Secure Communications and Co-operations in Open Networks

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

Abstract: Nowadays trends in information systems are characterised by aggregation of the systems to distributed interoperable component systems. The communication and co-operation between these system components is increasingly crossing organisational, regional and even national borders using open networks including the Internet. Such interoperability must be provided in a secure way. Therefore, the different programmes launched by the European Commission dealing with informatics, telematics and the challenges of the Information Society also concern security-related projects.

Value-adding the results of several projects within both the TAP and the ISIS programme of the EC as ISHTAR or TRUSTHEALTH on the one hand and MEDSEC or EUROMED-ETS on the other, a regional pilot in oncology for a secure health network has been developed and implemented. Specifying domains and their security policy, security requirements and solutions depending on the systems architecture and behaviour have been defined. Additionally to firewalls at the domain borders, security services based on cryptographic algorithms must be provided which concern application security and/or communication security according to the general security model specified, also taking into account that most of the attacks to domains are caused by insiders.

Domains, policies and policy bridging are discussed under the view of security concepts and the concepts-services-mechanisms-algorithms-data relationships developed. Looking for the specific requirements of secure communications in open networks, communication security services and mechanisms will be presented. In that context, an open communication security solution regarding secure messaging (secure EDI) as well as secure channels (SSL and TLS in WWW environments) has been developed and implemented and will be demonstrated in detail. The corresponding security infrastructure needed as user authentication tokens (Health Professional Cards = HPC) and Trusted Third Party (TTP) services are content of another paper [10] in this volume.

Key-Words: Security Networks Internet Communication Application Authentication Integrity Confidentiality Accountability *IMACS/IEEE CSCC'99 Proceedings,* Pages:3961-3967

1 Introduction

"Shared Care" is the answer of all industrial countries' healthcare system to the challenge for increased efficiency and quality of care provision. Caring the same patient, it requires increased communication and co-operation between different providers. Including different persons from different parties, threats and risks for the patient's data security and privacy are growing, challenging appropriate security services and mechanisms guaranteeing the socially, ethically and psychically determined trustworthy patient-doctor relationship [1, 4].

2 Security Threats, Risks and Solutions

This chapter reflects some results of the European ISHTAR project dealing with security threats, risks and countermeasures in health information systems [4]. Threats are normal events in our life and also in the context of using information systems. Threats occur either by accident (errors) or with intent (attacks). In general, *active* and *passive* attacks may be distinguished depending on whether attackers stimulate or influence their victims before evaluating their behaviour or not. Of course, active and passive attacks can be combined in any way and any order.

According to the ITSEC criteria, risk in the context of IT security is defined as an aggregate of

- the likelihood of something untoward happening, i.e., the likelihood of a threat actually occurring,
- the degree of ability to cope with "the happening", i.e., the vulnerability to a threat if it did occur, and
- the resultant consequences if "it" did happen.

The risks faced by a real system are largely determined by the social and economic context in which it is run and by the security that it provides. The impact of social and economic factors can be limited by adequate codes of conduct and security policies [18, 19] whereas the security of a system can be increased by appropriate technical countermeasures. A system is called *trustworthy* if its risk is in a sense acceptable for the participants working with it. Naturally, risk and trustworthiness are subjective matters that have to be cultivated constantly. Therefore, a *trust model* can be expressed in terms of a *threat model*, i.e., which parts of a system are assumed to be exposed to what threats. This approach has been comprehensively discussed in [4].

3 Security Model

Communication and co-operation in healthcare, but not only in that application field, have to be provided in a trustworthy way. Therefore, a basic requirement is the mutual and certified strong authentication between the principals involved (user, application, machine, system, device). This service is needed for many other security services and mechanisms mentioned below. The communicated information has to be integer and has to be realised as agreed (e.g. confidential) as well. Data and processes (functionalities) have to be accountable. This complex of security requirements is called communication security. To provide the services needed, cryptographic mechanisms have been used. Because the user could perform the communications from and to different domains (working places, departments, organisations) the involved mechanisms have to be managed globally (at least within the agreed user domain). According to the „Fair Information Principles“ and the legal and ethical basis of healthcare [2, 3, 4, 18, 19], the „Need to know“ principle and the trusty doctor-patient relationship have to be guaranteed. The access to information (data) and functionalities of applications and their quality and accountability have been concerned by the locally managed application security, dealing with authorisation, access control and its management object (document) classification, specification of roles and rules for decision support etc. (Figure 1). To facilitate analysis, specification and implementation of security services and mechanisms as well as to enable the navigation through, a common layered security model was developed. Based on an object-oriented analysis and design via the popular UML methodology [9], a concepts-services-mechanisms-algorithms-data scheme facilitates the different user groups' view. Beside the concept of security, also the concepts of safety and quality must be mentioned. Currently also these aspects are taken into consideration for standardisation within the European Health Informatics standardisation body CEN, PT38. However, these additional concepts are out of the present paper's scope.

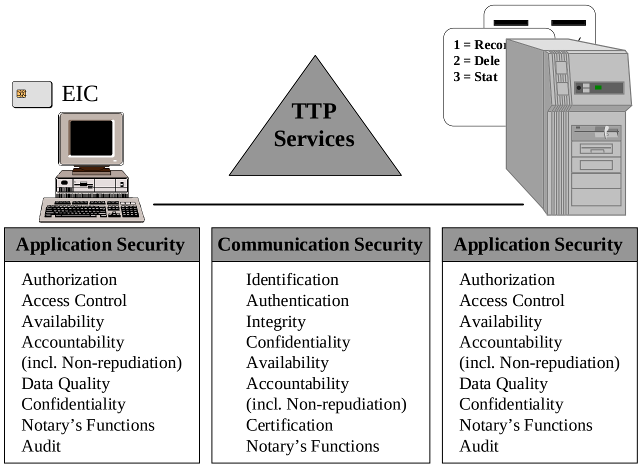

Figure 1: General Security Model

4 Domain Model

In the mentioned case of "Shared Care", an increasing number of different persons from different organisations use different methods at different times, forming temporary (or permanent) teams with the purpose to provide optimal health as physical, psychical and social well-being to the patient. To keep such complex "Shared Care"-supporting information systems manageable and operating, components of the system are grouped by common organisational, logical, and technical properties into domains. This could be done for common policies (policy domains), for common environment (environment domains), or common technology (technology domains) [4, 15].

A policy describes the legal framework with rules and regulations, the organisational and administrative framework, functionalities, claims and objectives, agreements, rights, duties and penalties, and the technological solution of information systems. Regarding the flexibility in handling properties and policies, the domain is of a generic nature, consisting of subdomains and building superdomains.

The smallest domain is the working place or sometimes even specific components of a computer (e.g. in the case of server machines). The domain will be extended by chaining subdomains to superdomains, which are characterised by specific policies. Such transaction-concrete policy has to be negotiated between the communicating and co-operating principals, which is also called policy bridging.

5 Network Security

Increasingly, the distributed architecture of shared care information systems is based on networks. Due to their user friendliness, the use of standardised user interfaces, tools and protocols, and therefore their platform independence, the number of really open information systems based on the Internet or Intranets (corporate networks, virtual private networks) has been growing during the last couple of years.

From the security point of view, a domain ensuring intradomain communication according to their own policy is commonly considered with need of protection only at its boundary against the external domains with their specific policies (or even the policy-free domain of the Internet). This is done by, e.g. with firewalls, proxy servers etc. Regarding the external environment, a domain is therefore often handled as a closed system (e.g. Intranet). Thereby, the internal domain is assumed as secure, often neglecting internal threats and attacks. However, we should mention, that most of the security attacks are caused by insiders. Investigations have shown, e.g., that about 70% of the attacks in German health information systems and even about 95 % of such attacks in US health care domain are caused by insiders. Therefore, the solution recommended is the realisation of networks of distributed security, also called end-to-end security networks or Virtual Private Networks (VPN) not only between the domains but also inside of them.

In the case of forming a common domain of communication and co-operation, there is a need to establish an agreed security policy (Figure 2), also called policy bridging.

Most of the security services currently available are based on system authentication (Kerberos, IPSec ...) [7, 14]. Regarding the specific requirements and conditions of healthcare, the underlying security model must consider the whole spectre of security services and mechanisms. Thus finally, a more realistic concept is solely that of secure micro domains only [3, 4, 6].

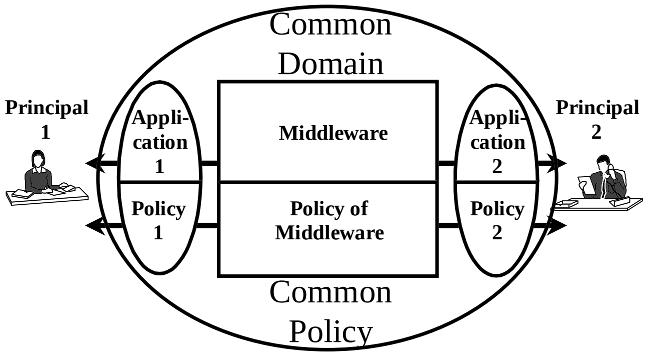

Figure 2: Policy Bridging

The need for strong user authentication is essential for all business which requires accountability (and audit) for legal or ethical reasons. A further service related to the user's secure identity is the confidentiality of information and procedures. Additionally, the demand of user authentication in healthcare is caused to fulfil the „need to know“ principle, to accept the privacy of patient's information, to bind information to the care purpose, and to facilitate the trustworthy doctor-patient relationship. Therefore in Europe, but increasingly also in other regions of the world, security tokens as personal and/or professional smart cards (chip cards with a crypto controller), in the future combined with biometric measures, have been introduced. They keep private keys and provide security services as authentication, digital signature, and encryption. As general security services and mechanisms independently of the Internet, cards and card readers, as well as principles and tools of the security infrastructure like TTP services are currently under standardisation [20, 21]. Security tokens as smart cards and the related TTP services are discussed in more detail in [10] in this volume.

6 Domain Interoperability

Any kind of communication internally to a domain is called an intradomain communication, whereas the communication between domains is called an interdomain communication. For example, communication could be realised between departments of a hospital internally to the domain hospital (intradomain communication), but externally to the domain of a special department (interdomain communication).

The general purpose of communication is the provision of services to a client requesting these services. Most of the services have to be provided by the functionalities of the healthcare information system often combined with human users interactions. Such application services are end-system services, indicating the case that the communication domain is only providing communication services but not additional application functionalities (see figure 3). Application security services are restricted to the requested principals' domain.

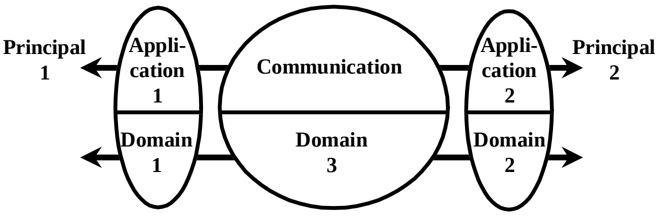

Figure 3: Domain Concept with Pure Communication Services

Currently, increasingly middleware concepts will be introduced into the practice of healthcare information systems [5]. In that case, requested services have been provided by both principals or the middleware. Such architecture could be presented by chains of different domains as shown in figure 4.

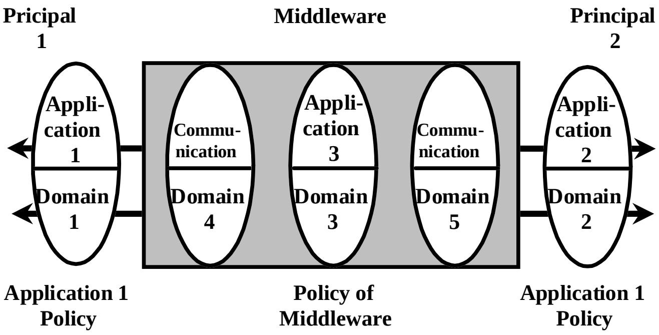

Figure 4: Domain Concept with Middleware Services

7 User Related Security Services

Sharing care and the resulting communication and co-operation in healthcare have to be person-related, also considering the ethics of the doctor-patient-relationship, the liability and legally binding property of business processes as well as the corresponding security services like authentication and digital signature [18, 19, 20, 21]. But also application security services as access control depending on structural or functional roles have to be person-related. 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.

An appropriate tool to provide person-related security services bearing information items needed as cryptographic keys or 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 means [20]. 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 functionalities as patients' medical data on Patient Data Cards (PDC) or patients' insurance cards.

Patient Data Cards (PDC) are smartcard-based medical application systems. Ensuring patient's informational self-determination, a PDC requires a specific access control management to keep the security level and trustworthy relationship guaranteed to the patient [4, 18]. Involved into the DIABCARD project [16] of smartcard-based information systems funded by the European Commission and supporting communication and co-operation of diabetes care, the Magdeburg Medical Informatics Department provides user-related security services. The combination of smartcard-based medical application systems and networked architectures is mediated by pointers on the PDC referring to information securely stored in databases within the net. The access to that information is controlled by the strong authentication of both the patient and the doctor using their EIC and by such a way electronically expressing the patient's consent.

8 The European Health Professional Card

Facilitated by several projects funded by the European Commission, the Health Professional Card (HPC) 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 allow communication and co-operation across the national borders, architecture and interfaces providing access to the card are currently in the process of standardisation at the international (ISO) or European scale (CEN). Also card readers and interfaces to the hardware and software components of the application environment must be agreed on. And EC-funded projects, e.g. TrustHealth [20], CARDLINK, and DIABCARD [16] are providing corresponding specifications. The management of generation, distribution, and revocation of keys, certificates or even cards as well as the provision of corresponding information services as public directory services, often summarised as card management, require an appropriate infrastructure of national or pan-European Trusted Third Party (TTP) services.

Within the regional distributed cancer registry of the Magdeburg Medical Informatics Department, the use of Health Professional Cards within a pilot scenario according to the TrustHealth specification has been implemented and will be expanded during the next project phase [8, 20]. The technical solution is already described, e.g., in [3, 8] and is going to be further developed in accordance with the new German specification for an electronic doctors' licence [13]. Further details about the (European) HPC and the TTP services needed are demonstrated in [10] in this volume.

9 Internet Based Security Infrastructure

Beside of the network security services mentioned above, currently, several projects (e.g. EUROMED) funded by the European Commission aim the development of a pan-European healthcare network based on the Internet and its WWW tools. In the EUROMED context, security infrastructures based on standardised hierarchical TTP structures have been installed by the EUROMED-ETS project [17]. They are managing a Public Key infrastructure and the related mechanisms, providing Certificate Authorities as well as cross certificates to other TTP hierarchies.

The first distributed international TTP architecture in healthcare has involved the pilot sites University of Athens in Greece (ICCS), University of the Aegean in Greece (UoA), University of Calabria in Italy (UniCal), and University Hospital of Magdeburg in Germany (UHM) [14].

Using the example of the Magdeburg UHM part of the solution, figure 5 presents the hierarchical TTP structure of this distributed international healthcare EUROMED-ETS TTP architecture. The 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 [17] 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).

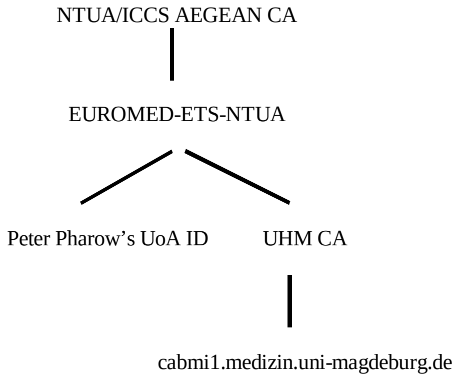

Figure 5: Schema of the Hierarchical TTP Structure

Internet tools as browsers are being completed with security functionalitiesl. Important Internet application environments as, e.g., Java have got 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 last IMIA WG4 Working Conference, 22-25 November 1997 in Osaka/Kobe, Japan in [7].

10 EDI Security Requirements

Communication and co-operation between providers within an organisation and just right between different organisations require especially in the healthcare domain extended security services to respond to the security requirements in health information systems.

In the EDI environment the threat model consists of at least two principals those are authorised to perform message transmissions to each other using several communication protocols over various infrastructures. Threats are active user (attacker) interactions causing the systems' vulnerability. According to the security policy, threats, vulnerabilities and accepted risks cause the security requirements fulfilled by appropriate security services. The following consideration is based on the common security model distinguishing the concepts of communication security rather globally controlled and application security rather locally controlled. Each of these concepts defines a set of security services, which are provided by sets of security mechanisms based on security algorithms applied to data. The different levels of granularity allow views of different groups of users (medical users, system administrators, implementers) within the same specification framework. Additionally, for implementation also the protocol-services-mechanisms relationships looking for standards and products have to be considered.

An unauthorised principal may try to attack the communication system using passive (as monitoring, listening and sniffing of data system exploration, traffic analysis) or active (as creation, insertion, deletion and replay of data) techniques. For example, this may enable the intruder to perform masquerading.

11 Security Model for EDI Communications

Regarding health information systems' security, internal security services provided by the communicating and co-operating information systems and the communication infrastructure can be distinguished from external security services provided by Trusted Third Parties (TTP) [10, 20, 21]. The internal security services needed are strong authentication, integrity, confidentiality and non-repudiation of origin and receipt (figure 8).

12 Protocol Relationships of Security Services

To realise secure distributed health information systems, different protocols enable security services on different levels of the ISO OSI model of open systems' communications as shown in table 1.

Table 1: Placement of Security Services

Security Services OSI Layers	Confi-dentiality	Integrity	Entity Authenti-cation	Data Origin Authenti-cation	Non-Repudiation of Origin	Non-Repudiation of Receipt
Data Link	SILS/SDE, PPTP, L2TP	SILS/SDE, L2TP	PPTP, L2TP, L2F	SILS/SDE, L2TP	–	–
Network	IPSEC, NLSP	IPSEC, NLSP	IPSEC, NLSP	IPSEC, NLSP	–	–
Transport	SOCKS, TLSP, SSL, TLS, PCT, SSH	SOCKS, TLSP, SSL, TLS, PCT, SSH	SOCKS, TLSP, SSL, TLS, PCT, SSH	TLSP	–	–
Application	SHTTP, SPKM, MHS, MSP, PEM, SFTP, PGP/MIME, MOSS, S/MIME, PKCS#7	SHTTP, SPKM, MHS, MSP, PEM, SFTP, PGP/MIME, MOSS, S/MIME, PKCS#7	SHTTP, SPKM, SFTP	SHTTP, SPKM, MHS, MSP, PEM, SFTP, PGP/MIME, MOSS, S/MIME, PKCS#7	SHTTP, SPKM, MHS, MSP, PEM, SFTP, S/MIME, ESS	SPKM, MHS, MSP, SFTP, S/MIME, ESS

The general solution for EDI security including the HL7 communications standard are two types of security services sets providing strong authentication, integrity check, confidentiality of messages transferred and non-repudiation of both origin and receipt. On the ISO OSI model application layer, the first one realises secured messages wrapping the information presented in a standardised format, e.g. HL7, EDIFACT, XML, MIME (figure 6) by security mechanisms like digital signature or encryption. This solution is also called “Secure Objects”. The second security services set establishes a “Secure Channel” on the ISO OSI model transport layer. Examples of that solution are SSL, TLS, SSH, Socks. Keeping the generic character of our approach, we refer any solution to the security services and to the corresponding concept-service-mechanism-algorithm-data relationship. Regarding the concrete implementation of secure EDI using different transport protocols, the handling of control data and application data must be considered separately. These details have been specified in the corresponding MEDSEC project deliverables [11, 12].

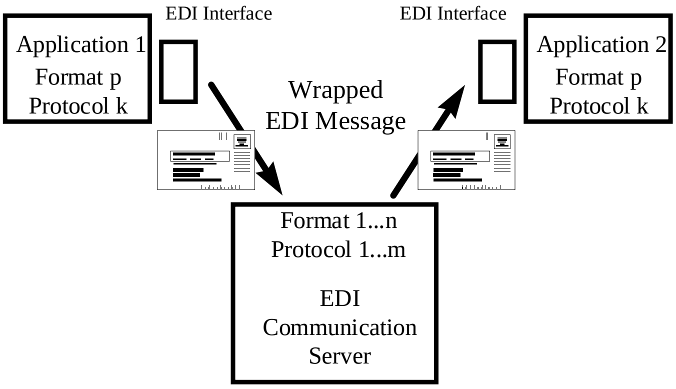

Bild 6: EDI Communication Security

14 Middleware Security Architecture

Another approach to security solutions is based on the OMG group work results. This work should only be mentioned here. Within the CORBA security specification [15], principals are acting on behalf of human users, systems or applications. In our security approach, the person-related user authentication is provided externally. Therefore, there is no need to instantiate the Principal Authentication object internally. The CORBA security services are used as described in detail in [6].

15 Conclusions

The results presented are part of international standardisation bodies’ activities (HL7, ANSI, CEN) as well as of national and international initiatives to provide pilot solutions for secure health information networks. In that context, in the Magdeburg region a secure Onconet supporting cancer patients’ “Shared Care” is under development. Security in health is not restricted to the technology which is available now. Ethical and social requirements including education, training to increase the users’ awareness are a huge challenge.

16 Acknowledgement

The work illuminated and reflected in the current paper was supported within the "Telematics Applications Programme" (TAP) framework of the European Union, and by the Ministry of Education and Science of the German Federal State Saxony-Anhalt. The authors are indebted to thank the colleagues of the related projects, the industrial and research partners, and the CORBA community.

References:

[1] Barber B, Treacher A, and Louwerse K (eds.) (1996) *Towards Security in Medical Telematics*. IOS Press, Amsterdam.

[2] Blobel, B. (1997) Clinical Record Systems in Oncology. Experiences and Developments on Cancer Registries in Eastern Germany, in *Personal Medical Information - Security, Engineering, and Ethics* (edr. R. Anderson), pp 39-56. Spinger, Berlin, New York 1997.

[3] Blobel B. (1997) Security requirements and solutions in distributed Electronic Health Records, in *Information Security in Research and Business* (eds. L. Yngström, and J. Carlsen), pp. 377-390. Chapman & Hall, London.

[4] Blobel B, Bleumer G, Müller A, Flikkenschild E, and Ottes F. (1996) Current Security Issues Faced by Health Care Establishments. *Deliverable of the HC1028 Telematics Project ISHTAR*, October 1996.

[5] Blobel, B., Holena, M. (1997) Comparing middleware concepts for advanced healthcare system architectures. International Journal of Medical Informatics 46 (1997) pp. 69-85.

[6] Blobel, B., Holena, M. (1998) CORBA Security Services for Health Information Systems. International Journal of Medical Informatics 52 1-3 (1998) pp 29-38.

[7] Blobel, B., Katsikas, S.K. (1998) Patient data and the Internet - security issues. Chairpersons' introduction. International Journal of Medical Informatics 49 (1998) pp. S5-S8.

[8] Blobel, B., Pharow, P. (1998) Securing Medical Record Systems by Smart Cards and TTP Services in Heterogeneous Networks Including the Internet. Proceedings Manual (Sup.) of the Conference „Toward An Electronic Health Record '98", San Antonio. Newton, 1998, pp 28-33.

[9] Blobel, B., Pharow, P., Roger-France, F. (1999) Security Analysis and Design of Secure Health Information Systems Based on a General Conceptual Security Model and UML. HPCN Europe ´99. April 12-14, 1999, Amsterdam, The Netherlands. In press in Lecture Notes in Computer Sciences. Springer, Berlin, New York 1999.

[10] Blobel. B, Pharow, P. (1999) European Trusted Third Party Services for Internet Security. In this Volume

[11] Blobel, B, Spiegel, V, Krohn, R, Pharow, P, Engel, K. (1998) Standard Guide for EDI (HL7) Communication Security (Draft). ISIS MEDSEC Project, Deliverable 30, August 1998.

[12] Blobel, B, Spiegel, V, Krohn, R, Pharow, P, Engel, K. (1998) Standard Guide for Implementing EDI (HL7) Communication Security (Draft). ISIS MEDSEC Project, Deliverable 31, August 1998.

[13] HPC Specification (1999) Draft version 0.81 of the Specification of the German Doctors' Licence including the Specification of related Certificates. http://www.hpc-specification.de

[14] Katsikas, S.K., Spinellis, D.D., Iliadis, J., Blobel, B. (1998) Using Trusted Third Parties for secure telemedical applications over the WWW: The EUROMED-ETS approach. International Journal of Medical Informatics 49 (1998) pp. 59-68.

[15] OMG (1995) The CORBA Security Specification. Framingham: Object Management Group, Inc., 1995, 1997.

[16] The DIABCARD3 Consortium. *Improved Communication in Diabetes Care Based on Chipcard Technology*. Project of the Fourth EU Health Telematics Applications Programme. http://www-mi.gsf.de/diabcard

[17] The EUROMED-ETS Consortium. *EUROMED - European Trust Structure*. Information Society Standardisation Programme. http://euromed.iccs.ntua.gr/

[18] The ISHTAR Consortium. *Implementation of Secure Health Telematics Applications in Europe*. Project of the Fourth EU Health Telematics Applications Programme. http://www.ehto.be/projects/ishtar/

[19] The SEISMED Consortium, (edr.) (1996) Data Security for Health Care. Volume I-III. Studies in Health Technology and Informatics, Vol. 31-33. IOS Press, Amsterdam.

[20] The TrustHealth Consortium. *Trustworthy Health Telematics 1, 2*. Project of the Fourth EU Health Telematics Applications Programme. http://www.ehto.be/projects/trusthealth/

[21] The TrustHealth Consortium (1997) Report on TTP development projects - German Site. *Deliverable D4.4 of the HC1051 Telematics Project TrustHealth 1*, July 1997.