European Trusted Third Party Services for Internet Security

PETER PHAROW and BERND BLOBEL
Medical Informatics Department
University Hospital of Magdeburg
Leipziger Strasse 44, D - 39120 Magdeburg
GERMANY

Abstract: Introducing the technological step into the next millennium, advanced communication means as global networks including the Internet become more and more important for a fast and convenient information exchange across regional and even national borders. Concerning the sector of public and private health care and welfare in Europe, new health information system, or citizens' information systems generally, are coming up to meet the needs of the whole society. Thus, developing and implementing those systems is one of the most important aims of the next framework of the European Commission.

But access to and communication of relevant patient-related administrative and medical information items means always a secure and trustworthy way of accessing and communicating data. Concerning the main aspects of specific legal, social, ethical, technical, organisational, and even political requirements for a secure access and a secure communication in terms of data protection, data security, privacy, safety and quality using unprotected networks as, e.g., the Internet, there is a strong and even growing need for a new fundamental technology to meet the whole range of the security categories as integrity, confidentiality, availability, accountability, and access control which have been discussed in detail in this volume [2].

For all these issues, different technical and administrative means are requested to be used. On the one hand a secure hardware token is required. In general, the ideal format for both storing personal information items and secret keys but also in terms of mobility is a processor smartcard with cryptographic library functions. It should be a standardised one. On the other hand the full scale of network-based and Internet-based Trusted Third Party services is necessary. These related security services are required for different purposes as e.g. the naming procedures of the principals, for personal and professional identification and registration, for key generation, for card issuing, for the creation of personal as well as professional certificates, and also for an updated directory service including certificate revocation procedures. Therefore, a pan-European framework based on both technical and legal agreements or even standards is required.

Key-Words: Security Networks Internet Smartcards TTP Authentication Integrity Confidentiality Proc.pp..3971-3977

1 Introduction

Meeting the challenges of the open systems' paradigm, nowadays information systems are exposed to an increasing number of threats causing risks for the enterprises involved in information storage, processing, communication, and co-operation. The latter is of a specific importance especially in distributed or at least interoperating health information systems, also called shared care information systems, medical networks, or even health networks. Security services can be defined providing secure information processing and secure communication, whereby most of them depend on a trustworthy and secure user identification and authentication.

Using strong asymmetric cryptographic algorithms for authentication and digital signature, the leading industrial companies in the world are nowadays able to provide a high security level meeting the requirements mentioned above. The integration and implementation of related technical and organisational means fulfilling also the new European legal initiatives' requirements support communication security and application security not only in the health care sector [1].

To overcome the weakness of existing solutions, additional properties or even new tools are required. In Europe, the combination of ownership and knowledge is used for strong authentication consisting of smartcards as token and the PIN identifying the card user as the card holder. So the ideal format for storing personal information items and secret keys is a processor smartcard with cryptographic functions. The smartcard provides symmetric and asymmetric cryptographic algorithms for identification and authentication. In the future, biometric procedures will be introduced. Legal bodies may require whether a Personal Identification Number (PIN) or a biometric authentication or even both. Furthermore, the card is able to bear the cryptographic keys and mechanisms

needed for other security services as e.g. integrity check by digitally signed hash values, and the protection of confidentiality by specific encipherment / decipherment algorithms. To technically enable the off-line use of such cards, related (card verifiable) certificates can be stored in the card. Relevant items including public keys have to be stored in and provided by certificates. The smartcard and the card-related infrastructure are able to handle the access to public directories as well.

All these items belong to a system of security components within domains, and have thus to be considered for a domain policy. Aspects of these components and the secure communication and co-operation between them using open networks are also mentioned in detail in [2] in this volume more focusing on issues of domains and policies.

Based on the experience, definitions and specifications of several security-related European projects as, e.g., „Trustworthy Health Telematics (TrustHealth-1 and TrustHealth-2) " [3] dealing with the use of smartcards, or „EUROMED-ETS" [4] dealing with Internet security and TTP, the department of the authors has introduced a professional smartcard for medical staff - the Health Professional Card (HPC) - and the related Trusted Third Party (TTP) services. In co-operation with national and international initiatives in the area and close to standardisation bodies as, e.g. DIN in Germany [5], CEN in Europe [6], and ISO as an international one, the pilot will support the improvement of the communication security as well as the application security in the context of a real medical application.

2 Trusted Third Party

It is typical for asymmetric cryptographic algorithms as, e.g., RSA to have key pairs to be used. Hereby the first part, the secret key, is stored in a secure way mostly on a hardware token as, e.g., a smartcard. The related public key as the second part of the key pair has to be stored publicly available as part of a certificate. Creating these certificates (Public Key or identity certificates and attribute certificates), storing them in a public directory service and keeping them up-to-date by Certificate Revocation Lists (CRL) is one of the most important issues of a trustworthy independent third party organisation therefore formally called a Trusted Third Party [3]. A general overview of the security services involved is given in figure 1.

Basic security services: By this one should understand fundamental security services and functions directly related to the secure communication between two parties. The services may also be applied in other circumstances such as for the authentication of the end user towards his or her workstation. The basic services compare to the security services described in the security framework of ISO OSI, and thus constitute a necessary basis for both the infrastructural and value added services.

Infrastructural services: Services which facilitates secure, open communications, particularly HL7 or EDI in general, in large scale, i.e. between a large number of users affiliated in various enterprises in various sectors, even in various countries, and where one cannot assume that all users can know or trust each other, or where there exists different security policies. The handling of unique names, keys, certificates and cards is a typical example of services which is not necessary in a world where only a few parties known to each other communicate. However, when an infrastructure for large scale open communication is established, the infrastructural security services will become necessary; even a prerequisite to establish trustworthy health telematics in a large pan-European context. when leaving a local health care establishment, a TTP is needed to provide some of these services. Note that both the basic and infrastructural services should be more or less transparent to the users; the users should not be involved more than absolutely necessary when using these services.

Value added security services: These are related to the business functions of the user or the communication of documents and messages. They can follow from purely business related conventions or agreements, or they can follow from regulations given by law or by provisions of the law. Examples of such services, relevant to health care, is registration of health care professionals, issuing of professional certificates, secure storage of documents, pseudonymisation, and other.

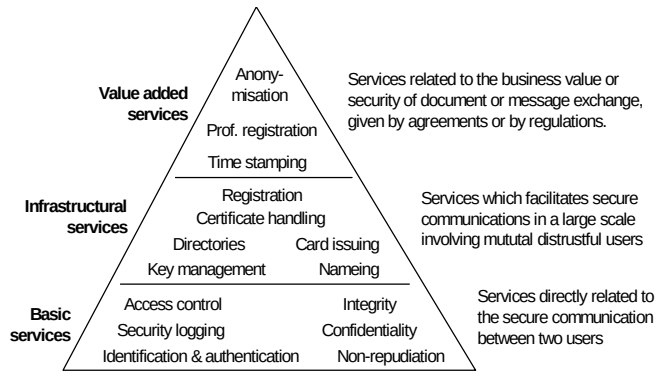

Figure 1. Security Services Categorisation

In the next chapters, the TTP will be described in a more detailed manner focusing on both the formal issues, the practical solution in several European countries, and the „TrustHealth-2" approach..

2.1 A TTP in general

This section describes the overall functional aspects of Trusted Third Party services required for trustworthy

health telematics. A detailed model consisting of functional roles and their interaction in a TTP infrastructure is described in brief focusing on the TTP functions which development, establishment and operation will be of particular importance to the health care sector.

To facilitate the infrastructural and value added security services described in the previous section, there will in most practical circumstances, and certainly in a pan-European context, be a requirement that the security services are provided by certain parties which are not formally attached to any of the communicating parties, but in some sense are trusted by these parties to fulfil all the requested services in a secure and trustworthy way. So in this chapter there will be a focus on the parts of the TTP infrastructure which are related to public key certification, i.e. a focus on the basic and infrastructural services.

To describe the structure of the relevant Trusted Third Party services one must again emphasise that a TTP comprises all of the independent organisation which offers and is responsible for a defined TTP service. One girder of such an organisation should be a secure IT and communication system, which as a whole or in parts might be outsourced to another organisation. However, this is not the only or even the most important girder for a TTP to fulfil its basic objective: to offer security services with the necessary degree of (technical and business) functionality and assurance. Its formal or legal position within its service domain might be equally important.

Further, a TTP service structure is not meaningful unless we define a set of roles and describe the objectives and tasks of these roles are an how the various roles interact. Figure 2 pictures the relevant roles and how the various roles might interact in a general TTP infrastructure.

Hereby a *User* is an individual entity. A *Public key registration authority (PK-RA)* is an entity which uniquely identifies and registers users applying for the DS services provided, whereas a *Professional registration authority (Pr-RA)* is an entity which registers (and possibly authorises) individuals as health care professionals. The *Naming authority (NA)* is an entity which appoints unique certificate names to users.

The naming authority may also handle the naming of health care professional classes (e.g. physician), specialities (e.g., internal medicine) and possibly sub-specialities (e.g., nephrology). The *Public key certification authority (PK-CA)* is an entity which certifies the linkage between the unique certificate name and the users public signature or decryption key by issuing public key certificates digitally signed by the PK-CA. PK-CA is also responsible for the revocation and re-issuing of public key certificates, whereas a *Professional certification authority (Pr-CA)* is an entity which certifies the linkage between the unique certificate name and the users professional status by issuing professional certificates digitally signed by the Pr-CA. Pr-CA is also responsible for the revocation and re-issuing of professional certificates. And last but not least the *Card issuing system (CIS)* is an entity which issue signature/decryption chipcards containing (at least) the private keys of the users (card owners). The generation of keys could be done by a *Local / central key generator (LKG/CKG)* as an entity either located locally (by the user or PK-RA) or centrally (by the PK-CA or CIS) which generates the required key pairs. The certificates have to be stored in a *Certificate directory (DIR).* It is an entity which provides the public key certificates, professional certificates, certificate revocation lists and possibly other information about users to other users at request.

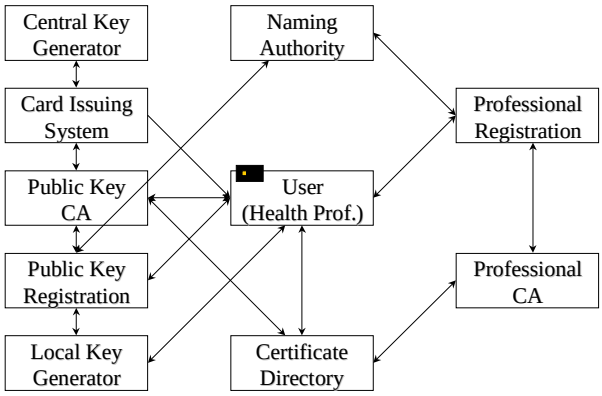

Figure 2. General TTP roles and possible interactions

In figure 3 the TTP roles and the interactions are shown which are primarily needed to influence functionality and security from the health care sector. The other roles which are less particular health care requirements has been dimmed. This does not mean that there are no requirements to these elements.

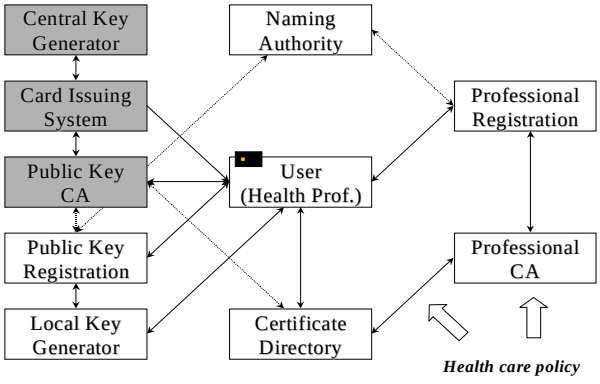

Figure 3. TTP roles and possible interactions – health care oriented model

However, the requirements are considered to be general requirements in the overall confidence in the TTP services provided in relation to the specified security policies and other relevant elements. This is described further in [2].

2.2 The German TTP - Current Status

On September 24th, 1998, the global German root-CA, the so-called "Regulierungsbehörde für Post- und Telekommunikationsdienste (Reg-TP)" has been established. It was the first CA completely following the German "Information and Communication services Act (IuKDG)" and the embedded "Digital Signature Act (SigG)" [7]. Besides the signature certificate, another one for time-stamping services and a third one for directory services has been issued. So the German Reg-TP is now allowed to offer a lot of services required for a trustworthy access and a secure communication based on HPC and TTP. The German SigG defines a hierarchical scheme for a CA structure. That means, that below the root-CA there is one (or more than one) level of CAs. And as usual, the root-CA was established to only certify other CAs. Thus, the Reg-TP will never issue any kind of user certificate.

Actually, there is only one certified CA in Germany that is allowed to issue user-related certificates by law. This one is a CA hosted by the German Telekom and is called Telesec. A second one is yet to come. The Telesec is officially on-line since January 1999. Thus, descriptions of policies, business continuity plans, and other organisational aspects are not publicly available right now. So UHM could not yet decide about the CA and the related directory service to be provided by the CA to be used for certifying users but will do so later.

Another aspect is the specification and the content of identity certificates (authentication certificates, signature certificates, encryption certificates) on the one hand and professional attribute certificates on the other. The definition of those certificate structures is still in progress. So the paragraphs starting with 2.4 are an attempt to define and to adapt a general scheme that is compatible to what is expected to be provided soon by an official German policy definition body in the near future. But before these specifications are available we will introduce the German TTP approach some aspects of the „TrustHealth-2" project [3] mentioned above will be illuminated.

2.3 The TrustHealth TTP Approach

The „TrustHealth-2" (TH-2) project is a project within the Health Telematics sector of the Telematics Applications Programme (TAP) of the European Commission 4th framework programme. The project started in June 1999, and aims on the basis of the results of former European projects as TrustHealth-1, ISHTAR, EUROMED-ETS, DIABCARD3, and SIREN to demonstrate a multi-national TTP-platform in a European framework and integrate real applications and users in various projects.

2.3.1 TrustHealth-2 in General

The objective of the TTP-related work items of TH-2 is to implement and provide the required Trusted Third Party infrastructure. This objective also includes definition and execution of the procedure policies for TTP services, based on TH1 results on TTP policies. Thus, the main task will be to harmonise and implement the services in the direction of the procedures and policies defined in several European as well as national directives and initiatives (e.g. in Belgium and Germany).

Finally, the special requirements from the health care sector on the TTP services will have to be investigated, described and implemented by the TTP providers. A major effort will be to set up the appropriate procedures to meet the requirements for services at the various user sites as regards not only to security but also to convenience and effectiveness.

2.3.2 TrustHealth-2 in Germany

In the current phase, the University Hospital of Magdeburg (UHM) will contribute to the development and will at least host the TTP in terms of Naming and Registration for non-physicians and in terms of a related local directory service in close co-operation with both the Physicians' Chamber of Saxony-Anhalt (PCSA) and the Physicians' Chamber of Lower Saxony (PCLS). The Cancer Centre is located in the Medical Faculty of the Magdeburg University, supported by the Medical Informatics Department of the Magdeburg University hosting the oncological medical record system (cancer registry) itself. This structure is the hosting organisation for all persons and institutions in the region who are involved in the cancer care both directly and indirectly.

The Physicians' chambers in general are the regulatory organisations for all physicians, thus the PCSA becomes responsible for providing the physicians-related part of the TTP services for professional cards for the health care and welfare sector of Saxony-Anhalt. Within the PCSA database, all information items about the Saxony-Anhalt physicians' training (e.g. education, approbation, qualification, profession, speciality, examinations) as well as information items about the physicians themselves (name, address, employers' or office's address respectively) are available. The PCSA will act as Naming Authority (NA) and Registration Authority (RA) for physicians of the UHM in terms of individual as well as professional purposes - as long as other public organisations do not provide similar services.

2.4 The Magdeburg TTP

Fulfilling the different requirements of the current German legislation, related rules and regulations, and further ”legal” activities, the former approach of the UHM projects in Germany (meaning that e.g. TH-2 Germany intended to provide its own TTP services completely) has slightly changed. As far as there is a publicly available and certified CA service, TH-2 Germany will use it. That means the different TTP functions are provided by different partners inside and outside of the project.

The policy of the TTP described here in detail, includes the procedures of card request, naming, individual and professional registration, individual and professional certification, card issuing, directory services including revocation procedures, and card distribution [2]. The current TTP structure and infrastructure including the different roles to be played by the UHM and their partners are shown in figure 4 below.

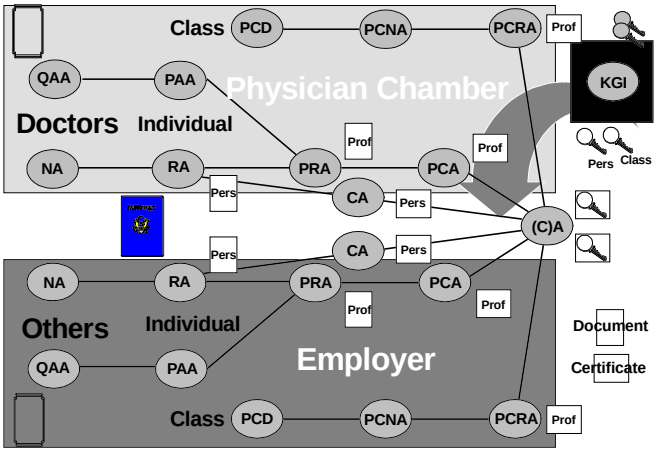

Figure 4. The Magdeburg TTP structure

In the next part, TTP functions as Naming, Registration and local Directory including some technical and organisational decisions and solutions will be described for the Magdeburg TTP solution.

2.4.1 General Remarks

There are two Naming Authorities (NA), UHM and PCSA. UHM will provide services for non-physicians, PCSA will provide related services for physicians. The same procedures are used for individual and professional Registration (RA). A local Directory service will be provided technically by UHM with PCSA managing it in terms of revocation lists and updates. For the reasons mentioned above, the CA part cannot be described completely in detail in that context.

2.4.2 Request for an HPC

The Health Professional fills in the official German registration form with the details asked for, and gets his distinguished name (DN) by the Naming Authority (NA) which is responsible for him. The PCSA for all physicians and the TRM (UHM) for non-physicians verify and ”certify” the identity and the professional details as qualification 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”.

2.4.3 The Naming Authority (NA)

The UHM TTP has agreed in a certain structure for all naming purposes. The distinguished name of a user is structured as follows:

DN = CN.SN.D.C

The last part of the DN is always ”TRM.DE” and ”LKS.DE” respectively. Hereby ”TRM” stands for Tumorregister (cancer registry) Magdeburg and means the responsibility of the legal entity Cancer Centre Magdeburg for the non-physicians. ”LKS” stands for Landesärztekammer (Physicians’ Chamber) Saxony-Anhalt; the chamber is responsible for all physicians. The country code ”DE” means simply Germany (similar to the Internet policy). The distinguished names of the NAs themselves are O=PCSA and O=TRM respectively.

The distinguished names are created by the Physicians’ Chamber of Saxony-Anhalt (PCSA) and the Cancer Centre of Magdeburg (TRM), following the recommendations of the TrustHealth project. As mentioned before, the Physicians’ Chamber of Saxony-Anhalt is responsible for all naming issues concerning the physicians in the federal state of Saxony-Anhalt. Because the professionals besides the physicians are not obliged to be organised in a chamber, the Cancer Centre as the responsible authority provides TTP naming services for all professionals who are non- physicians. The DN is valid both for individual and professional usage and realises the connection between individual (Public Key) certificates and professional (attribute) certificates.

2.4.4 The Public Key Registration Authority (RA)

In the first realisation phase this TTP functionality is supported by PCSA, UHM, and an industrial partner (GMD Germany) via a database. The information items necessary are provided by PCSA and TRM via paper form using the German registration forms and sheets for Health Professionals in general. This registration forms have been developed by the Physicians’ Chamber of Lower Saxony (PCLS) and UHM, and are available at the moment in German only. The paper forms also include an informational introduction related to a policy

approach of how to manage the process of requiring and getting an HPC. The Health Professional requesting an HPC has to complete all the details of the different forms and sheets. Hereafter he identifies himself by his inland or travel passport directly at PCSA and TRM respectively.

2.4.5 The Public Key Certification Authority CA

As long as there are no certified and (in the sense of German legislation) well-accepted authorities for certification, this TTP functionality will be supported by the GMD using their own CA Management tool, which originates from the security toolkit "Security Development Environment" (SECUDE) [8]. Thus in the first phase the GMD could act as the top-level CA but not following the German Digital Signature Act. For the TH2 verification and demonstration phases and especially for planned cross-border and interoperability activities, it is decided to use "official" X.509 version 3 certificates issued by an officially certified CA. All software components are already prepared for the new certificates' version.

2.4.6 The Professional Part

Professional static and dynamic roles and functions as well as professions and specialities will be certified using separate certificates - professional attribute certificates. In Germany that seems to be the best way to handle the access rights in terms of legal regulations but also technical decisions regarding cards and directories. Actually, there are discussions in Germany how to describe professional roles, education, qualifications, specialities etc. within certain attribute certificates. PCLS has prepared a framework which is used for all German TH2 validation sites and scenarios. The contents of the attribute certificates may differ between the different players in German Health care. Physicians have their own ideas about what could and should be certified. Nurses, dentists, pharmacists may have different opinions. End of the 1st quarter of 1999, the first versions of professional attribute certificates are expected to be defined finally.

2.4.7 The Directory System

The German Digital Signature Act has already defined requirements and conditions for those who intend to run a public Directory service. It does not seem to be useful for UHM / PCSA to establish their own directory service following completely the German law. Too much effort for a few users are not capable within the project. So the former approach has slightly changed.

As soon as a publicly available Directory service close to the CA that is responsible for issuing the TH-2 Public Key certificates is established it will be used. Besides that, the certain structure of the UHM pilot infrastructure allows a local mirror directory in order to hold the certificates close to the application. So during the verification phase of the project there will be the "official" X.500 Directory service of the CA and the local one at UHM available. In the meantime, first discussions between Magdeburg, GMD and several X.500 directory vendors as, e.g., Siemens-Nixdorf and ControlData from Germany, iD2 from Sweden, and BALTIMORE from Ireland have taken place in order to find out how to implement the local Directory service (and server) in Magdeburg in terms of requirements, connections to the CA, regular updates, CRLs, availability, further technical data, additional administrative data, infrastructural data, back-up, etc.

It is planned to have two local Directory services for the phase after the tests. The first Directory service is the Magdeburg one, provided by UHM in close connection with PCSA. The PCSA will handle all administrative items within the service as certificates, CRLs, and additional items. UHM will provide the technical basis. The second one (a mirror site) will be established by PCLS in Hannover using the same technical means. The mirror system will improve the security and will (hopefully) avoid misuse.

2.4.8 Distribution of Cards and PINs

As soon as all the procedures concerning card issuing and the related TTP services are finalised (the key pairs are generated, the card is initialised and personalised, the certificates are created, and the directory update is done), the card and a first PIN code to open it are sent to the responsible Registration Authority (RA) by postal or courier service using separate ways. PCSA and TRM (UHM) get the card and the PIN code to deliver both to an identified and authenticated user. He or she can do this identification by providing his or her inland or travel passport. Within the RA environment a small test application can be used to verify the card and PIN operations. So the user is asked to check both the card and the PIN before he or she leaves the office. Additionally, the user is requested to define a new PIN (user PIN) after this first use of the HPC.

If everything works properly as expected, the Health Professional is able (and allowed) to use his or her card for every security functionality within the pilot environment.

3 Conclusion

The functional and administrative benefits and advantages of smartcards (both professional cards and patient cards) in health care and welfare have been demonstrated by several projects world-wide. Applications as e.g. the oncological network mentioned above as a German prototype for specific real medical applications have been developed, researched, and tested for and with a HPC from the interoperability point of view. With reference to medical applications,

the projects have considered developing a portable electronic medical record whose essential information can be stored in a card together with pointers to extended medical record systems that may be available in remote data bases. Other applications are aimed at providing medical information about the patient in emergency situations (emergency data set) or to keep track of medications and prescriptions. Finally, several on-going initiatives of patient data cards deal with specific categories of patients (chronic diseases like cancer, diabetes, cardiac risks, pregnant women, new-borns, dialysis, etc.), strongly connected with the HPC for access functions.

The technology used in large majority is an electronic card (containing a read/write memory of different capacity) or a smartcard (a memory and an electronic circuitry for internal data processing for additional security functions, data encryption, and digital signature). Recently, applications have been proposed that are actually built around a multi-functional smartcard. So the card takes the full advantage of the possibilities offered by the smartcard technology to access independently and securely different memory areas and functions of one single card. This may allow to use the same individual card for different applications (identification and authentication, banking, health care, social benefits, etc.) considering may be different security policies connected to the applications.

Combining the results of several security-related projects funded by the EC as ISHTAR (policy), EUROMED-ETS (Internet), DIABCARD (patient data cards) and especially the TAP projects TrustHealth-1 and TrustHealth-2 (HPC and TTP) with the related data security initiatives in Germany, a framework for a secure access to and a secure communication of administrative as well as medical data in health care and welfare has been established to meet the new and even growing requirements of a pan-European health care system in the future [3, 4, 6]. New aspects as distributed medical and even health record systems and the exchange of medical data crossing national boundaries will lead to new models and new challenges for data protection and data security.

The on-going development process in Germany's health care and welfare mainly influenced by those projects and their results is already dealing with the new requirements brought up by an advanced IT use in all fields of our information society.

Based on definitions and specifications of former work, the Magdeburg Medical Informatics Department has introduced a professional smartcard for physicians and other medical staff. In co-operation with current national and international projects in the area, the Magdeburg pilot will help to improve communication and application security in the context of a real medical application.

4 Acknowledgement

The authors are in dept to the European Commission and to the Ministry of Education and Science of the German Federal State Saxony-Anhalt for funding European and regional initiatives and projects dealing with data protection and data security in healthcare and welfare as well as with issues closely related to the smartcard and TTP topics. We want to thank all the other partners and task force members in the different projects, standardisation bodies, and initiatives for their kind co-operation.

References:

[1] B.Blobel, P.Pharow (1997) Security Infrastructure of an Oncological Network Using Health Professional Cards, *L.van den Broek, A.J. Sikkel (Eds.): Health Cards '97*, Series in Health Technology and Informatics Vol. 49, IOS Press Amsterdam, 1997, pp. 323-334

[2] B.Blobel, P.Pharow (1999) Secure Communication and Co-operation in Open Networks, in: 3rd IMACS / IEEE CSCC '99 International Multiconference, Athens, Greece.

[3] The TrustHealth Consortium (1997) Project Description, Partners, Deliverables, Work Items. http://www.ehto.be/projects/trusthealth

[4] The EUROMED-ETS Consortium (1997) Project Description, Partners, Deliverables, Work Items. http://euromed.ece.ntua.gr

[5] HPC (1999) The German HPC Specification for an electronic doctor's licence. Version 0.81, February 1999. http://www.hpc-protocol.de

[6] CEN/TC 251 PT 037. A CEN Project Team for Secure User Identification for Healthcare Strong Authentication using Microprocessor Cards. http://www.centc251.org

[7] IuKGD (1997) The German „Information and Communication Services Law" including the „Digital Signature Law". http://www.iukdg.de

[8] SECUDE (1999) A General Purpose Security Toolkit. Specification of the SECUDE Software. http://www.darmstadt.gmd.de/secude