ONCONET: A SECURE INFRASTRUCTURE TO IMPROVE CANCER PATIENTS' CARE

B. Blobel

Medical Informatics Department, Magdeburg University Hospital, Magdeburg, Germany

Abstract: The shared care paradigm is the current response to the crisis of industrial countries' health systems. The underlying information systems have to meet the shared care paradigm of communication and co-operation between all the partners involved in. This communication and co-operation must be provided in a secure way. The paper presents the required security infrastructure which has been analysed, specified, and developed within the TrustHealth projects funded by the European Commission. Meeting the challenges of the TrustHealth-2 project for large scale implementations of secure real applications, the ONCONET has been established in the German federal state of Saxony-Anhalt facilitating the shared care of cancer patients. Both security infrastructure and application functionalities are demonstrated in some detail.

Keywords: Cancer Care; Shared Care; Health Networks; Security; Health Professional Card; Trusted Third Party Services; Public Key Infrastructure

INTRODUCTION

The challenge for increased efficiency and improved quality of the health systems in all developed countries can only be met by specialisation, decentralisation, transparency of processes, procedures and outcome as well as by certain competition for best practice. In such a framework, the provision of optimal care to the patient as a whole strongly requires extended communication and co-operation between the patient and all the partners in the health care domain. This includes care providers such as GPs and hospitals, aftercare organisations, but also service providers as pharmacies, laboratories, etc, health system sponsors and facilitators like private and public insurance companies, governmental and other health-related institutions. But even complex health provision structures themselves such as health maintenance organisations (HMOs) or health care establishment clusters organised in Community Health Information Networks (CHINs) have to establish extended interoperability between their components. The information exchanged and the services provided are sensitive in the sense of personal privacy of patient or staff involved as well as confidentiality of business information etc. Furthermore, they are exposed to different threats and risks. Therefore, communication and co-operation require appropriate security services to be implemented according to the policy agreed [4, 28]. This paper focuses on the security of personal medical information. As the different institutions involved in the health care system have a different distance to the patient's care, they have different needs for access to personal medical information and therefore also different needs for specific security services. The paper describes security requirements and solutions in the context of a real medical routine application.

THE ONCONET ENVIRONMENT

As mentioned in the introduction, there is no alternative for patient's shared care itself requiring shared information systems. The ONCONET is an approach to improve care of cancer patients in an area like a German federal state by open communication and co-operation according to the care process requirements and to the patient's consent. The kernel of the ONCONET consists of the regional Clinical Cancer Registry Magdeburg/Saxony-Anhalt which currently comprises 57 clinics and more than 160 GPs specialised or at least commonly involved in the domain of oncology. The GPs are organised in the Oncological Aftercare Organisation of the Doctors' Statutory Association ("Kassenärztliche Vereinigung") of the German federal state Saxonony-Anhalt ("KV Sachsen-Anhalt"). In the future structure, about 75 clinics and all GPs interested will be online in the ONCONET.

From the beginning in 1993, the Clinical Cancer Registry Magdeburg/Saxony-Anhalt has been established as a regional documentation system for oncology, that could be implemented within the German legislation framework only with appropriate security solutions. To fulfil these requirements, a strong and productive communication and co-operation has been developed between the Medical Informatics Department at the Magdeburg University Hospital and the Saxony-Anhalt Data Protection Ombudsman.

Main functionalities of the Clinical Cancer Registry are the comprehensive documentation of cancer cases according to the Cancer Basis Documentation, the Cancer Extended Basic Documentation and the Organ-Specific Cancer Documentation. Furthermore, the data for the epidemiological cancer registry of the East-German federal states are recorded, packed, encrypted and sent to a central institution called "Gemeinsames Krebsregister der Bundesländer Mecklenburg-Vorpommern, Brandenburg, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen und Berlins" which is located in Berlin. As a registry software, the Giessen Tumour Documentation System (Gießener Tumordokumentationssystem GTDS) has been implemented [2].

Based on the information recorded, processed, stored, and communicated, the registry supports research and development as well as education on cancer. This includes development and assessment of best practice guidelines and quality assurance for cancer care, clinical studies and the organisation and administration of care procedures (including co-ordinated scheduling, creation of doctor's reports). Relying on a comprehensive and highly sophisticated information and communication structure an Electronic Health Care Record (EHCR) system in oncology is provided.

Meeting the growing challenges of the German health care system, the revolution in technology, and the stepwise development of the European legal framework, the first German health care system solutions for secure communication and co-operation have been established step by step in the regional Clinical Cancer Registry Magdeburg/Saxony-Anhalt. Just from the beginning, secure connections to remote clinics have been implemented and routinely deployed using public analogous lines. In 1994, a test implementation of a distributed EHCR system has been provided which was based on the SequeLink® middleware. In 1995, secure connections to the LAN of the Oncological Aftercare Organisation of the Saxony-Anhalt Doctors' Statutory Association have been implemented using public ISDN lines. After the first European implementation of a TrustHealth HPC in the Magdeburg registry environment in 1997, in the same year the first international Internet-based TTP structure for healthcare could be realised including the universities of Athens, Calabria, and Magdeburg. At the same time, a test implementation of a distributed EHCR system based on the CORBA®[1] middleware could be demonstrated. A secure EDI[2] solution meanwhile standardised in US and used, e.g., for HL7[3]

[1] Common Object Request Broker Architecture, the middleware approach of the Object Management Group (OMG) [20]

[2] Electronic Data Interchange

[3] Health Level 7, health industry communication standard [16]

communications and the secure transfer of images has been specified in 1997 and implemented in the Clinical Cancer Registry in 1998. After specifying and implementing a security solution for secure patient data card (PDC) applications (DIABCARD), in 1999 the implementation of the Saxony-Anhalt ONCONET started. Most of the mentioned solutions being presented in the following sections in more detail are innovations on international scale.

THE ONCONET SECURITY INFRASTRUCTURE

At the beginning, the security solutions of the Clinical Cancer Registry were based on system-related security services using symmetric cryptographic algorithms at the beginning or dedicated key management in case of asymmetric algorithms in the ISDN environment respectively. Because of the legal, ethical and organisational requirements in health regarding the user and his/her accountability, user-related security services were being specified and implemented in the Magdeburg registry environment. The implementation of a large scale network secured by user-related services requires an appropriate Public Key Infrastructure (PKI), however. Requirement analysis, specification of corresponding security tokens, services, and mechanisms have been the issues of the European Commission funded project "TrustHealth-1" the Magdeburg Medical Informatics Department has been involved in [5, 6, 30]. For analysis of system requirements, system design, specification, implementation, and maintenance, a generic component model approach and the Unified Modelling Language (UML) methodology have been applied [8, 9, 15]. The usability of the methodology regarding the composition of different levels of abstraction and granularity enabling different views has been demonstrated in [3].

SECURITY SERVICES BEING ADDRESSED

Security is a very complex concept considering security, safety and quality as important prerequisites for trustworthy communication and co-operation via computerised information systems. Subsequently, only the security concept will be considered, which is separated in sets of communication security services and application security services. Nowadays, most of them are realised using cryptographic algorithms.

Communication security services are

- identification and authentication of principals (users, systems, devices, applications, components, objects) including the control of access to them,
- their accountability,
- integrity, confidentiality, and availability of communicated information as well as
- notary's functions.

Application security services comprise

- authorisation, access control, and accountability of principals for recorded, stored, and processed information,
- confidentiality, accuracy, and availability of information and procedures,
- audit as well as
- notary's functions.

The principals' identity (ID) may be specified at "global" level and is rather stable in time. Some identity-related attributes are valid at least on a national or state level such as roles in the sense of qualifications and permissions. Application security services as, e.g., authorisation and access control, however, depend additionally on concrete local and actual requirements and conditions expressed by a specific policy. Therefore, these services must be managed locally according to the policy established.

Identification and authentication are basic security services enabling most of the other security services for both communication and application. In an open environment as well as for legal reasons, identification and authentication but also identity-related services and attributes need to be certified. Depending on the scale of certification, decentralised Trusted Third Party (TTP) structures using cross-certificates or centralised ones can be established. Therefore, security infrastructures for trustworthy information systems particularly concern identity and authentication and identity-related services, but in some countries like, e.g., Germany additionally identity-related issues such as roles (see the next sections).
Regarding the security services mentioned, only the communication security availability service has not yet been implemented in the registry.

HEALTH PROFESSIONAL CARDS

Confirming and continuing the ”Trusted Health Information Systems” (THIS) project chaired by Gunnar Klein [29], smart cards have been defined as appropriate tokens securely bearing both the private keys needed for authentication, digital signature, and decryption (e.g. of session keys) on the one hand and the certificates for that keys on the other hand. Beside this identity-related (identity card) functionalities, some attributes concerning profession, professional qualifications and permissions to practice, but also other profession-related owner-linked information (e.g., exposition of radiologists to radiation) are certified and stored on the card extending its character to an Health Professional Card (HPC). Contrary to the identity-related certificates, attribute certificates are not bound to keys. Generalising that principle, card functions may be separated according to certificates applied as ID certificates, professional and organisational certificates, and application-specific certificates. More details on HPC are given in [5]. Suggesting open solutions, RSA[4] has been favoured as the algorithm to be used. RSA, however, needs a crypto-co-processor for processing the algorithm which extremely increases the costs for cards [23]. Therefore, alternatives are under development and exploration as, e.g., elliptic curves only using the standard smart card.
Another usage of smart cards storing and processing sensitive personal information is the Patient Data Card (PDC) realising the concept of the patient’s informational self-determination. Such MPC[5]-based health information system could contain specific data as the patient’s emergency data set agreed on the ISO level, or essential information supporting the care of special diseases such as diabetes (DIABCARD) [10, 25]. As a further PDC function a pointer to patient’s EHCR locations managed by the patient himself/herself could be imagined. These exemplified functionalities should be combined with identity card functions.
Within the TrustHealth-1 project, only the Magdeburg Medical Informatics Department was able to implement a real TH.HPC according to that specification in the sense of the feasibility study required.
Meanwhile, the HPC has been standardised on the European level as CEN prENV 13729 “Health Informatics – Secure User Identification – Strong Authentication using Microprocessor Cards” [14] as well as consistently on the German national level as the HPC Protocol [17]. The ONCONET Saxony-Anhalt is based on the TH.HPC described fully implementing the features mentioned.

TRUSTED THIRD PARTY SERVICES

In order to deal with security services based on asymmetric cryptographic algorithms, a PKI or TTP structure is inevitable. A TTP summarises all the structural components which provide TTP services and belongs to one or to several organisations. Beside the fundamental work of

[4] Asymmetric cryptographic algorithm developed by Rivest, Shamir and Adelman
[5] Microprocessor card, integrated circuit card (ICC)

the European TrustHealth project, several other projects have been launched by the European Commission in the framework of "European Trust Services – ETS" over the last three years [26]. The original objective of ETS was the investigation and possible resolution of issues related to the creation of an environment by industry and commerce to deal with health information in a secure way. Such environment shall enable the use and provision of security services related to principals or procedures such as authentication, non-repudiation, confidentiality and time stamping. These services may be offered by pan-European Trusted Third Party Service infrastructures, as required by the market.

ETS has addressed the resolution of the issues and the measures necessary for the design, specification and market-driven implementation of a European TTP Service infrastructure which will support the information security services needed to enable the European and global information society. Such an European information infrastructure for health has been piloted in a series of EUROMED projects for creation of a pan-European Internet-based health network. Within the EUROMED-ETS project, such a pan-European TTP Service infrastructure has been established practically between Greece, Italy and Germany in 1997 including the universities of Athens, Calabria, and Magdeburg [5, 20, 27].

The goal of ETS has been to tackle, to the greatest possible extent, technical, economical, legal and regulatory aspects that govern the use of cryptography for authentication, confidentiality and non-repudiation, and to resolve the dilemma posed by the increasing importance of encryption in our information society.

Simply summarised, the paper-based world must be transferred properly to an electronic counterpart. Considering identification, authentication, and certification of persons and her professional attributes, figure 1 formally describes the equivalencies to be provided.

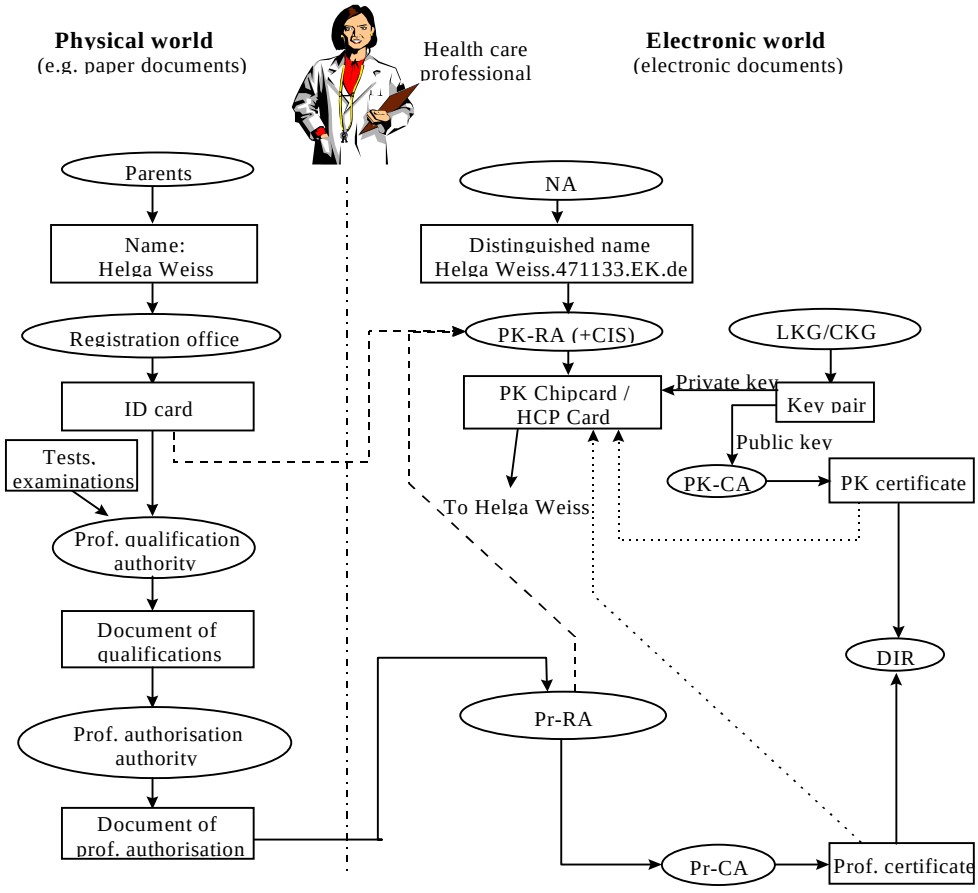

Figure 1: Electronic vs. Paper-Based World

The TTP generates and issues the cards, certifies the public keys, and combines them with valid timestamps. The certificates held in a directory (directory service, revocation service) must be permanently available for enabling signature checks (authentication and integrity service) as well as the sending of encrypted data (confidentiality service). All user-related information as, e.g., the personal identity, professional qualifications and specialities are stored in certificates.
As mentioned above, the certificates may be hold on the card for off-line checks. However, this implies possible disadvantages in the context of updating and revocation of certificates in time.
To describe the structure of 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 objectives: 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.
In the following context, a user is an individual or organisational entity. A Public Key Registration Authority (PK-RA) is an entity which uniquely identifies and registers users applying for the Digital Signature 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 that appoints unique certificate names to users. The NA 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 that certifies the linkage between the unique certificate name and the user's 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) 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 issues chip cards containing (at least) the private keys of the users (card owners) for authentication, signature, and decryption. 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 key pairs required. 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.
TTP services specifically needed to influence functionality and security in the health care sector should be established in health care institutions as the Physician Chambers or the Doctors' Statutory Association as proposed by the German ATG[6] and implemented for the ONCONET solution. Such services are, e.g., NA, Pr-RA, Pr-CA, LKG, PK-RA, and DIR. Regarding the other roles, the requirements are considered to be general requirements for overall confidence in TTP services provided in relation to the specified security policies and other relevant elements also by organisation outside of the healthcare domain like governmental, private, or commercial ones. More information might be found in [22].
As long as not all health professionals are organised in health professional chambers, a TTP structure for health must be established fulfilling both the legal framework and common

[6] "Aktionsforum Telematik im Gesundheitswesen, an initiative of the German health system representatives [1]

requirements. Therefore, some authorities – needed for provision of certain services – must be implemented separately in the cancer center framework. For protection of investment in technology and organisation, as much authorities as possible have been installed within the future chamber structure, by that way fulfilling basic requirements of the German HPC framework [17]. Figure 2 presents the actually implemented ONCONET TTP services and role schema.

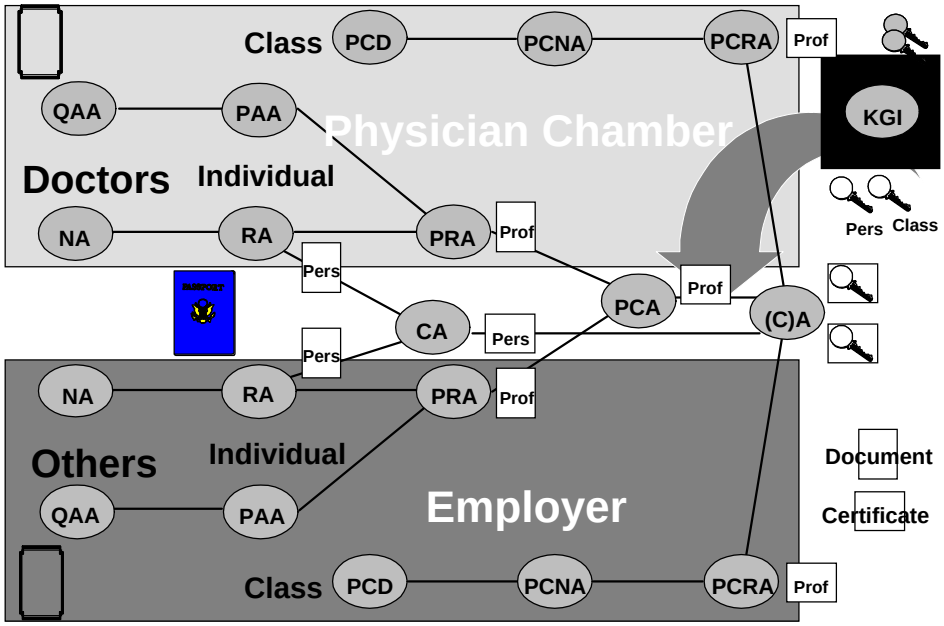

Figure 2: TTP Structure of the Saxony-Anhalt ONCONET

The procedure of HPC order and delivery is presented in the figure 3 as an UML sequence diagram.

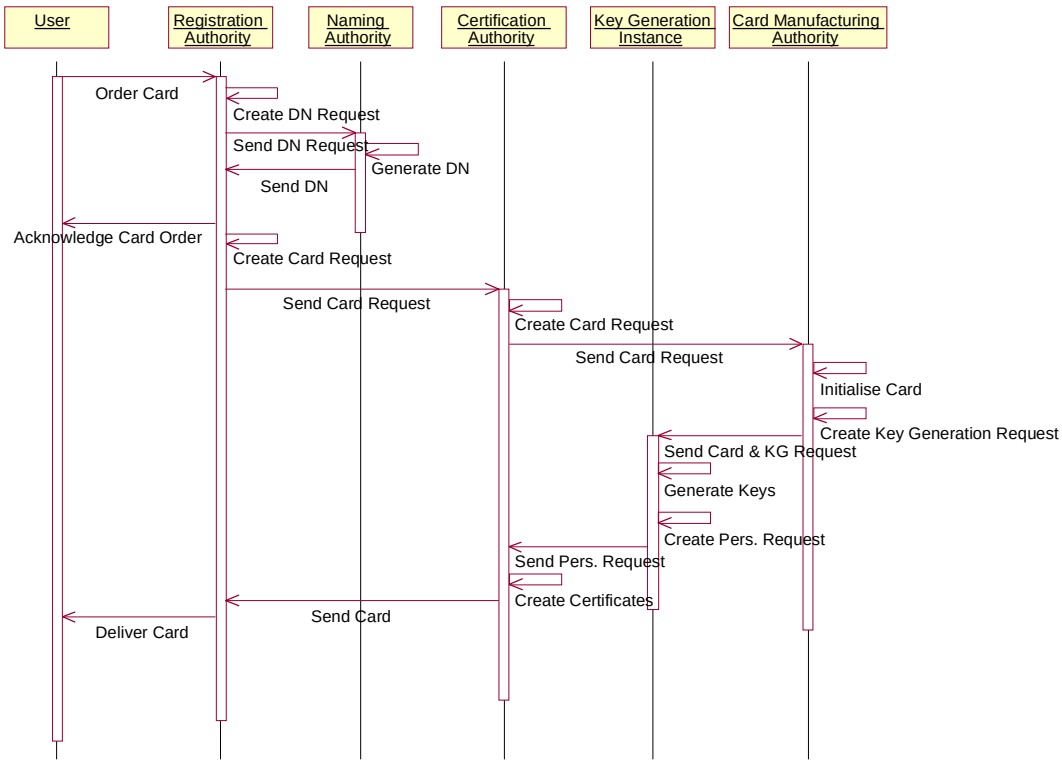

Figure 3: Sequence Diagram of Card Ordering and Delivery

THE SECURE ONCONET SOLUTION

The ONCONET enables secure communication between the regionally distributed users as well as between them and the comprehensive cancer documentation established at the Clinical Cancer Registry. For that reason, additionally to the communicating systems an infrastructure for trustworthy communication has been installed consisting of a communication server, a proxy server for functional interoperability, and appropriate TTP services. As an interim solution, the CA Management System of the SECUDE GmbH Darmstadt, developer of the SECUDE™ (Security Development Environment) products used in our environment, has been applied [24]. Figure 4 shows the principle architecture of the ONCONET solution.

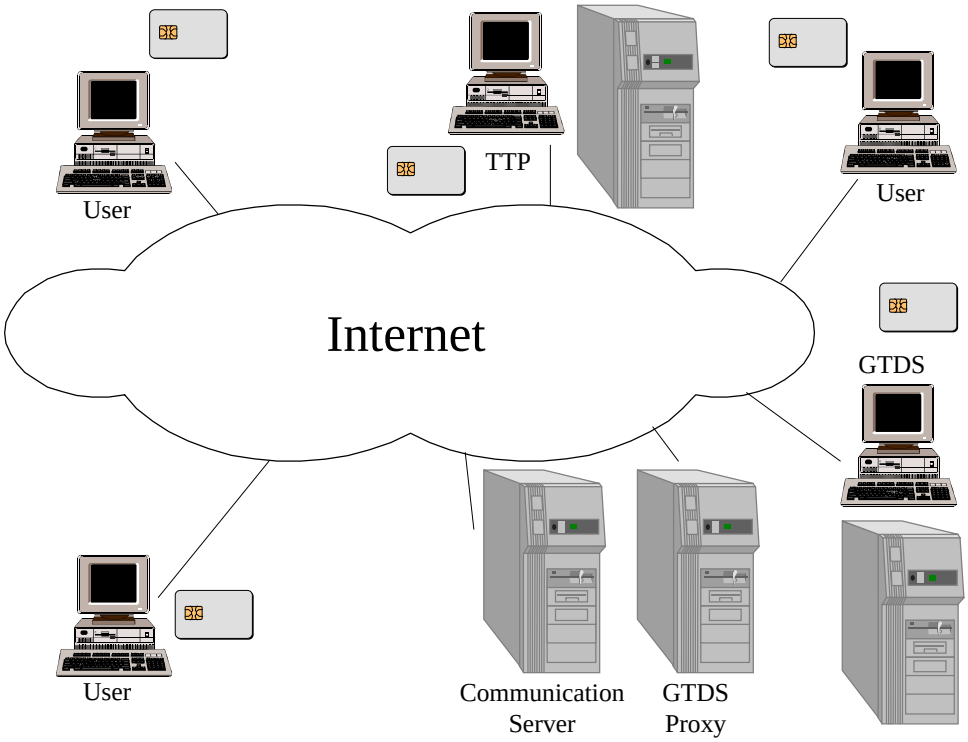

Figure 4: Saxony-Anhalt ONCONET Schema

Starting with a high level of abstraction and a low level of granularity, figure 5 presents the UML use case diagram for secure asynchronous communication between health professionals (i.e. the doctor responsible by law) and the Medical Documentation Assistants at the registry site for transferring the doctor's report.

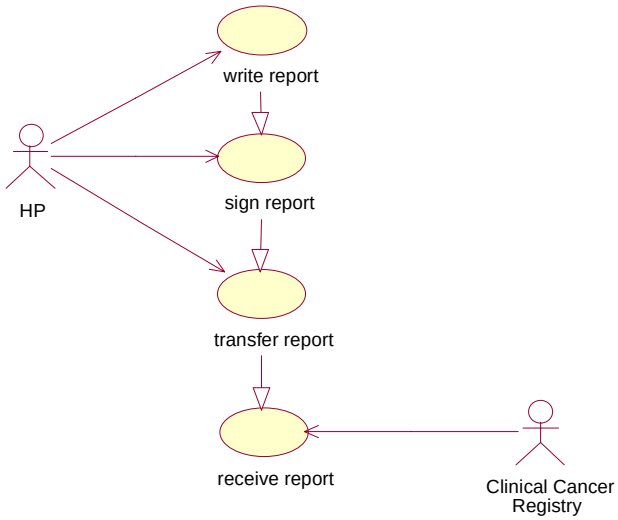

Figure 5: Use Case Diagram of Doctor's Report Transfer

Usually, the doctor's report will be created using text processor systems such as Microsoft Word. The report communicated has to be integer and confidential. The user must be authorised for communication. Additionally, his/her professional role as doctor is verified by checking the corresponding attribute certificates. Using both the HPC and the SECUDE development system, a Visual Basic for Application (VBA) macro has been programmed by the Magdeburg Medical Informatics Department that integrates the signature and encryption mechanisms into the Microsoft Word application via a Dynamic Library Link (DLL). The trustworthy communication is based on a strong mutual 3-way authentication according to the ISO specification [18, 19]. Afterwards, the transfer is realised securely via the Secure File Transfer Protocol (SFTP) meanwhile approved as an HL7/ANSI[7] Standard. This universal EDI protocol, which enables the communication of any type of data with unlimited extension, is widely used in many contexts (e.g. also HL7, images) around the world. It is described in more detail in [7, 11, 12, 13]. For legal reasons, all incoming information signed by its originator is securely stored in a separate electronic archive at the register site. Figure 6 shows the sequence diagram giving a detailed description of the procedures of doctor's report transfer.

[7] American National Standards Institute

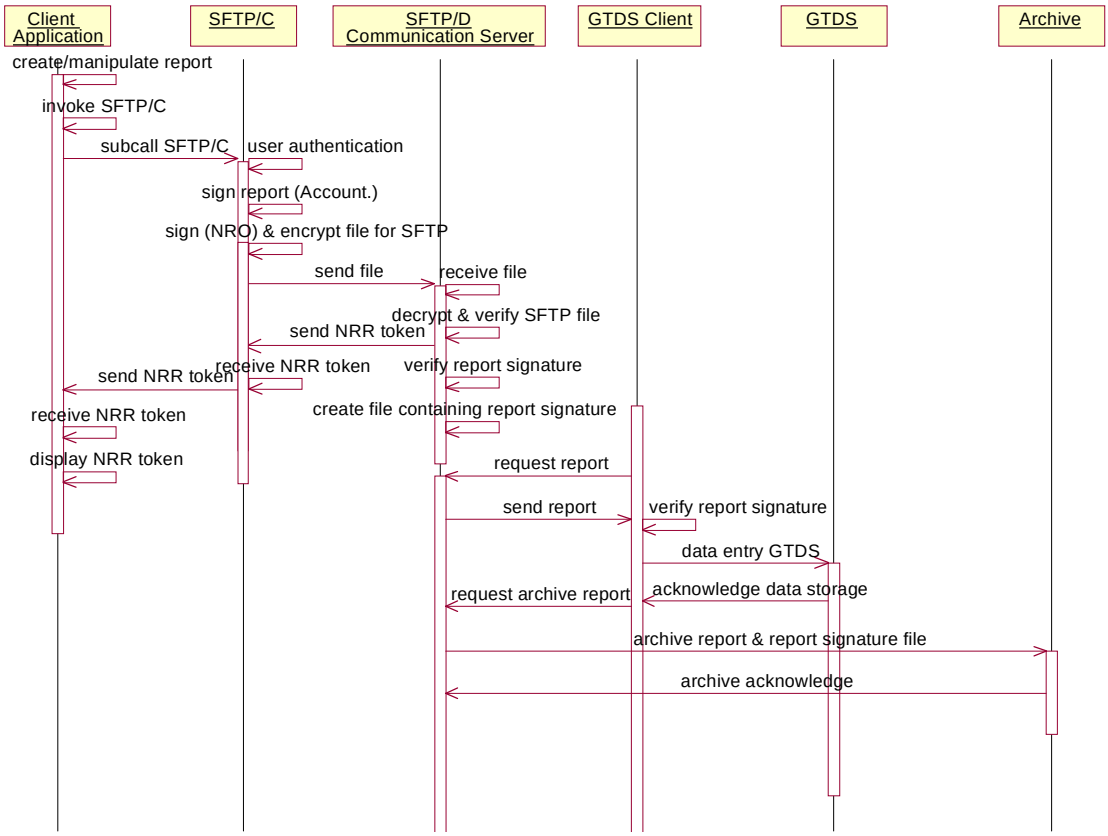

Figure 6: Sequence Diagram of the Doctor's Report Transfer Use Case

A further scenario of ONCONET deals with general communications between network partners as GP - GP on the one hand or GP - clinic on the other hand. Examples for that communication are doctor's report transfer in the context of referrals, discharges, or collegial information, but also agreements or scheduling in reaction of planned activities of the co-caring establishment which are accessible to the partners in real-time. For getting that information from the regional oncological health care record regarding his/her patients, the doctor can retrieve information using Structured Query Language (SQL) queries. The doctor is enabled to transfer the whole health record of one of his/her patients. Furthermore, he/she can get aggregated data of his/her patients by predefined or even free formulated SQL queries. The predefined queries concern "statistical" overviews related to the organisation, to certain entities characterised by specific diagnoses or therapies as well as other care-related information usable, e.g., for process optimisation, research, education, and quality assurance. Figure 7 demonstrates the use case diagram for the request and provision of data from the registry. The refinement of the use cases contained can be realised combining the underlying security-related use case types [8, 9]. The communication between the strongly authenticated principals doctor and record system is provided in a trustworthy way as described above. To protect the registry system, there is no direct user access to it. A proxy retrieves the information on behalf of the user representing his/her role to the system for the right authorisation. On behalf of the register, the data permitted are transferred to the requestor by that proxy in a trustworthy manner, signed and encrypted using the requestor's public key. No unauthorised principal can decrypt the data, if it is listening the communication line.
Figure 8 presents the sequence diagram of the request of patient information by SQL queries.

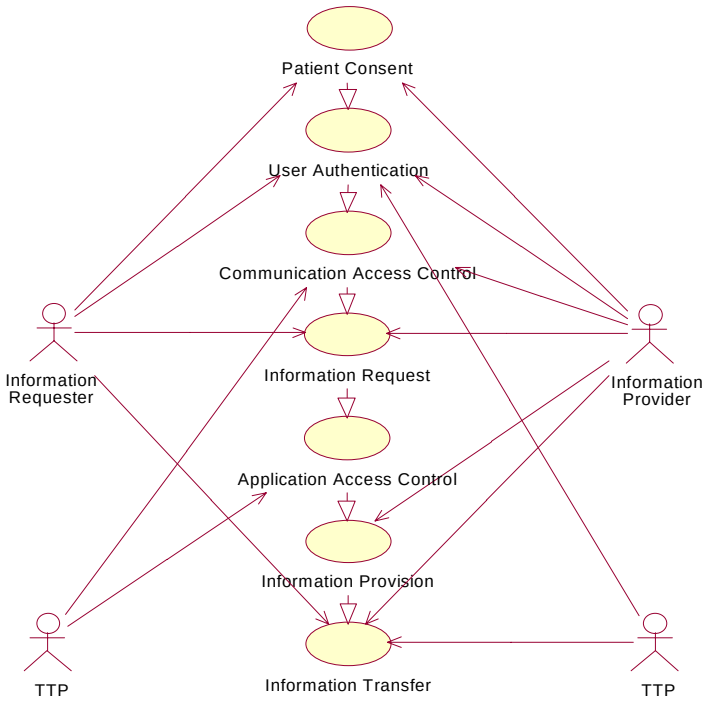

Figure 7: Use Case Diagram of Patient Information Request

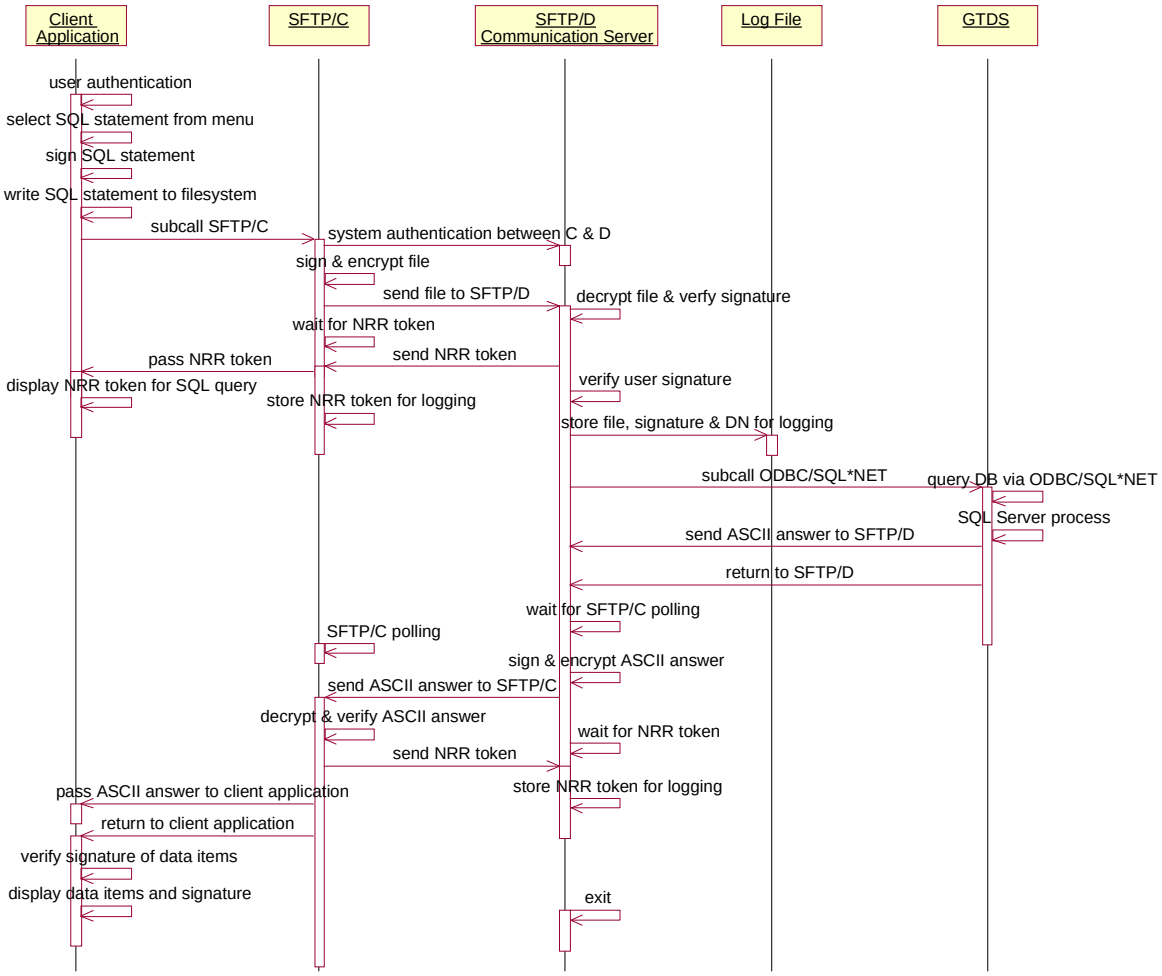

Figure 8: Sequence Diagram of the SQL Query Use Case

Evaluation of the ONCONET Solution

Exploring requirements and possible solutions for a pan-European secure health network, the TrustHealth–2 project was also designed to investigate the legal and organisational framework as well as the social and behavioural implications of secure health networks including cross-border communication and co-operation. Commonly, such assessment has been performed using standardised questionnaires. In some of the six countries involved in the TrustHealth-2 project, also interviews have been deployed [30].

The questionnaire consisted of a demographic part characterising personality, education, professional experiences and facilities of the user also reflecting both the professional and private use of computers. Another part served for elucidation of the user's security awareness. The third part was searching experiences, imagination, evaluation and feeling regarding stability, user-friendliness, comfort and easy to use of IT hardware and software. Collating the results, the influence of acceptance of the solution, the need for integrating the security services in the application environment, and the importance of education and training to achieve appropriate awareness have been derived. Details of the evaluation procedure and results are published in [30, 31].

Due to the long-term experience and education established at the Magdeburg register site with its big number of different successful pilots for security solutions, the evaluation result of the secure ONCONET implementation was much better as that of the partner sites in different countries. Nevertheless, the results achieved confirmed the comments made before.

Conclusions

Embedded in several European projects and supported by many results from our engagement in the American standardisation on IT in health, a trustworthy health network could be specified, developed, and implemented. Contrary to most of the other German health network initiatives supporting some common, not really health-related services such as secure e-mailing, the ONCONET enables communication and co-operation between medical applications. It directly supports medical procedures like planing and organisation of chemo-therapy based on a huge set of therapy schemas, development and provision of clinical guidelines, but also administrative procedures as appointments, scheduling, reports, etc. Furthermore, research and development issues are directly facilitated such as clinical studies, quality assurance, optimisation of diagnosis and therapy as well as epidemiological studies. Finally, education can be enabled. Last but not least, outlines, trends, and decisions can be derived for health policy and administration based on the information available.

Beside those cancer care related services, also common services for health could be established such as doctor-doctor communications mentioned above or the transfer of CT images from external institutions to the University Hospital Magdeburg asking for and getting second opinions.

The ONCONET has been established to improve cancer patients' care. Depending on the success achieved, the network could be expanded as a general health network of the region.

The solution specified, developed, and implemented is based solely on standards. This is true for the security infrastructure based on international, European, and German standards and specifications. For that purpose, standardised HPC for identification, authentication, digital signature, decryption as well as appropriate TTP services (public key infrastructure) have been implemented[8]. Furthermore, the protocols applied follow open solutions and standards

[8] In the future, also special functionalities such as role assignment, education tracking, registration of exposition to particular conditions (e.g., radiation) etc. might be available on the HPC.

widely used, like secure FTP or mailing procedures. As the electronic health care record for oncology, on the cancer registry site a well specified schema for authorisation and access control has been implemented.
The solution presented is one of the European large scale pilots within the TrustHealth project framework, but also the first demonstrator of the German HPC. With the TrustHealth project itself co-operating with other European and international security-related activities, the European Commission aimed to provide a security infrastructure solution for health applicable by the other projects and initiatives launched. Therefore, there was no intention for competing solutions and concepts so far.

ACKNOWLEDGEMENT

The author is indebted to the German and the European TrustHealth-2 project partners. Especially, he'd like to thank the colleagues of his department, of the Physician Chamber Saxony-Anhalt as well as of the health care establishments involved in the ONCONET for their engagement.

REFERENCES

1. Aktionsgemeinschaft Telematik im Gesundheitswesen. http://atg.gvg-koeln.de
2. Blobel B (1996) Clinical Record Systems in Oncology. Experiences and Developments on Cancer Registries in Eastern Germany. In: Preproceedings of the International Workshop "Personal Information - Security, Engineering and Ethics" pp 37-54, Cambridge, 21-22 June, 1996, also published in: Anderson R (edr) Personal Medical Information - Security, Engineering, and Ethics, Spinger, Berlin, New York 1997, pp 39-56
3. Blobel B (2000) Application of the Component Paradigm for Analysis and Design of Advanced Health System Architectures. International Journal of Medical Informatics (submitted).
4. Blobel B, Katsikas SK (1998) Patient data and the Internet - security issues. Chairpersons' introduction. International Journal of Medical Informatics **49,** pp. S5-S8
5. Blobel B, Pharow P (1997) Security Infrastructure of an Oncological Network Using Health Professional Cards. In: Broek L van den, Sikkel AJ (eds) Health Cards '97, Series in Health Technology and Informatics Vol. 49, IOS Press Amsterdam, pp. 323-334
6. Blobel B, Pharow P (1998) Results of European Projects Improving Security of Distributed Health Information Systems. In: Cesnik B, McCray AT, Scherrer J-R (eds) MEDINFO '98. IOS Press Amsterdam, Berlin, Oxford, Tokyo, Washington DC, 1119-1123
7. Blobel B, Pharow P, Engel K, Spiegel V, Krohn R (1999) Communication Security in Open Health Care Networks. In: Kokol P, Zupan B, Stare J, Premik M, Engelbrecht R (eds) Medical Informatics Europe '99, Series in Health Technology and Informatics Vol. 68. IOS Press, Amsterdam, pp 291-296
8. Blobel B, Pharow P, Roger-France F (1999) Security Analysis and Design Based on a General Conceptual Security Model and UML. In: Sloot P, Bubak M, Hoekstra A, Hertzberger B (eds) High Performance Computing and Networking, Lecture Notes in Computer Sciences 1593. Springer, Berlin, Heidelberg, New York, pp 919-930
9. Blobel B, Roger-France F (2000) A Systematic Approach for Secure Health Information Systems. International Journal of Medical Informatics (submitted)
10. Blobel B, Spiegel V, Pharow P, Engel K, Engelbrecht R (2000) Secure Interoperability of Patient Data Cards in Health Networks. In: Hasman A, Prokosch U, Engelbrecht R (eds) Medical Informatics Europe 2000, IOS Press, Amsterdam (in press)
11. Blobel B, Spiegel V, Krohn R, Pharow P, Engel K (1998) Standard Guide for EDI (HL7) Communication Security, http://www.hl7.org
12. Blobel B, Spiegel V, Krohn R, Pharow P, Engel K (1998) Standard Guide for Implementing EDI (HL7) Communication Security, http://www.hl7.org

13. CEN TC 251 (1999) prENV 13608: Health Informatics - Security for Healthcare Communications,
14. CEN TC 251 (1999) prENV 13729: Health Informatics - Secure User Identification – Strong Authentication using Microprocessor Cards (SEC-ID/CARDS)
15. Eriksson H-E, Penker M (1998) UML Toolkit. John Wiley & Sons, Inc., New York
16. HL7 Inc. http://www.hl7.org
17. HPC (1999) The German HPC Specification for an electronic doctor's licence. Version 0.81, February 1999. http://www.hpc-protocol.de
18. International Organisation for Standardisation: Information technology, Open Systems Interconnection, Security frameworks for open systems, multiple Parts (1-7).
19. International Organisation for Standardisation: Information technology, Security techniques, Entity authentication, multiple Parts (1-5).
20. Katsikas SK, Spinellis DD, 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**, pp. 59-68
21. OMG Inc. http://www.omg.org
22. Pharow P, Blobel B (1999) Trusted Third Party Services for Internet Security. In: Mastorakis NE (edr) Recent Advances in Signal Processing and Communications, World Scientific and Engineering Society Press, pp 379-385
23. Schneier, B. (1996) Applied Cryptography. John Wiley & Sons, Inc., New York
24. SECUDE (1999) A General Purpose Security Toolkit. Specification of the SECUDE Software. http://www.darmstadt.gmd.de/secude
25. The DIABCARD Consortium. http://www-mi.gsf.de/diabcard
26. The ETS Projects. http://www.cordis.lu/infosec/src/ets.htm
27. The EUROMED-ETS Consortium. http://euromed.ece.ntua.gr
28. The ISHTAR Consortium. http://www.ehto.org/projects/ishtar
29. The THIS Consortium. http://www.etho.org/projects/this
30. The TrustHealth Consortium. http://www.ehto.org/projects/trusthealth
31. Wenzlaff P, Blobel B, Pharow P (1999) Health Professional Cards: Awareness for Security in Health Care Networks. In: Sicurello F (edr) Health Cards '99, XASI, Milan, pp 121-125

Address for correspondence:

Dr. Bernd Blobel
Head of Medical Informatics
Magdeburg University Hospital
Leipziger Str. 44
D-39120 Magdeburg
Germany
email: bernd.blobel@mrz.uni-magdeburg.de