierarchical CA structure with top policy-CA	Needs for governmental decisions & EU harmonisation in healthcare TTPs
2 – TRUSTHEALTH Trustworthy healthcare systems through TTPs in Europe.	a) Healthcare oriented functional TTP model b) Use of HCP cards and professional registration c) Professional Certificate based on X.509v3, c) Hierarchical directory naming	Decentralised and centralised CA hierachies	Global security policy for all National security policies for each project participant.
3 - EUROMED-ETS TTPs on the WWW for telemedical applications	a) Adds security components on existing distributed network (EUROMED) b) Certification authority and Directory operating via WWW (TCP/IP) c) Scenarios for secure messaging on WEB	Two different CA schemes can be applied: decentralised – centralised.	Overview of existing laws and recommendations.
4 - OPARATE Horizontal architectural & organisational TTP aspects	a) Definition of a set of TTPs roles b) Architectural framework for interoperable TTPs, c) Field trial (network of 3 TTPs)	National TTP hierarchies & cross certificate	a) Definition of legal crietria for TTP operation b) Financial TTP estimations
5 - EUROTRUST Pan-European CA services	a) Secure e-mail (MailSecure plug-in) b) Secure web browsing (UniCert)	Pan-European CA-hierarchy	Overview of existing laws and recommendations.
6 -TRUSTWEB Review of WWW status with respect to ETS	a)Time stamping, data certification and non-repudiation services for WWW posting and origin/delivery of filled forms, c) Signed code	Proposals for CA cross-certification	
7 - INTRACLINIC Intranet Health Clinic	Security at four levels: Firewall, SSL, S/MIME & PGP for secure e-mail, encryption and digital signatures in XML documents.		Overview of existing laws and recommendations.
8 - NETLINLK Recommendations for interoperable healthcare information systems in Europe	a) Scenarios for interoperability in secure: access to patient data card (free + protected), messaging, database access, procedure simplification, b) Recommendations for technical components involved in scenarios		Overview of standards, EU/G7 interoperability dataset (description, proposals for modifications)
9 – ISHTAR Horizontal aspects of healthcare information security	a) Overview of threats and corresponding solutions for healthcare information systems –Extraction of security requirements b) Healthcare Incident Reporting Scheme		a) Healthcare security guidelines (SEISMED) b) Legal reports, especially for telemedicine
10 – SEISMED Security guidelines for the healthcare sector			Healthcare security guidelines (published by IOS Press) – The SEISMED guidelines
11 – SIREN accompanying measure for healthcare security	a) Combination of existing results in the field of healthcare security and TTPs b) Training material and dissemination events		
12 – MEDSEC Standards for security in healthcare systems			Taxonomy, promotion and identification of gaps in healthcare security standards.
13 - VITAL-HOME Vital signs telemonitoring	CRAMM methodology – Risk assessment		a) Overview of legal framework , b) Security policy
14 – SEMRIC Secure communication of medical record information	Medical record transfer at message & object level (for EDIFACT, ASN.1, SGML) – Standard based methodology (PKCS#7, SSL).		Pre-standardisation activity for the secure communication of medical record information.
15 – VIRTUOSO Visual simulation and treatment in radiooncology	Access control system & encryption used as security mechanisms.		Recommendations for security policy.

EUROMED-ETS [4], on the other hand, did not provide any specific framework for the professional authorisation and certification, but focused on the exchange of medical information and data over the WWW, based on an existing telemedicine platform (EUROMED). In this way, the project demonstrated the possibility of adding security components (via a TTP development) in existing networks operating over the WWW, in order to serve specific medical scenarios where secure communication is needed.

As far as the TTP organisational structure is concerned, THIS proposed an hierarchical structure with a policy CA on top of all CAs, while TRUSTHEALTH examined the advantages and disadvantages of decentalised and centralised CA structures. Cross certification was also considered. The same approach was used in EUROMED-ETS as well, the basic conclusion being that both schemes are possible to implement but a global CA policy should initially be established.

Taking into account the above points, the following observation is made: TRUSTHEALTH & THIS and EUROMED-ETS are addressing different aspects of healthcare oriented TTPs and, in this respect, they could probably complement each other in an overall TTP architecture development. This should be considered in future applications, where secure transactions of medical data over the WWW is a key issue, but the HCP certification and role based authentication are also crucial.

In addition to the above three major TTP projects, the projects OPARATE, EUROTRUST and TRUSTWEB were considered in the review, although not directly healthcare oriented, since healthcare was mentioned as their possible application domain. OPARATE proposed recommendations for building interoperable TTP architectures, examining also financial issues. EUROTRUST suggested a pan European TTP trust model over the WWW, addressing aspects of cross certification. Last, TRUSTWEB covered aspects of TTPs on the WWW, including issues of signed code, data certification and non-repudiation services for WWW posting and origin/delivery of signed forms [11].

Some other security solutions, besides TTPs, which, according to the review, seem to be common practice in healthcare are: Firewall technology (INTRACLINIC); SSL protocol for security at the transport level (EUROMED-ETS, INTRACLINIC, NETLINK, SEMRIC); S/MIME, PGP for secure e-mail transactions (INTRACLINIC, NETLINK, ISHTAR); Data encryption – decryption (INTRACLINIC, NETLINK, SEMRIC, VIRTUOSO); Use of XML for secure data communication (INTRACLINIC); Secure communication of medical records at message and object level and in different message formats (SEMRIC); Interoperability issues in different scenarios of medical information exchange: free & protected access to patient data card, secure messaging, database access (NETLINK); Healthcare Incident Reporting Scheme (ISHTAR); Risk assessment in healthcare environments using CRAMM methodology (VITAL-HOME).

Regulatory and legal issues are also crucial in healthcare security. SEISMED and ISHTAR projects defined a detailed security policy for users, healthcare managers and technical staff. This policy has been used in other projects as well and has been published under IOS press as healthcare security guidelines. Besides this, most reviewed projects provided an overview of existing legal and regulatory framework in the field of healthcare security. The needs for European harmonisation and for governmental decisions in this field are outlined. Security standards for healthcare are also important. MEDSEC made an overview in existing standards, while SEMRIC was itself a pre-standardisation activity for the secure medical record communication.

Outcome from general TTP security projects

In parallel with the healthcare projects review, general TTP projects (non-healthcare related) were also examined, especially those conducted under the framework of the DGXIII INFOSEC Programme on European Trusted Services [11]. From the analysis of these projects, an important outcome is the need for TTPs inter-connection and inter-working in Europe. According to the ETS Evaluation study, only EUROTRUST and OSCAR provided a functional network of TTPs and this subject is still open for further research and developments. Furthermore, added value services are crucial, like key management (KRISIS, EAGLE) and time-stamping (OSCAR, PKITS). Legal TTP aspects are also pending (AEQUITAS, LEGAL), as well as business and commercial TTP analysis (BESTS, SEDUCER, COMETS). Last, it should be mentioned that most ETS projects provided pilot implementations of certain services; this experience could be useful for new TTP infrastructures.

Results - Discussion

A first result from the projects' evaluation is that the field of security in telemedicine applications over the WWW is still open for research and development in Europe. New solutions and new services should be defined, in order to be in line with the current user needs, as well as with the current market and business trends. At the moment, the most direct TTP and healthcare related projects are TRUSTHEALTH and EUROMED-ETS; their results could be combined providing healthcare professional registration and role based authentication, as well as secure medical data communication over the WWW.

A second result is that there is currently a lack of functional pan-European TTP implementations and TTPs inter-working over national borders remains a crucial issue. TTPs architectural interoperability can fill this gap, as well as compatibility with existing standards. In a pan-European framework, national TTP hierarchies and cross-certification at European level seems to be the best organisational scheme, in order to be compatible with national laws and restrictions in the field of security.

Furthermore, new TTP (added value) services are becoming more and more important in medical networks, including, among other, signed code, non-repudiation services for WWW posting and for origin/delivery of filled forms, time-

stamping. This is related with the use of WWW related formats (XML, JAVA) for the exchange of medical information. Smart cards are also emerging as a major added value service for strong authentication and medical data storage. This is in accordance with the e-Europe smart cards and Health on-line initiative of the European Commission.

Besides technical aspects, policy development is quite crucial for the security in healthcare information networks. The SEISMED and ISHTAR guidelines can provide a starting point for defining an overall security policy. Risk assessment seems to be a common practice in defining security threats and corresponding solutions in healthcare environments. CRAMM methodology and CC Tool are possible ways to perform such assessments. Besides, incidents reporting schemes can also be used for determination of possible threats and for the prevention of security "holes". Last, but not least legal and operational TTP aspects (ex. costs) should not be underestimated, since they actually set the institutional and organisational framework for the application of technical solutions.

The above results are indicative of the needs and requirements for healthcare security. Such requirements involve: TTP interoperability and inter-working over national borders, pan-European PKI architectural structures, new (added value) TTP services for WWW implementations, utilisation of WWW related documents formats for the exchange of medical information, policy development, standards compatibility, definition of legal and operational TTP aspects (ex. costs).

Conclusions

The aim of the review presented in this paper was to identify and evaluate existing EU projects on TTPs and security in the healthcare sector, in order to define the state of the art of research and application development in this field in Europe. In the course of this exercise, 15 healthcare related projects were examined, according to pre-defined criteria (technical, organisational, legal & regulatory and financial). The projects were all representative of the current work (in terms of security) conducted so far in Europe and were grouped in categories, according to their specific objectives and scopes. Besides, non-healthcare oriented TTP projects were reviewed, in order to identify generic results that could be applied also in healthcare. The experience gained through this review will enable the development and implementation of new applications and tools for healthcare security, covering existing needs and requirements and contributing to further technical and organisational enhancement of the healthcare information systems.

Acknowledgements

The authors would like to thank the European Commission for supporting the HARP project, leading to the overview in this paper. We would also like to thank the HARP partners for reviewing this paper.

References

[1] HARP Project, Deliverable D.2.2. *State of the art review of security technologies in the telemedicine.* Athens: NTUA, 2000.

[2] THIS Project, Final Deliverable, Part 2. *Trusted Third Party Services.* Stockholm: SPRI, 1995.

[3] TRUSTHEALTH Project, Deliverable D.4.1. *Functional Specification of TTP Services.* Stockholm: SPRI, 1996.

[4] EUROMED-ETS Project, Final Report. *Trusted Third Party Services for Healthcare in Europe.* Athens: ICCS-NTUA, 1998.

[5] INTRACLINIC Project, Deliverable WP06, Part 3. *Guidelines for the development of a high-level security policy and a database security policy for IHC.* Thessaloniki: AUTH, 1999.

[6] NETLINK Project, Deliverable D.2.2. *NETLINK Requirements for Interoperability,* 1999.

[7] ISHTAR Project, Deliverable D09. *Current Security Issues Faced by Healthcare Establishments.* Magdeburg: UHM, 1997.

[8] VITAL-Home Project, Deliverable D3. *Technical, legal and regulatory framework for implementing a secure VITAL-Home pilot.* Athens: AUEB, 1999.

[9] SEMRIC Project, Deliverable D6.4. *Conclusions on the Methodology Development – General object security methodology and conclusions on syntax specific development,* 1998.

[10] VIRTUOSO Project, Deliverable D3.1, *Report on Data Security Requirements.* Athens: NTUA, 1998.

[11] P. Heider, H. Nilsson, D. Pinkas, *Evaluation of the European Trusted Services Programme*, 1999.

Address of correspondence

Athena Bourka, Biomedical Engineering Laboratory, Department of Electrical and Computer Engineering, National Technical University of Athens, 9 Iroon Polytechniou, 15773, Athens, Greece, Tel: +30 1 7722430, E-mail: abourka@biomed.ntua.gr