31

Security requirements and solutions in distributed Electronic Health Records

B. Blobel
Otto-von-Guericke University Magdeburg, Faculty of Medicine
Institute of Biometrics and Medical Informatics
Leipziger Str. 44, D-39120 Magdeburg
phone: +49-391-6713542, fax: +49-391-6713536,
e-mail: bernd.blobel@mrz.uni-magdeburg.de

Abstract

The healthcare systems in all developed countries are changing to labour-shared structures as *Shared Care*. Such structures require an extended communication and co-operation. Medical information systems integrated into the care processes must be able to support that communication and co-operation adequately, representing an active and distributed Electronic Health Record (EHR) system. Distributed health record systems must meet high demands for data protection and data security, which concern integrity, availability, confidentiality including access management, and accountability. Communication and co-operation in information systems can be provided by middleware architectures. For the different middleware architectures used in healthcare as EDI (HL7, EDIFACT), CORBA or DHE, the architectural principles and security solutions are shortly described in the paper. Supporting open information systems, these security solutions are independent of applications and transparent to the user. For trusted communication and cooperation, application-related and user-related security mechanisms are required. Such mechanisms have to fulfil the security policy of the application domain. They are using the basic security mechanisms of the underlying communication- and cooperation-supporting systems.

The discussed policy, threats, and countermeasures are referred to the first German regional distributed medical record, which is developed and step by step refined in the Clinical Cancer Registry Magdeburg/Saxony-Anhalt.

Keywords

Electronic health record, middleware, data security, security services, chip cards, TTP

1 INTRODUCTION

Due to the changed basic conditions of healthcare systems in all developed countries, which are characterised by the demographic development with an increasing number of elderly and multiple-diseased patients, rapidly growing and expensive medical and technical progress, and a generally increasing demand of health services, there is a substantial requirement for efficient and still high quality healthcare. The response of choice is the structural change of healthcare systems enforcing Shared Care, i.e. a continuous and coordinated activity of different care providers including the patient itself to give an optimal medical, psychological and social help to the patient (Blobel, 1996b; Blobel, 1996c). Such distributed, decentralised, labour-shared healthcare structure must be supported by an adequate information system structure, consisting of highly specialised and highly effective components enabled to optimal communication and cooperation. Therefore, these processes are accompanied with improving and extending electronic communication. The content and extent of communication as well as the used both services and communication infrastructure determine new threats, define the need for protection, and facilitate new measures for data security. The consideration here is restricted to issues related to middleware concepts as well as to services and threats within our distributed EHR (DEHR) solution. Communication in healthcare can be characterised by communication content, communication partners, communication infrastructure, and communication services. In a combinatorial way, different communication contents, partners, infrastructure, and services present different communication conditions and lead also to different security threats and requests for adequate countermeasures. A general approach to system security and a categorisation of architectures with respect to their threat models and trust models including an extended discussion of common communication services is given in (Blobel et al., 1996). The paper concerns especial advanced communication services, e.g., provided by middleware systems. Comprehensive guidelines on security of healthcare systems have been published in (The SEISMED Consortium, 1996).

2 SECURITY SPECIFICATION AND DOMAINS

Personal medical data are highly sensitive information. In this context, legal, medical, social, and technical aspects must be considered. For extended communication of such information in Shared Care systems and for trustworthy and non-repudiated cooperation, the basic security dimensions of data integrity, availability, confidentiality, and accountability of information and processes have to be ensured. The latter concerns also the non-repudiation of origin and receipt of data as a basic foundation of interoperability (Blobel, 1996b; Blobel, 1996c; Blobel et al., 1996).

We distinguish the globally manageable *communication security* from the locally managed *application security*, the former dealing with data transfer between two or more authenticated principals (users, processes, devices, etc.), the latter dealing with access of

these principals to application resources (access control, management of rights or privileges) (Blobel, 1996b; OMG, 1995). Therefore, pure communication services as simple middleware services concern communication security, whereas application security is related to the requested and provided application functionality (data or service of the upper 7th OSI layer), but also to advanced middleware services (functionalities). Such services are e.g. the CORBA[1] common facilities. Differently to purely commercial domains (the customer takes something and pays for them), in healthcare only the rights of access to patient-related medical information can be given. The grant of access rights is provided solely in responsibility of the information owner or the application administrator. The basis of decision are singular facts (case-related patient-user relationship, patient's right of informational self-determination) as well as rule-based scenarios (roles) (Council of Europe, 1995). Figure 1 presents a scheme of that two security types and the related measures discussed below.

As information systems scale to regionally, nationally, and even internationally distributed systems, their complexity has to be reduced in order to remain manageable with respect to both the security specification and the threat model. This is usually achieved through collecting similar components into security domains, representing special scope to the system. Common features allowing grouping are, e.g., organisation, functionalities, responsibilities, obligations, technical basis, policy, application domain, jobs. According to (OMG, 1995) there are three major types of security domains:

- the *security policy domain*,
- the *security environment domain*, including *message protection domain* and *identity domain*,
- the *security technology domain* (Blobel et al., 1996).

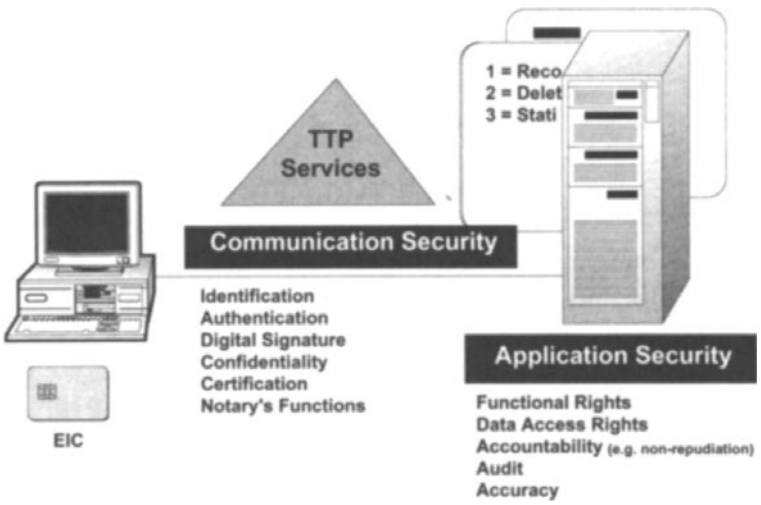

Figure 1 Security types

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

The purpose of security domains is to form groups of mutual trust defining special level of risks and therefore demanding a set of countermeasures. Assuming adequate characteristics, departments, enterprises, institutions and even organisations can be considered as domains. These domains are assumed as trust environment, which must be only protected against external threats. Therefore, special security measures are required only for communication between different domains and are implemented at the domain boundaries. Nevertheless, the challenges and conditions of Shared Care, the use of widely spread and distributed middleware architectures, and the integration of many care and system providers require the consideration of current and future health information systems as open and distributed systems, accepting the untrustworthiness of the communication environment as well as involving several domains. Therefore, the communication partners and also the middleware system could belong to different technology domains, environment domains, or even policy domains.

3 MIDDLEWARE SERVICES AND THEIR SECURITY CONCEPTS

To meet the requirements of the future healthcare for efficient and interoperable healthcare information systems, some application-layer-specific advanced services were developed. These services, also called middleware, mediate the communication and the co-operation of application systems from different vendors on different platforms and with different application environments including also legacy systems. Related security requirements are discussed in section 7.3.5. The middleware architectures referred to below provide services on different levels involving EDI[2] and/or middleware products as CORBA, Microsoft's OLE/DCOM[3], or DHE[4].

Because information to the here only shortly discussed advanced services is published in a large number of standards and specifications, review articles are cited referring to the genuine sources. In this context the first comparative study of all the discussed architectural approaches should be mentioned (Blobel and Holena, 1996).

3.1 HL7

Architectural Approach

HL7 (Health Level Seven) is a communication standard for information interchange (electronic data interchange = EDI) in healthcare environments, supporting communication at the OSI application layer (level 7). The actual focus on hospitals will be extended within the next versions (V. 2.3, V 3.x) of the standard.

[2] Electronic Data Interchange; provides open communication, requiring specialised servers (communication servers) or standardised middleware products to serve interoperability

[3] Object Linking and Embedding / Distributed Common Object Model

[4] Distributed Healthcare Environment, the European Health Information System Architecture (HISA)

HL7 enables communication between any systems independently of their architecture and hardware basis. This is achieved by standardising the syntax and semantics of exchanged messages. HL7 interfaces realise the request/service procedure in the sense of sending and receiving these messages, including the transformation from the proprietary format to the standardised format and vice versa. The communication is managed by communication servers or by a standardised middleware architecture, which is not a part of the HL7 communication standard. Not HL7, but only the underlying middleware architecture as a very complex service system is able to provide interoperability between systems.

The basic principle of HL7 is a *point-to-point information interchange paradigm* (1:1 or 1:n in the case of broadcast). Communication is controlled either by *trigger events* (in the case of trigger event paradigm of process coupling, *unsolicited* or real time) or by *query/response interchange* (in the case of query/response paradigm of retrospective interchange or *solicited*). Therefore, HL7 enables healthcare information systems to manage concurrent processes and non-concurrent interchange of messages. Using unique object identifier, a controlled time order of messages is supported. HL7 provides both basic and enhanced acknowledgement paradigms.

HL7 has been widely introduced in the US healthcare sector and is increasingly used in some European countries, especially in Germany. The successful dissemination of HL7 will be promoted by the harmonisation of the different healthcare information interchange protocols, performed by the Joint Working Group for Common Data Model in Healthcare (JWG-CDM) and chaired by IEEE. The objective of JWG-CDM is to develop object-oriented models and specifications that are needed to support a generic messaging standard. In addition, interfaces to standard middleware architectures like ASN.1, CORBA, and OLE will soon be realised. Industry driven working groups like the HP-promoted AndoverGroup focus on JWG-CDM compliant products, starting with HL7 related procedures, followed by CORBA integration.

EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) is the European pendant of HL7, but is actually not achieving a similar significance in the healthcare domain.

Security Services

The similar security concept of HL7 and EDIFACT is based on separately useable services for identification, authentication, digital signature, certification/assurance, data compression, encryption, notary's office functions (e.g. time stamps) to ensure the above mentioned security dimensions. The services could be used at the level of functional groups or transaction sets. The security mechanisms could be provided exclusively or in combination as requested realising transparency and response to special technology and policy requirements or conditions. The services are provided between security originator and security recipient and certified by an assurance originator and recipient structure respectively.

3.2 CORBA

Architectural Approach

The CORBA of the OMG is a middleware standard, which provides an open generic concept including implementation tools for general and object-oriented interoperability of distributed applications. It realises all functions below the application layer using only some basic assumptions for simple transport protocols. CORBA consequently defines distributed objects, which are characterised by a set of methods and a set of attributes fulfilling all needs of environment for supporting co-operation. The objects are implemented using of *OMG-interfaces* in an open system involving all applications and providing all services needed for the communication and co-operation within the system aggregation. The interfaces are specified using an *interface definition language* (*IDL*). Different services have to be managed, which is performed by an *Object Request Broker* (*ORB*) giving that architecture the name *Common Object Request Broker Architecture* (*CORBA*). The CORBA services are separated into

- low level services
- common object services providing common functions for data handling (e.g. naming or transaction and time management),
- advanced services
- common facilities as well as application objects, both providing direct support of applications

The common facilities are divided into horizontal and vertical common facilities. The horizontal common facilities are related to functions needed in different application domains. Examples are user interface (connection to user environment, e.g. Microsoft's OLE or OpenDoc), information management (handling application data), system management, task management and others. Vertical common facilities are related to a specific application domain like healthcare (e.g., *Medical record object model framework* and *Master patient index framework*).

Using CORBA, the users (including application programmers) need no knowledge about its underlying architecture, available services, their location etc. In CORBA, the services needed can be implemented transparently. Via prepared interfaces, different CORBA implementations can be bridged together. In this way, CORBA enables even the collaboration of objects distributed in extended networks, such as Internet.

The intensity and quality of CORBA utilisation depends on the availability of vertical common facilities. DHE managers (see the next paragraph) could provide such application related services, provided they get compliant to the object orientation of CORBA.

Because of the short history, only a few healthcare projects are using the CORBA architecture. An important impulse to CORBA should come from the activities of the American JWG-CDM, including all organisations involved in healthcare communication standards. By these object-oriented solutions for communication standards, the healthcare applications will get access to CORBA services for optimal systems' interoperability.

Security Services

Domain-specifically, CORBA provides all important security services, such as identification and authentication, authorisation and access control, security auditing, security of communication including mutual authentication of clients and targets, integrity protection and confidentiality protection, non-repudiation, and administration of security (OMG, 1995). Basic principles for an object-oriented security architecture within CORBA are simplicity, consistency across the distributed co-operating systems, scalability and usability (transparency), flexibility of security policies, independence of security technology, application portability, interoperability, and sufficient performance. Security pertains to various components of the CORBA architecture. A considerable part of security functions is implemented directly through the ORB or through their bridging mechanisms. Others are confined to transaction services or to additional security services, implemented through specific security-related objects. Finally, security services are also provided by the underlying operation systems and communication services.

Identification and authentication of principals (users, processes, devices, etc.) requesting any object services is provided either by the outside system or by a Principal Authenticator object. The Principal Authenticator creates for each principal a Credentials object, containing the principal's privilege attributes, e.g. the access identity, groups to which the principal belongs, roles, security clearance, and capabilities concerning various groups of objects. A security aware target application may obtain attributes of the principal responsible for the incoming request, to make its own authentication-depending access decisions. The information contained in Credentials can be obtained either directly or through the Current, an interface of the Transaction Services, which holds reference to the current execution context at both client and target objects.

The privilege attributes are first needed for making a secure invocation, which is mediated by the ORB. Whether the invocation can take place, as well as the way in which it is mediated, depends on the client and target security policies. As mentioned above, security policies concern such issues as access control, establishing trust in client/target, protection of messages for integrity/confidentiality, time restrictions, or delegation of privileges. If a request initiates a chain of invocations, then the security policies of all objects in the chain are taken into consideration through delegation mechanisms, including all intermediate objects.

As far as access control is concerned, applications can enforce their own access policies. Typically, details of access control are isolated from the application itself, and are implemented through an Access Decision Object, specific to the access policy. In addition, there is an Access Decision Object associated with the ORB and used for the invocation access policy, which is enforced internally by the ORB. The decision whether to allow access to a given function or data depends on the privilege attributes of the initiator of the request, control attributes of the target, and on the execution context. Access policy can be actually shared by a whole domain of objects with similar security requirements. In that case, reference to the corresponding Access Decision Object is available via the Current interface.

Similarly, applications can also enforce their own audit policies, which can be again managed via a domain structure. Each application writes its audit records to an Audit

Channel object. One such object is created at ORB initialisation time and is used for all system auditing. Application can use different Audit channel objects.

Finally, CORBA supports optional Non-repudiation services, providing generation and later verification of evidence concerning performed actions and data associated with those actions. The evidence can be generated using either symmetric cryptographic algorithms requiring a trusted third party as the evidence generating authority, or asymmetric cryptographic algorithms assured by public key certificates issued by a certification authority. Keys or other information needed for generating or checking the evidence are available via Credentials.

3.3 DHE

Architectural Approach

DHE is an integration platform, which supports the development of new applications and their integration with existing legacy systems in a distributed hospital information system. This is achieved by providing a functional infrastructure composed of a set of healthcare specific services. Services are grouped into appropriate data managers (such as the Patient Manager, the Resource Manager, etc.) according to the type of information that is managed. Using the standardised services, openness and compatibility between different healthcare applications is achieved. The services have been defined and validated on top of a generic healthcare centre data model based on experiences and projects involving several European healthcare centres.

Essentially, the DHE is a healthcare specific middleware which supports the distribution of applications and the transparent interaction between them. It includes transversal functionalities such as the Act Management concept which defines a relationship between healthcare providers and requesting parties ensuring a permanent line of communication between them. In this manner full interoperability is achieved between completely independent applications, realised by the healthcare specific DHE middleware of services with its API. In contrast with CORBA, DHE provides only advanced services on top of a so-called 'bitways' layer ensuring a technical platform for supporting network and distribution requirements.

All issues concerning data and transaction management or distribution are managed at the DHE level, leaving the application developer free to concentrate on the actual needs of the users for which the application is being developed. The architecture does not dictate any specific organisational structure, to the contrary, it provides a flexible means for describing the systems so that the IT infrastructure may follow the adopted organisational structure, even if it evolves over the time. It also conforms to the pre-standard proposed by PT-013 of CEN TC 251 Working Group 1 describing the standard European architecture for Healthcare Information Systems.

The basic concepts of the DHE and its architecture not only support different types of healthcare centres, but also offer migration strategies for the future.

DHE is based on the RICHE architecture, also represented by a consortium. The differences consist especially in the availability of the corresponding managers for the various healthcare-related functionalities (Blobel and Holena, 1996).

Security Services

The DHE security concept is similar to that of CORBA, also regarding services for secure communication as well as services to provide application security of external systems and DHE managerial functionalities alike. Regarding DHE managers as common vertical facility type CORBA components, the integration of the different approaches can also be extended to the security concepts discussed in the next sections.

3.4 Architectures' Relationships

Each of the architectures HL7, CORBA and DHE/RICHE integrates components of distributed health information systems. The extent of integration, however, is different.

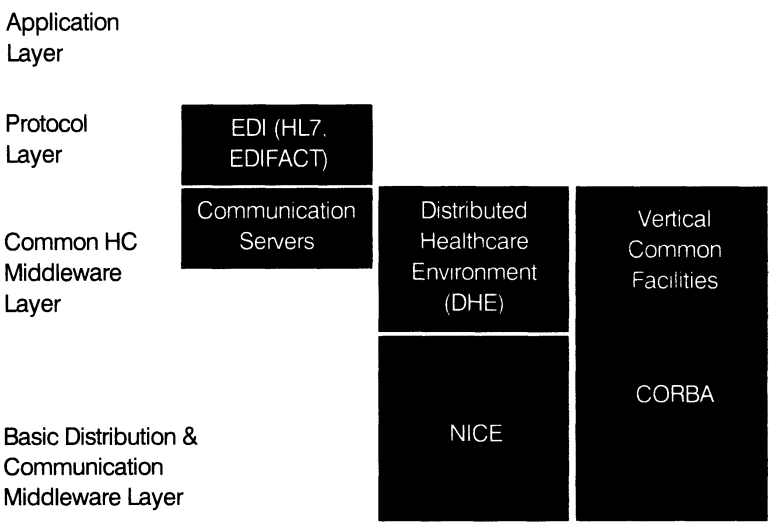

Figure 2 A joint architecture of essential middleware approaches (HANSA Consortium, 1996)

HL7 specifies standardised messages at the application level. DHE/RICHE provide complex healthcare-related services transparently supporting the co-operating applications. These services correspond to the vertical common facilities of CORBA. Apart from these facilities, CORBA defines general middleware services and facilities as well as implementation tools enabling transparently the interoperability of any systems in an object-oriented way. A joint architecture (figure 2) was proposed by (HANSA Consortium. 1996). For further details see (Blobel and Holena, 1996).

3.5 Common Security Aspects

The architectures considered above are a significant step beyond distributed cooperating systems. They provide not only communication services between security environment domains of end-users but they also provide application specific services to them. In addition to the service related threats, architecture specific threats caused by the advanced services need to be considered, which sometimes be provided by third parties with their own policy, environment, and technological domains in the sense of untrusted providers. Similarly to provided network services also the functional services of the middleware can be corrupt.

The above architectures vary considerably in the maturity of their security approaches. So far, HL7 respects security rather elementary whereas CORBA provides a mature and up-to-date security concept. Because the advanced security services of application-related communication protocols (EDI: HL7, EDIFACT) and of middleware architectures (CORBA, DHE) have to be

- transparent to the users or applications, ensuring security also for security unaware users or applications, and
- flexible for different domains requirements,

different security services must be provided. These services can be combined supporting authentication, confidentiality, accountability as non-repudiation, and access control on behalf of principals. CORBA uses credentials bearing corresponding attributes, which can be delegated or replaced in order to fulfil an HCE's policy. Furthermore, there are middleware-specific functionalities providing integrating services, such as system-wide identification of patients (Master Patient Index) and semantic tools supporting interoperability of heterogeneous systems consisting of different applications. For that purpose, the related security mechanisms must be provided independently of any application control.

Keeping in mind the combination of standardised middleware products (section 3.4), figure 3 outlines a structural model with essential security-related objects in distributed systems using middleware approaches. The scheme describes application visible objects and implementation security objects, controlled by advanced delegation and replacement mechanisms, assuming a scenario that an application A requests a service from an application B mediated by a (set of) middleware. Both applications as well as the underlying middleware could belong to different domains with respect to policy, environment, technology, mechanisms and services. Details of the presented structure are published in (Blobel, 1997).

In current security models, the service providers, including middleware services, are viewed as untrusted, following the basic concept to trust nobody and to organise security mainly by the communicating and co-operating partners (Blobel et al., 1996). Especially for distributed middleware architectures involving a number of hosts, Varadharajan proposed to install, on each of them, security functions (e.g., encryption/decryption, signatures), a security information base, secure factory objects (objects responsible for creation and deletion of other objects), and secure interfaces (Varadharajan and Hardjono,

1996). Most of these services can also be provided by functionalities specified in CORBA (OMG, 1995).

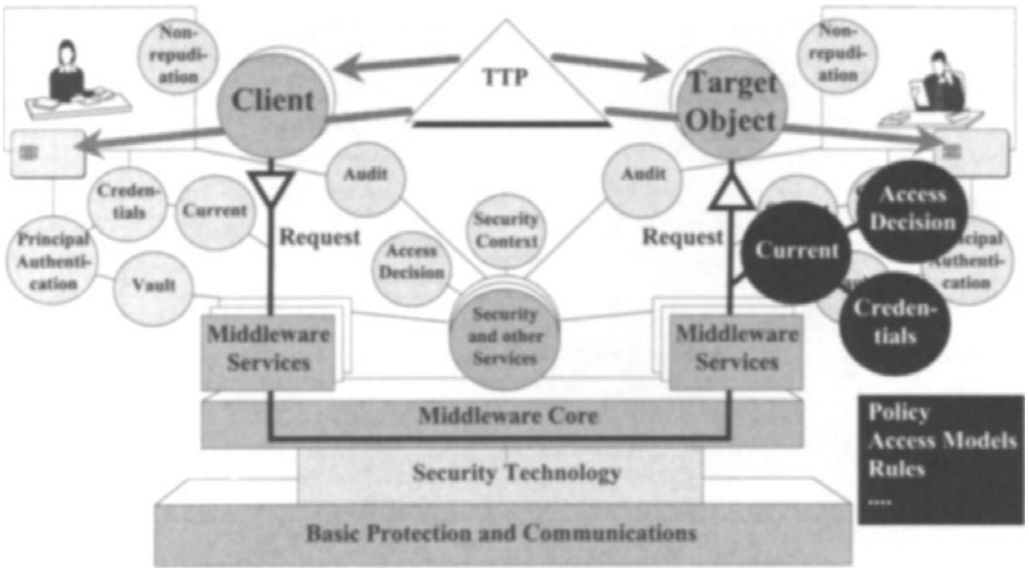

Figure 3 Structural model of a common middleware security

4 SECURITY ARCHITECTURE OF A ONCOLOGICAL DEHR

In the Clinical Cancer Registry Magdeburg/Saxony-Anhalt, the first German distributed EHR in oncology was implemented to support quality and efficiency of cancer care (Blobel, 1996b; Blobel, 1996c). For a catchment area with about 1.2 million inhabitants, more than 50 clinics and the Oncological Follow-up Organisation Centre are online connected to an extended patient-centred and case-oriented tumour documentation. The stored, processed, and cooperatively used information is highly sensitive. Therefore, our Cancer Registry was the first German healthcare application with advanced security mechanisms ensuring strong authentication of users as well as integrity and confidentiality of data. Improvement and further development of the system is embedded in several projects, related to both security and architecture and funded by the European Union. Currently, for communication and cooperation between a doctor's workplace and the registry middleware concepts (DHE, OLE, HL7) are being introduced. In coordination with the TRUSTHEALTH project (TRUSTHEALTH1, 1996a, 1996b), the system is also involved into the German Model Project "Health Professional Cards" (HPC) employing HPC for strong and certified authentication and additional communication security services mentioned in section 2 (Arbeitskreis, 1996). The task of providing a distributed oncological EHR is part of the telemedicine initiative of the German federal state Saxony-

Anhalt (Blobel, 1996a). An important challenge is the implementation of an adequate organisational and technical security infrastructure including Trusted Third Party (TTP) services. Figure 4 shows the Magdeburg TTP solution.

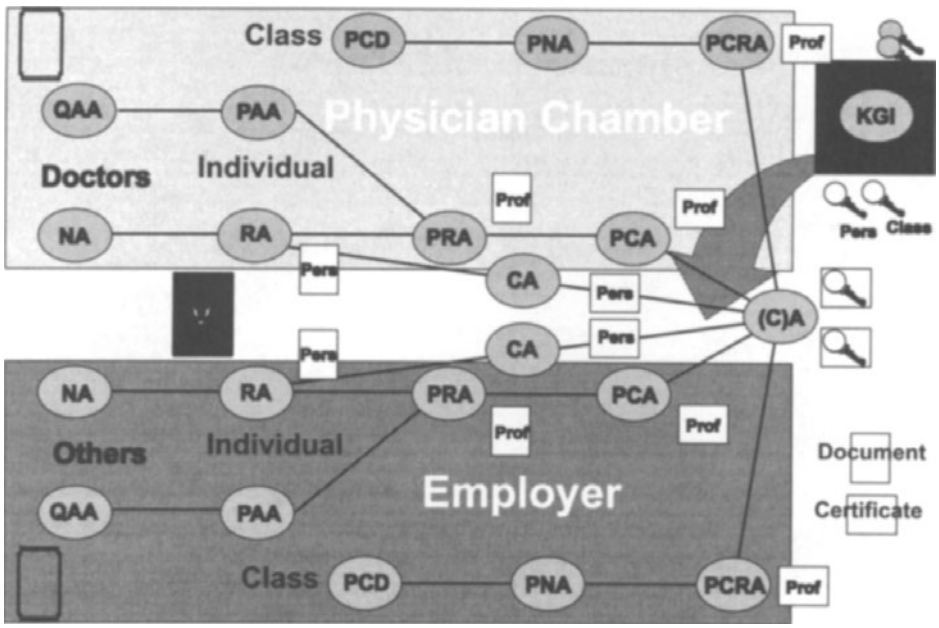

Figure 4 Magdeburg TTP solution

5 CONCLUSION

Currently, all industrial countries are trying to enhance the efficiency of their healthcare systems employing the Shared Care paradigm. Information technology plays a key role in these efforts. Information systems have to support decentralisation, communication, and cooperation by their own architecture. Numerous groups are pushing forward process-related and patient-centred open distributed and interoperable information systems developing and using middleware standards. Such systems are characterised by high requirements for data protection and data security. Important middleware approaches and their underlying security concepts are discussed. An interoperability trend of the different coexisting middleware architectures could been mentioned. On that basis, a structural model of a common security concept has been developed. The presented solution for an distributed EHR demonstrates need and feasibility of security solutions in open distributed heterogeneous health information systems supporting Shared Care.

6 ACKNOWLEDGEMENT

This work was supported within the "Telematics Applications Programme" framework of the European Union, and by the Ministry of Education and Science of the German Federal Sate Saxony-Anhalt. Furthermore, the author is obliged to thank the colleagues of the CORBAmed Task Force and the HL7 SIG Secure Transactions for kind cooperation.

7 REFERENCES

Arbeitskreis (1996) „Health Professional Card" der Arbeitsgemeinschaft „Karten im Gesundheitswesen": *Deutscher Modellversuch „Health Professional Card (HPC)"*, Göttingen, Stand Oktober 1996.

Blobel, B. (1996a) Konzeption für Telematikanwendungen im Gesundheitswesen sowie für ältere und behinderte Menschen. *Telematik-Initiative des Landes Sachsen-Anhalt.* Magdeburg, 19. Februar 1996.

Blobel, B. (1996b) Clinical Record Systems in Oncology. Experiences and Developments on Cancer Registers in Eastern Germany, in *Preproceedings of the International Workshop "Personal Information - Security, Engineering and Ethics"* pp 37-54, Cambridge, 21-22 June, 1996 (announced in LNCS, Spinger-Verlag).

Blobel, B. (1996c) A Regional Clinical Cancer Documentation System for an Optimal Shared Health Care in Cancer, in *Medical Informatics Europe '96* (edrs. J. Brender, J.P. Christensen, J.-R. Scherrer, P. McNair), pp 1019-1026. IOS Press, Amsterdam.

Blobel, B. (1997) An Object-oriented Security Approach Involving HL7, CORBAmed, and DHE Standards, *in Preceedings of the Conference „Toward An Electronic Patient Record '97"*, Nasville, April 26 - May 3, 1997 (submitted).

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.

Blobel, B. and Holena, M. (1996) Advanced Healthcare System Architecture Using Middleware Concepts - A Comparative Study. *Deliverable of the HC 1019 Telematics Project HANSA*, July 1996.

Council of Europe (1995) EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Strassbourg.

HANSA Consortium (1996) Middleware Approaches in Healthcare. A Presentation for the Healthcare Management (Draft). August 1996.

OMG (1995) The CORBA Security Specification. OMG Doc.No. 95-12-01.

The SEISMED Consortium (edr.) (1996) Data Security for Health Care, Volume I - III. IOS Press, Amsterdam.

TRUSTHEALTH1 (1996a) Selection of Security Services and Interfaces (Version 1.0). 1996-07-29.

TRUSTHEALTH1 (1996b) Functional Specification of TTP Services (Version 0.6). 1996-07-29.

Varadharajan, V. and Hardjono, T. (1996) Security Model for Distributed Object Framework and its Applicability to CORBA, in *Information Systems Security* (eds. Katsikas, S.K., and Gritzalis, D.), pp. 452-463, Chapman & Hall, London.

8 BIOGRAPHY

Dr Bernd Blobel is Head of the Department of Medical Informatics at the University of Magdeburg and chair of the first German distributed cancer registry. The department is involved in several projects, funded by the EU (e.g., HANSA, TRUSTHEALTH, ISHTAR, DIABCARD, EUROMED-ETS, MEDSEC). Dr Blobel is the German representative on the IMIA WG4 and WG13. He is cochair of the CORBAmed security group, represents the DHE Consortium within CORBA, and is involved in HL7 activities. Furthermore, he is chairing various German security groups as well as telemedicine initiatives with special responsibility to security aspects.