5

The Need and Practice of User Authentication and TTP Services in Distributed Health Information Systems

BERND BLOBEL, PETER PHAROW
Institute for Biometrics and Medical Informatics, Otto-von-Guericke University Magdeburg, Leipziger Str. 44, D-39120 Magdeburg, Germany.
E-Mail: Bernd.Blobel@MRZ.Uni-Magdeburg.DE

Key words: Security services; Security mechanisms; Smart cards; Trusted Third Party

Abstract: Shared care requires open distributed information systems for supporting communication and co-operation. Regarding the sensitive character of personal medical information, such communication and co-operation must be provided securely. Meeting the European as well as national legislation, several projects such as ISHTAR, TrustHealth, MEDSEC, EUROMED-ETS, and HARP have been launched by the European Commission for specifying, implementing and evaluating appropriate security solutions. Based on the mentioned projects' results, a trustworthy shared care infrastructure is discussed in the paper.

1. INTRODUCTION

The well-known changes in healthcare like specialisation and decentralisation, the need for efficiency and efficacy, but also the increased mobility of patients and health professionals, the flexibility (working in different application environments) as well as regionalisation or even internationalisation of healthcare cause a paradigm change in health to shared care. Adequate health information systems, which have to be distributed and co-operative must support shared care structures, too. Exchanging personal medical data, communication and co-operation especially in health have to be provided securely.

In Europe, the basic legal issues about security for personal and medical information are ruled in the „European Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data“ [1] and in the „European Recommendation No. R(96) of the Committee of Ministers to Member States on the Protection of Medical Data“ [2]. Based on results of several projects related to security in healthcare and funded by the European Commission, such as ISHTAR, TrustHealth, MEDSEC, EUROMED-ETS, and HARP, some security solutions for the mentioned type of systems will be discussed in the paper [3, 4].

The care of cancer patients is a long-standing example of shared care. As an integrated clinical cancer documentation system, the Clinical Cancer Register Magdeburg/Saxony-Anhalt has been the first distributed interoperable regional healthcare information system in Germany. The highly sensitive content of the Clinical Cancer Register information and our open system architecture are demanding a high level of security, reliability, and privacy of information records and communication procedures.

2. SECURITY REQUIREMENTS AND SOLUTIONS IN DISTRIBUTED MEDICAL RECORD SYSTEMS

Communication and co-operation between a large number of varying users across the boundaries of domains as departments, organisations, regions, or even countries are increasingly bearing security threats of the personal medical information collected, stored, processed, and communicated in Health Care Establishments (HCEs) [5, 6].

Security is a very complex issue related to legal, social, ethical, physical, organisational, and technological dimensions defined as security policy. In that context, security addresses human, physical, system, network, data, or other aspects. Regarding basic requirements of secure communication[1] and secure co-operation[2] in distributed systems based on networks, basic security services are required [5, 7]. These services have to provide identification and authentication, integrity, confidentiality, availability, audit, accountability (including non-repudiation), authorisation, and access control. Additionally, infrastructural services such as registration, naming, directory services, certificate handling, or key management are needed. Especially but not only in healthcare, value added services protecting human privacy rights as

[1] communication security consisting of secure connectivity and secure message transfer
[2] application security

anonymisation or providing accountability as time stamping and registration of professionals are indisputable. The services mentioned could be provided by applications or by external objects. With the growing use of complex middleware architectures such as CORBA, DCOM/ActiveX et al., this functionality will also be served by the implemented middleware. For further details see [5, 8].

The Magdeburg Medical Informatics Department is hosting and maintaining Germany's first health record system in oncology supporting different providers who are involved in cancer patients' care and belong to different organisations within the regional shared care system in oncology. Structure and functions of the Clinical Cancer Register Magdeburg/Saxony-Anhalt are described, e.g., in [9, 10].

The next sections are going to discuss some of the models used, shortly considering the services mentioned.

2.1 Security Services

For analysis and design of secure health information systems, a comprehensive set of models has been developed at beginning of the nineties which is only partially issue of this paper. The approach is based on a generic component paradigm, e.g., published in [11]. This paradigm reflects the different views according to the ISO Reference Model – Open Distributed Processing [12] as the view on the enterprise hosting the system, the view on the information managed, the view on the computational principles, the view on the engineering aspects, and finally the view on the technology used. Regarding the granularity, different levels from concepts through services, up to mechanisms and algorithms can be defined. Such a layered model is shown in figure 1. At the conceptual level, the concepts quality, safety, and security, and regarding the latter the concepts of communication security and application security can be distinguished. The basic service considering communication between principals (users, systems, applications, components, objects, etc.) is the strong mutual authentication of these principals controlling the access to the other principal. Furthermore, the principals' accountability for information communicated as well as its integrity, confidentiality, and availability must be guaranteed. Additionally, notary's services like certified time stamps have to be delivered. Regarding application security services, authorisation and accountability according to the dedicated roles of principals following the rules established in the policy have to be controlled. Furthermore, also access control to information as well as its integrity, confidentiality, and availability must be ensured. Beside notary's functions, the comprehensive and trustworthy audit is essential [5, 7].

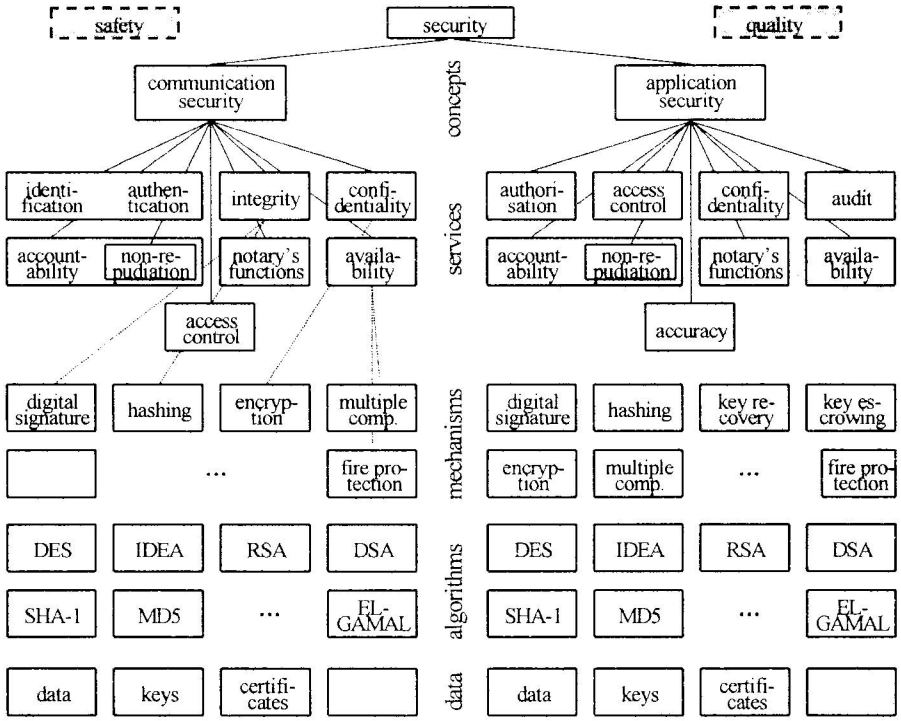

Figure 1. Layered Model of Concepts-Services-Mechanisms-Algorithms-Data Relationship

2.2 Domain Model

As information systems scale to regionally, nationally and even internationally distributed systems, their complexity has to be reduced in order to remain manageable with respect to both security specification and threat model. Collecting similar components into security domains, representing special scope to the system usually does this. Common features allowing grouping are, e.g., organisation, functionality, responsibilities, obligations, technical basis, policy, application domain, or jobs. According to the CORBA Security Model [5], there are three major types of security domains:

- the security policy domain,
- the security environment domain, including message protection domain and identity domain, and
- the security technology domain.

A security policy domain comprises participants and system components that are intended to operate under the same security policy. A security policy is a contiguous strategy of organising security by establishing consistent rules, duties, and liabilities to enforce information security, as well as by defining and controlling authentication, access control, accountability, and others [6, 7]. A *security authority* administers each security policy domain.

A security environment domain is the scope over which the enforcement of the security policy is achieved by means local to the environment, i.e. without any help from other domains. A security environment domain is implementation-specific in the sense that it uses services from the underlying operating systems, basic protection mechanisms and communication services of the lower OSI layers to provide message protection. Therefore, the domain is also called message protection domain. Within a security environment domain, an identity domain can often be defined specifying common access control rules, rights and privileges. Usually, weak authentication procedures are in place (mutual trust of members). A typical example of a security environment domain is a department. In rare cases, where a whole enterprise employs a closed (centralised) system the enterprise as a whole can be regarded as a security environment domain, too.

A security technology domain uses homogeneous technology to enforce a security policy. Given this homogeneity, a department or a whole institution can represent a security technology domain. However, in open distributed systems such homogeneity rarely occurs.

To give a practical example, the purpose of security domains is to form groups of mutual trust defining a special level of risks and therefore demanding a set of countermeasures. Assuming adequate characteristics, departments, enterprises, institutions, and even distributed organisations can be considered as domains. These domains are assumed trusted and trustworthy environments, which must only be protected against external threats. Therefore, special security measures are required only for communication with partners outside the domain and are thus implemented at the domain boundaries. Examples for such advanced security measures are *firewalls, proxy servers,* and *external access LANs.* External services like WWW are kept outside the security domain. Bypassing the firewall by, e.g., "private" lines to the outside world using modem-mediated connections without special security measures must be prevented. To avoid unauthorised access, *routers* provide the association of locally external members of the enterprise representing the same security policy domain but different security environment domains. Because of the different security environment and security technology domains, message protection as well as authentication means are often required. To protect sensitive data according to the common view, between different security policy domains the highest

level of security, but within the same security environment domain representing an identity domain (and even the same security technology domain) the lowest level of security, is required.

At least partly, centralised architectures and non-co-operating institutions fulfil the scope of the domains described. They are traditionally considered as closed and therefore secure systems. The trustworthiness of such systems is mainly based on the trust of both technology and involved subjects (users and administrators). Distributed systems are more vulnerable to security breaches than the traditional systems, as there are more places and opportunities that the system can be attacked. Further, we find the more complicated conditions of different domains. Nevertheless, the structural changes in healthcare systems as well as technological developments are demanding the inherent distributed nature of health information systems.

On the other hand, 70 to 95 percent of attacks on information systems are executed by insiders, as could be shown by own investigations performed in Germany as well as by data from the USA [8]. In that context, the following chapters describe future health information systems and related security, assuming open and non-trusted conditions. The shared care approach requires that the reliability of processes and information must be assured by corresponding security-related measures [5].

3. USER RELATED SECURITY SERVICES

Sharing care as well as the resulting communication and co-operation in healthcare have to be person-related. Beside social and human reasons, this is caused by the legally binding property of business processes (including liability issues) with its corresponding security services like authentication and digital signature [3, 4, 6]. In addition, application security services such as authorisation and access control depending on structural or functional roles have to be person-related too. The structural role reflects position and responsibilities within the organisational hierarchy, whereas the functional role reflects the concrete functional and procedural activities in the care environment [5, 7].

Communicable medical information systems need not be bound to networks. Data may be recorded, stored, and processed at other media. In that context, the development of smartcard technologies especially in Europe enables alternatives.

Patient Data Cards (PDC) are smartcard-based medical application systems. Providing patient's informational self-determination as a specific type of user relationship, a PDC requires a special access control management to keep the security level and trustworthy relationship

guaranteed to the patient [1, 2, 5, 9]. Involved in the DIABCARD project [3, 4] of smartcard-based information systems funded by the European Commission and supporting communication and co-operation of diabetes care, the Magdeburg Medical Informatics Department has specified and implemented corresponding user related security services considering both health professionals and patients [13].

An appropriate tool to provide person-related security services bearing information items needed as cryptographic keys and certificates is the use of identity-bound and role-bound tokens. In Europe, the smartcard technology has been preferred as secure and payable solution provided as Electronic Identity Card (EIC) and/or Health Professional Card (HPC), which could also be used in a pan-European Healthcare Network based upon the Internet and its tools [3, 4, 14]. Guaranteeing a bilateral trustworthy patient-doctor relationship, the patient needs such a token like an electronic Patient Identity Card (PIC), too. This PIC could be combined with other functionality as patients' medical data on Patient Data Cards (PDC) or patients' insurance cards. Currently, such PDC with PIC functionality is under implementation as next generation DIABCARD.

Facilitated by several projects funded by the European Commission, the Health Professional Card will be widely used in most of the European countries. This process is supported by governmental laws as, e.g., in France or by common initiatives of the physicians' organisation and other bodies of the physicians' self-government as, e.g., in Germany. To enable communication and co-operation across national borders, architecture and interfaces providing access to the card have been standardised at the European scale as CEN TC 251 prENV 13729 "Health Informatics – Secure User Identification – Strong Authentication using Microprocessor Cards (SEC-ID/CARDS)" [15], which is compatible, e.g., to the German HPC Specification [16]. Also card readers and interfaces to the hardware and software components of the application environment must be agreed on. EC-funded projects such as TrustHealth, CARDLINK, and DIABCARD [3, 4] provided corresponding specifications. The following sections explain the HPC concept and its related TTP infrastructure in some more detail.

4. THE EUROPEAN HEALTH PROFESSIONAL CARD

The cryptographic basis for the HPC security functions' model is an asymmetric algorithm, e.g. RSA or elliptic curves. Therefore, a specific key pair is generated, consisting of a private key (the owner's secret) and a public key. The private key is securely stored in the HPC and does never

leave this environment; the public key is stored in a public directory as part of a public certificate. To enable different security services, three key pairs are required to fulfil the security needs. There is one key pair for authentication procedures, another one for digital signatures, and the third key pair for encryption/decryption of, e.g., session keys. In some specifications, a fourth key pair is requested for encrypted storage of data in databases or electronic archives in order to allow a key-escrowing scheme only for storage keys if needed.

The HPC is further prepared to store additional information about the cardholder's identity, e.g. his or her name and address. Nevertheless, the HPC is a professional smartcard. And as stated before, the care process in general and the related communication and co-operation in healthcare and welfare have strictly to be person-related, considering the liability and the legal binding as well as corresponding security services. Therefore, Public Key (PK) certificates are used. Connected by identification means, the related attribute certificates are dedicated to access control functions [17]. Especially the application security services as, e.g., access control depending on structural or functional roles have to be established in a secure manner. Hereby, the structural role reflects administrative aspects as the position and the related responsibilities within the organisational hierarchy, whereas the functional role reflects the concrete functional and procedural activities in the context of the specific care environment. Currently it is not yet decided whether certificates will be stored only in directories, only in the card or possibly both could be done. If it should be done in the card, a lot of further work has to be done in the area of Card Verifiable Certificates (CVC)

5. THE RELATED TRUSTED THIRD PARTY STRUCTURE

The European TrustHealth project has started to describe the processes within the real world and the electronic world in terms of security services and their service specification [18]. Trusted Third Party (TTP) organisations have to provide different services.

In the traditional world of papers, one will find the authorities responsible for issuing authentic documents of an individual. That includes e.g. a registration office for inland and travel passports and a qualification authentication authority (QAA) for diploma etc. Regarding our movement to eHealth, any kind of information or certain data items are processed and transmitted from the real world into the electronic world by specific interfaces. All authorities of the electronic world are components of a Trusted Third Party structure.

Based on the formerly real world data items mentioned above, and connected to a unique distinguished name (DN) created by a Naming Authority (NA), a Registration Authority (RA) within the electronic world issues authentic documents (paper or database) of identity (Public Key Registration Authority - PK-RA) of profession (Professional Registration Authority - Pr-RA). Besides that, a Key Generation Authority (KGA) generates specific key pairs (see above). This could be done as a centralised process within the TTP (CKG), or it could be done locally within the user's secure environment (LKG). The decision whether it is allowed to generate keys outside a TTP environment is more a political than a technical one.

Authentic links between an individual's DN, his or her authentic ID documents and his or her Public Key are used to issue a Public Key Certificate (PK-Certificate) by a public Key Certification Authority (PK-CA). A Professional Certification Authority (Pr-CA) linking professional information items without any key to issue a Professional Certificate (Prof. Certificate) does the same. All different data items, keys, and related certificates are necessary to establish the security services of identification and authentication, integrity, confidentiality, availability, and accountability. For legal reasons (responsibility) and for reasons of trust (professional bodies), different organisations become responsible for the different steps of the registration and certification processes. Now, how is this rather complicated procedure really performed within the Magdeburg pilot environment?

The University Hospital of Magdeburg (UHM) including its cancer centre on the one hand and the Physicians' Chamber of the German federal state of Saxony-Anhalt (PCSA) on the other are currently authorities of the real world in terms of profession. For identity purposes, the German inland passport issued by an official German registration office is used. Considering current developments, electronic components of the TTP at UHM and at PCSA acting both as NA and Pr-RA have been established which are also applicable as a PK-RA using the individuals' passport for identification. For issuing PK certificates, our German TrustHealth partner GMD Darmstadt (Gesellschaft fuer Mathematik und Datenverarbeitung) provides the services needed. In the future, a CA officially based on the requirements of the new German Digital Signature Law and Act will be introduced. The CA has set up a public directory service including the procedure of Certification Revocation List (CRL). A locally managed directory service as a back up of the CA service is available as long as connections between a health professional and the Magdeburg Registry will occur.

The generation, distribution, and revocation of keys, certificates or even cards as well as the provision of corresponding information services as directory services, often summarised Public Key Infrastructure (PKI),

require an appropriate infrastructure of national or pan-European TTP services.

Within the TrustHealth project mentioned already, the Magdeburg Medical Informatics Department developed, implemented, and evaluated a trustworthy health network for shared care in oncology called ONCONET [10]. As the first one in Germany, the ONCONET is based on standardised tokens and services such as HPC and TTP services. At the same time, the ONCONET has been the first pilot for the German electronic doctor's license [16]. The ONCONET will be presented shortly at the end of the paper.

6. THE PROCEDURE OF HPC DISTRIBUTION

The health professional fills out an application form consisting of several specific registration forms [3, 4] with all details asked for, and gets his distinguished name (DN) by the Naming Authority (NA). The PCSA for all physicians and the UHM (Cancer Centre) for non-physicians verify and "certify" the identity and the professional details as qualification, speciality, role etc. of the health professional by signing the complete registration form. As a Registration Authority (RA), they send the preliminary authentic paper form or the related electronic authentic document to a selected Certification Authority (CA) "by law" which simply means that the CA has to be evaluated by legal authorities in Germany and has thus to be certified as strictly following German electronic signature legislation.

As soon as all the procedures of card issuing and the related TTP services are finalised (the keys are generated, the card is initialised and personalised, the certificates are created, and the directory update is done), the card and the PIN code to just open it are sent to the responsible Registration Authority (RA) using separate ways. PCSA or UHM get the card and the PIN code to deliver both to identified and authenticated users. The health professional can do this identification by providing either inland or travel passport as mentioned above.

Within the RA environment, a simple test application is used to verify card and PIN operations. Therefore, the user can check both the Health Professional Card and the access to it before he or she leaves the office. The user is requested to specify a new PIN after this first use of the HPC because the former PIN is just a so-called "transport PIN". If everything works as properly as expected, the health professional is able and allowed to use his or her HPC for each security functionality within the given pilot environment. The medical background of the Magdeburg cancer documentation

application and the related oncological network will not be described here. This information can be found in [9].

For improved data protection and data security reasons, the further development of smartcards and related authentication mechanisms will lead to the use of biometric algorithms as, e.g., fingertip, eye analysis, or voice analysis. The current European HPC concepts consider this new trend by specifying requirements for those biometric algorithms and describing the needs of related interfaces.

7. INTERNET BASED SECURITY INFRASTRUCTURE

Beside of the network security services mentioned above, several projects funded by the European Commission currently aim the development of a pan-European healthcare network based on the Internet and its WWW tools. In that context, security infrastructures based on standardised hierarchical TTP structures have been installed. They are managing a Public Key infrastructure and the related mechanisms, providing CA services including cross certificates to other TTP hierarchies [3, 4].

Figure 2 shows the general schema of this first distributed international TTP architecture in healthcare developed for another European project called EUROMED. EUROMED-ETS itself has involved the pilot sites University of Athens in Greece (ICCS), University of the Aegean in Greece (UoA), University of Calabria in Italy (UoC) and University Hospital of Magdeburg in Germany (UHM).

Using the example of the Magdeburg UHM part of the solution, figure 3 presents the hierarchical TTP structure of this distributed international healthcare EUROMED-ETS TTP architecture. ICCS at the National Technical University of Athens (NTUA) in Greece hereby represents the root-CA. Below this top-level CA, ICCS has implemented another CA service for the EUROMED-ETS (ETS Consortium) purposes. This CA called EUROMED-ETS-NTUA has been certified by the root-CA and has then certified the Magdeburg CA (UHM CA) located at a specific CA server (cabmi1.medizin.uni-magdeburg.de). Besides the certification of other CAs, the ETS CA has to issue identity certificates for the ETS community, as shown in the example above following the hierarchical scheme leading to a user ID certificate (Peter Pharow's UoA ID).

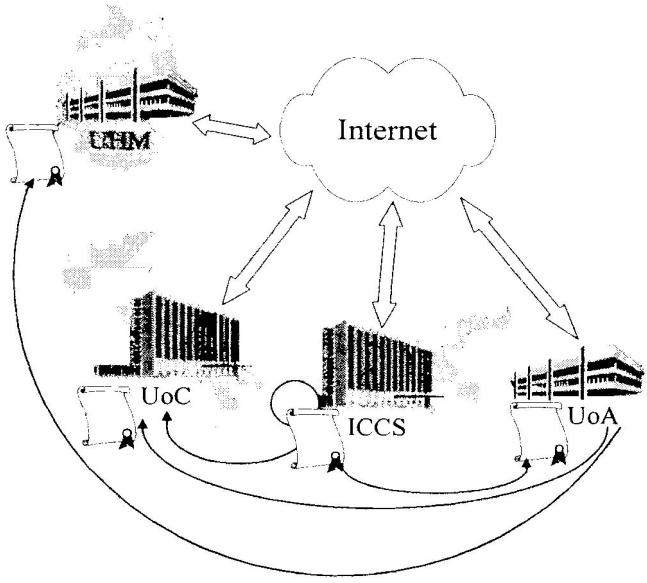

Figure 2. EUROMED-ETS Pilot Architecture for Internet Security Services

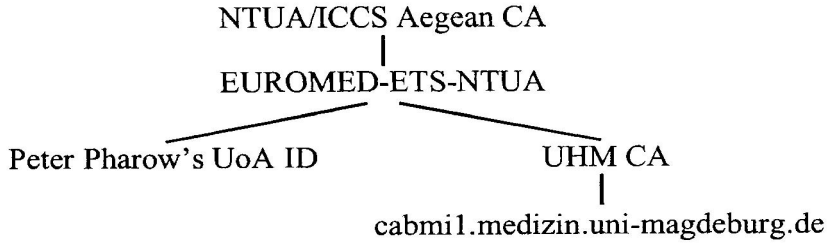

Figure 3. Schema of the Hierarchical TTP Structure

Internet tools as browsers are being completed with enhanced security functionality soon. Important Internet application environments as, e.g., Java have and will further get improved security mechanisms. Additionally, the HPC has been introduced in the Internet-based communication infrastructure mentioned above. Finally, especially security requirements for handling patient's medical and administrative data using the Internet have been mentioned during the IMIA WG4 Working Conferences held in Osaka and Kobe (Japan) in 1997 and in Vancouver (Canada) in 2000 (e.g. [8, 14]).

Following the requirements of the market as well as the European e-Health strategies, the European Commission has agreed to further investigate Internet and security issues. Started in January 2000, a project called "HARP – Harmonisation for the security of the web technologies and applications" is currently focusing on secure medical applications accessible via Internet [3, 4]. Based on former investigation especially in the context of traditional TTP services such as card generation and certificate issuing for human beings, HARP is dealing with a more flexible strategy concerning also systems, documents, applets, etc. as part of a security infrastructure thus allowing them to authenticate themselves towards other *principals* and to e.g. sign transmitted data.

The overall objective of the HARP project is the development of new technologies and tools for the integration of Web-oriented security systems and the combination of coherent services to demonstrate and quantify the value of security tools/mechanisms/systems harmonisation in business and citizen needs in the Information Society. This overall objective is broken down into the following sub-objectives:

a) Review/analyse Web components used in the telemedicine sector in terms of security;
b) Investigate the impact of TTPs in the security of Web-based telemedicine applications;
c) Develop harmonising software and tools to cope with the diversity of the Web components;
d) Design, integrate, validate a harmonising, cost-effective, user-friendly security platform based on TTPs for securing integrated telemedicine applications;
e) Demonstrate HARP's integrated security solution in the telemedicine sector;
f) Disseminate the project results to the widest possible audience.

To achieve the project's objectives the work is split into four phases. In phase A ("Feasibility Study"), HARP has already adopted and newly developed metrics, methods, criteria and test methodologies. These means have been used to identify, classify, evaluate and compare Web components, to investigate how TTP technology can be used to prevent the various risks introduced by the Web use, and to draw evaluation criteria for the project results and pilot operation targeted in the telemedical sector.

As an outcome of phase A, the HARP consortium decided to follow both server-centric and user-centric approaches to introduce a security infrastructure over the open Internet that is prepared to allow secure access to, and secure download of, documents, guidelines, application form, software applets, etc. After all, this strategy will allow HARP to offer both products and services.

In phase B ("Design and Development") that has started recently, harmonising tools and mechanisms are to be designed so as to allow TTPs to cope with the diversity on the Web-based telemedical applications. A cross-security platform based on the TTP technology will be introduced soon. Platform-specific security features will be isolated and communicate with them through an abstraction layer that will work for all platforms. This will be accomplished by letting visible interface of a platform specific case define how client code accesses a function without regard of how the function is implemented.

In phase C ("Pilot Evaluation"), the designed platform and the developed TTP services/functions will then be integrated and evaluated by medical users (hospitals). For the evaluation, phase A will be used as a yardstick. The trial network will reflect the TTP architecture in specific telemedicine scenarios designed already.

Finally, phase D ("Promotion") includes the production of guidelines that will cover all the information cases, techniques and algorithms. Workshops and meetings with key actors from health authorities, industry, business and academia will help defining security specifications and conditions for commercial deployment of related products. HARP will establish a continuous collection and dissemination of results obtained in security projects.

8. THE ONCONET SAXONY-ANHALT

Within the European TrustHealth project, a German demonstrator based on the solutions illuminated has been established presenting a comprehensive security infrastructure for health information systems. Supporting communication and co-operations between HCEs dealing with cancer patients' care, the healthcare network demonstrator is called ONCONET. Using HPCs and TTP services at least partially provided by the Physician's Chamber of the federal state Saxony-Anhalt, the network enables communications between health professionals as well as between them and the Clinical Cancer Registry Magdeburg/Saxony-Anhalt which is hosted at the Magdeburg Medical Informatics Department. It allows the trustworthy exchange of doctor's reports but also any type of file (HL7 messages, images). Furthermore, pre-defined or even free SQL (Structured Query Language) queries are possible. For more detailed information about the ONCONET solution see, e.g., [10].

9. CONCLUSIONS

Meeting the shared care paradigm, future health information systems will be distributed, interoperable and Internet-based. Because such health networks deal with personal medical data, information systems must run in a trustworthy way. Within its research and development programmes, the European Commission launched a set of projects for specifying, implementing, and evaluating advanced solution for security services in health information systems. Exploiting the results of different projects, the first German distributed secure health network and electronic medical record system has been implemented. In that context, the standardised European Health Professional Card has been combined with Trusted Third Party services which are currently under enhancement within the HARP project. Including security solutions for smartcard-based medical information systems held by the patient as Patient Data Cards, a comprehensive security framework for health could be provided first in Europe.

10. ACKNOWLEDGEMENT

The authors are indebted to the European Commission for funding as well as to the partners of the projects ISHTAR, TrustHealth, EUROMED-ETS, MEDSEC, and HARP. Furthermore, they would like to thank the colleagues of the Physician Chamber Saxony-Anhalt as well as of the health care establishments involved in the ONCONET for their engagement.

11. REFERENCES

1. CE: Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Strasbourg 1995.
2. CM: European Recommendation No. R(97) of the Committee of Ministers to Member States on the Protection of Medical Data. Strasbourg 1997.
3. European Commission: Projects of the Fourth EU Health Telematics Applications Programme. http://www.chto.be/projects/
4. IBMI Projects. http.//www.med.uni-magdeburg.de/fine/institute/ibmi/dmi/respro.htm
5. Blobel B, Baum-Waidner B: Current Security Issues Faced by Health Care Establishments and Resulting Requirements for a Secure Health information System Architecture. In: The ISHTAR Consortium (Edr.): Implementing Secure Healthcare

Telematics Applications in Europe, pp. 101-147. Studies in Health Technology and Informatics, Vol. 66. IOS Press Amsterdam 2001.

6. The SEISMED Consortium (Edr.): Data Security for Health Care. Volume I-III. Studies in Health Technology and Informatics, Vol. 31-33. IOS Press Amsterdam 1996.
7. Blobel B, Roger-France F: A Systematic Approach for Secure Health Information Systems. Accepted in Int. J. Med. Inf..
8. Blobel B, Katsikas SK: Patient data and the Internet - security issues. Chairpersons' introduction. International Journal of Medical Informatics 49 (1998), pp. S5-S8
9. Blobel B: Clinical Record Systems in Oncology. Experiences and Developments on Cancer Registries in Eastern Germany. In: Anderson R (Edr.): Personal Medical Information - Security, Engineering, and Ethics, pp 39-56. Spinger, Berlin 1997.
10. Blobel B: Onconet: A Secure Infrastructure to Improve Cancer Patients' Care. European Journal of Medical Research (2000) 5: 360-368.
11. Blobel B: Application of the Component Paradigm for Analysis and Design of Advanced Health System Architectures. Int. J. Med. Inf. 60 (2000) 281-301.
12. ISO/IEC 10746-2: Information Technology – Open Distributed Processing – Reference Model: Part 2: Foundations
13. Blobel B, Spiegel V, Pharow P, Engel K, Engelbrecht R: Secure Interoperability of Patient Data Cards in Health Networks. In: Hasman A, Blobel B, Dudeck J, Engelbrecht R, Gell G, Prokosch H-U (Eds.): Medical Infobahn for Europe, pp 1059-1068. Series in Health Technology and Informatics Vol. 77. IOS Press, Amsterdam 2000.
14. Katsikas SK, Spinellis DD, Iliadis, J, Blobel B: Using Trusted Third Parties for Secure Telemedical Applications over the WWW: The EUROMED-ETS Approach. Int. J. Med. Inf. 49 (1998) pp. 59-68.
15. CEN TC 251: prENV 13729: Health Informatics - Secure User Identification – Strong Authentication using Microprocessor Cards (SEC-ID/CARDS), Brussels 1999.
16. The German HPC Specification for an electronic doctor's licence. Version 0.81, February 1999. http://www.hpc-protocol.de
17. Wohlmacher P, Pharow P: Applications in Health Care using Public-Key Certificates and Attribute Certificates. In: Proceedings 16th Annual Computer Security Applications Conference. IEEE Computer Society, Los Alamitos 2000.
18. Blobel B, Pharow P: Experiences with Health Professional Cards and Trusted Third Party Services Providing Security in Distributed Electronic Records in Oncology. Proceedings of the Conference „Toward An Electronic Health Record Europe '97", pp 29-39. 20-23 October 1997 London.