Security Analysis and Design Based on a General Conceptual Security Model and UML

Bernd Blobel[1], Peter Pharow[1], and Francis Roger-France[2]

[1]University of Magdeburg, Medical Faculty, Institute of Biometrics and Medical Informatics, Leipziger Str. 44, D-39120 Magdeburg, Germany
bernd.blobel@mrz.uni-magdeburg.de
peter.pharow@medizin.uni-magdeburg.de
[2]Catholique Université de Louvain, Cliniques Universitaires St. Luc,
10 Avenue Hippocrate, Box 3716, B-1200 Brussels, Belgium
roger@infm.ucl.ac.be

Abstract. To facilitate the different users' view for security analysis and design of health care information systems, a toolset has been developed using the nowadays popular UML approach. Paradigm and concepts used are based on the general security model and the concepts-services-mechanisms-algorithms-data scheme developed within the EC "ISHTAR" project. Analysing and systematising real health care scenarios using appropriate UML diagrams, only 7 use case types could be found in both the medical and the security-related view. Therefore, the analysis and design might be simplified by an important degree. The understanding of the approach is facilitated by (incomplete) examples. Based on our generic scheme and with the results described, the security environment needed can be established by sets of such security services and mechanisms.

1 Introduction

Shared care as the answer to the challenge for efficient and high quality health care systems must be supported by appropriate information systems' architectures as health care networks, distributed health record systems etc. Dealing with sensitive, personal medical data and often communicating these data across organisational, regional and even national borders, such information systems have to meet comprehensive security requirements to respond threats and risks in distributed health information systems. Regarding security in general, we have to look for the concepts of security, safety and quality [10]. To keep the approach feasible, the consideration in most of the chapters is restricted on the concept of security only.

Considering nowadays health information and communication systems, most of them do not fulfil the security requirements or provide partial add-on solutions only.

2 Methods

For a systematic and open analysis, design and implementation of security services and mechanisms in interoperable health information systems, an agreed or even standardised methodology is inevitable. The popular object-oriented paradigm as well as the further development and harmonisation of the corresponding tools for analysis, design and implementation based on the Unified Modelling Language (UML) provide the open and comprehensive solution to respond to these challenges [11].

3 General Security Model and Scheme

For an appropriate granularity of security issues in distributed information systems to provide feasible solutions, on the one hand the domain concept is used defining the domain concerns via the Security Policy. Beside the definition of Security Policy Domains, Security Environment Domains and Technology Domains have been specified. For details see, e.g., [2, 3]. On the other hand, a concepts-services-mechanisms-algorithms-data scheme has been developed to systematise and support aspects and views or different user groups [5, 6].

4 Modelling of Users' Security Needs

In general, analysis and design of systems in hardware and software is based on a model describing state and/or behaviour of that system. Also the currently popular OO modelling techniques of Grady Booch, James Rumbaugh and Ivar Jacobson provide such an overall model consisting of the components classes, class categories, objects, subsystems, modules, processors, devices, and the relationships between them. These model components mentioned possess properties which identify and characterise them. They can appear in none, one, or several of a model's diagrams associated with other components. Thus, looking for the different components,

- the class category contains class diagrams and scenario diagrams associated with its components: classes and their objects, and nested class categories,
- the subsystem contains module diagrams associated with its components: modules and nested subsystems,
- the class contains its state diagrams,
- a model's top level contains the diagrams for its top level components as class categories, classes, subsystems, and modules, and its process diagram.
- In OMT-2, four partial models allow capturing as well as analysis and design of the considered system or domain: the logical, the physical, the static, and the dynamic model. Contrary to other approaches the UML methodology, which is based upon the Booch methods, the OMT-2 methods of Rumbaugh, and the OOSE and Objectory methods of Jacobson, facilitates different views of the overall model described verbally by specifications and through different diagrams (e.g., logical dia-

grams, class diagrams, class structure diagrams, scenario diagrams, collaborations diagrams, component diagrams, distribution diagrams, activity diagrams, use-case diagrams, sequence diagrams).

4.1 The UML-Methodology

The UML views are:

- The use case view showing the functionality of the system as perceived by external actors. The use case view is described in use case diagrams and activity diagrams. Use case diagrams are basic descriptions influencing the other views. While the use case looks from outside the system using natural languages to describe the use case, the collaboration (context and interaction) diagram has an inside the system perspective to describe interactions in time (sequence diagram), in space (collaboration diagram) and concerning the work (activity diagram). Finally, the scenario diagram describes a scenario in time (sequence diagram), in space (collaboration diagram) and concerning the work (activity diagram) via an execution path through the system.
- The logical view showing how the functionality is designed inside the system, in terms of the system's static structure and dynamic behaviour.
- The component view showing the organisation of the code components.
- The concurrency view showing concurrency in the system, addressing the problems with communication and synchronisation present in a concurrent system.
- The deployment view showing the deployment of the system into the physical architecture with computers and devices called nodes.

A scenario is a sequence of important interactions between objects as instances of classes within concrete application environments. Scenarios are used to represent critical requirements, depict the action of key mechanisms, and demonstrate desired series of operational cases. The scenarios can be described, considered and manipulated by two types of isomorphic scenario diagrams: the object message diagram and the message trace diagram. An object message diagram illustrates the existence of objects and the communication as the flow of messages among them.

Responding to the enduser requirements for security enhancement, only a part of the UML methodology is really needed. In that context, the use case diagram (and sometimes the sequence diagram as well as the activity diagram) must be mentioned.

The use case defines a framework for using a (information) system. Starting with an abstract use case type, the use case instances describe concrete application scenarios in the sense of the description of .business processes and their communication/interaction with actors. Actors in the healthcare domain are health professionals (doctors, nurses, administrators, technical staff, management, ...) and patients, but also people from other domains. Often, the domain-specific description of the use case is done verbally. Looking for security in information systems, specially security-related use case instances must be mentioned.

To model the needs of the health professionals (medical users, medical and technical staff, administration, management, legal experts), the use of the UML toolset should be recommended. Depending on the different user groups' need, an appropriate granularity of the model may be depicted. The specific components can be described by abstract types using the OO properties like inheritance etc. Complex scenarios may be created combining the abstract or basic types needed. Investigating legal implications on security solutions within the „TrustHealth-2“ project (a TAP project of the 4th Framework Programme), very simple abstract types and complex scenarios are used fulfilling the legal experts' needs.

4.2 Medical Use Cases

Analysing and grouping the real-world scenarios, basic scenarios or abstract use cases may be defined, which enable the description on any real scenario by compositions of use cases types specified.

Regarding the last 2 years activities results of the „ISHTAR“ project funded by the European Commission, administrative tasks (use cases) and medical tasks (use cases) might be distinguished. Grouping these tasks, the following abstract administrative and medial use cases can be found (the relationship to the Swedish approach described in the next paragraph is mentioned by reference numbers):

Table 1. Abstract Administrative and Medical Use Cases

Administrative Use Cases	Medical Use Cases	Ref. #
Admission, discharge, transfer		1
	Diagnosis, assessment, decisions, conclusions	2
Scheduling and appointments		3
Financial transactions	Activities: Visits, Diagnostic procedures, Treatments, Care procedures	4
Non-medical communications: Insurance Communications, Supplier communications	Medical communications: Order entry, Result reporting, Access to patient information	5
	Reports (medical documentation)	6

Currently modelling and developing an Swedish Electronic Health Record, the groups involved have found the following abstract use case types:

1. Establishment of contact between patient and health care professional
2. Assessment/conclusion by the health care professional
3. Creation of a specific health care plan for the patient
4. Activities are initiated, performed and looked after
5. Access to patient information
6. Record of health care information
7. Conclusion

4.2.1 Medical Use Case Examples – Request Patient Information

The medical use case types mentioned above might be illustrated by some practical examples of real-world systems implemented in the Magdeburg cancer registry. The security solution for this architectural approach of the first German regional cancer registry has been described in detail in [1, 4,].

Considering the very complex challenges to such regional Electronic Health Record (EHR) systems as the Clinical Cancer Registry Magdeburg/Saxony-Anhalt, the first distributed and secured EHR in Germany, only one typical example will be presented in the following paragraphs. As such example, the doctor's request of patient information from the cancer registry or from other Health (Care) Professionals (H(C)P) have been selected. However, this example covers the complete set of the security-related use case types explored in our studies.

A typical scenario in the shared care environment is the doctor's request of information about his currently cared patient.

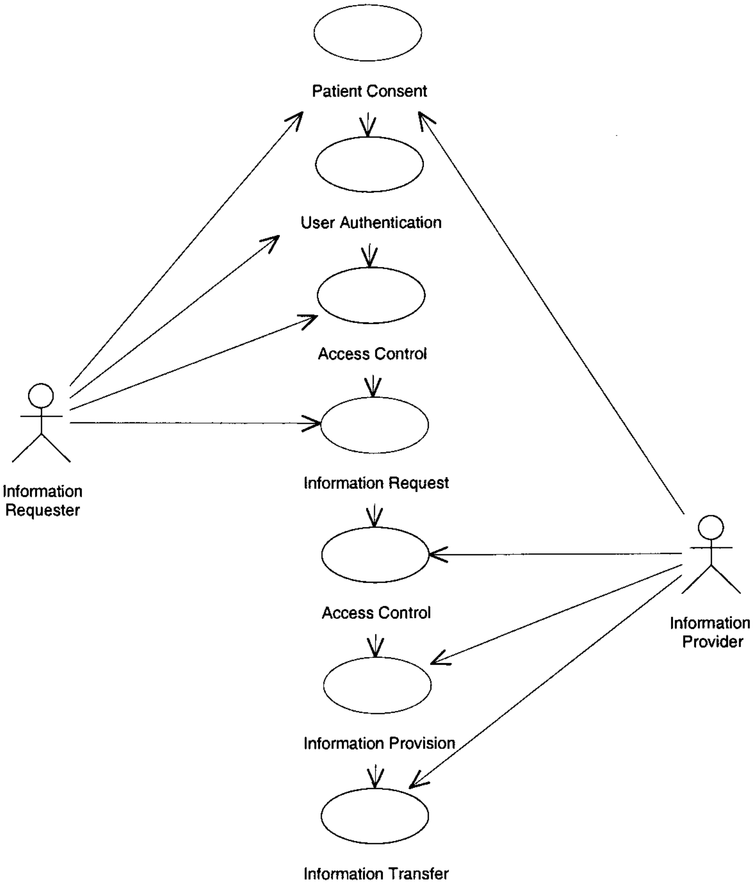

Fig. 1. Use Case "RequestPatientData"

This medical use case may occur to receive needed information from former diagnosis or treatment as well as to ask for a second opinion. The requested party could be, e.g., another HCP or a documentation system like an electronic archiving system or as in our case a clinical cancer registry. In the telemedicine/telematics framework, such request is considered as "remote" independent of the real distances bridged over by the communicating and co-operating systems, which could be located even on the same sever. Figure 1 presents that medical use case expressed in the UML notation. To respond to the different possibly communicating parties, the principals in the use case diagrams are neutrally tagged as information requester and information provider.

4.3 Security-Related Use Cases

To describe security-related use cases for open systems communication and co-operation, a set of abstract use case types have been defined. Afterwards, the different security-related use cases can be created combining the appropriate basic use cases.

Abstract use case types are:

- the users management
- the user authentication,
- the patient consent
- the communication initialisation,
- the information request,
- the access control,
- the information provision and
- the information transfer.

In the following paragraphs, these use case types mentioned will be described in more detail using the UML methodology. In that context it should be emphasised that each of the use case components may consist of subcomponents and can establish supercomponents etc., as shown in the medical use case example which represents all the use case types mentioned here. Due to the restrictions in the papers' extension, only a very short explanation is given to the different use cases which will be explained in more detail in [7].

4.3.1 Users Management

The security policy describes the complex of legal, organisational, functional, medical, social, ethical, and technical aspects which have to be considered within the context of data security and privacy. The security policy defines the framework, rights, and duties of persons and organisations involved, but also the consequences in the case of non-compliance to the agreement. Therefore, the security policy also specifies the users' roles and rules.

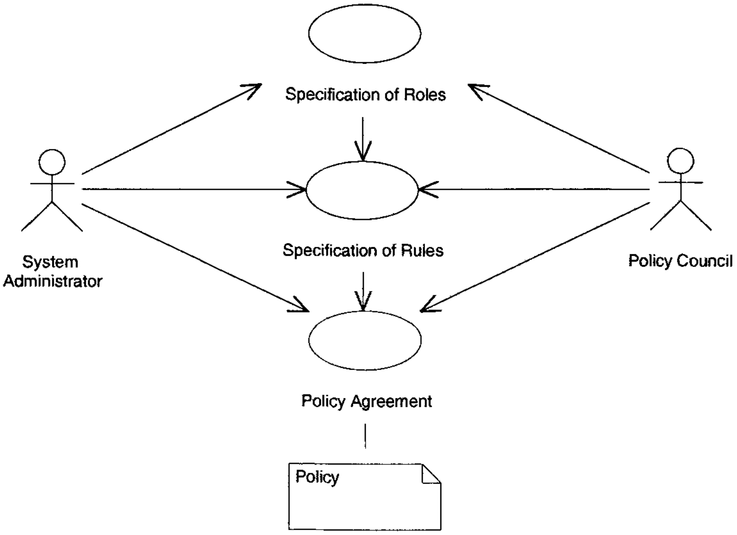

Fig. 2. Abstract Use Case "UsersManagement"

4.3.2 User Authentication

The authentication of principals communicating and co-operating via information systems is the basic service also needed for other security services and mechanisms as authorisation, access control, accountability etc. Authentication in health information system must be provided mutually and in a strong way using cryptographic algorithms. In our context, we consider human users keeping in mind the generalisation to principals. The TTP provides the user's identity certificate.

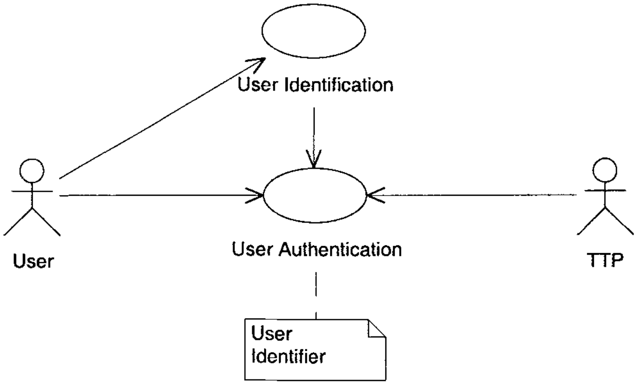

Fig. 3. Abstract Use Case "UserAuthentication"

4.3.3 Patient Consent

According to the principles of the European data protection directive [8, 9] and German laws on data protection, the patient's consent is required in the case of collecting, recording, processing, storing, and distributing his/her personal medical information.

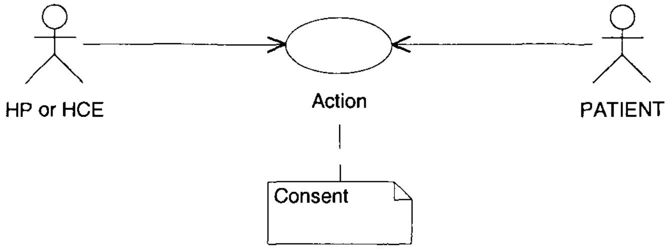

Fig. 4. Abstract Use Case "Patient Consent"

4.3.4 Initialisation of Communications

For bilateral and multilateral communication and co-operation, the mutual identification and authentication of the partners (principals) involved is needed. The authentication must be verified by the certificates provided by the TTP.

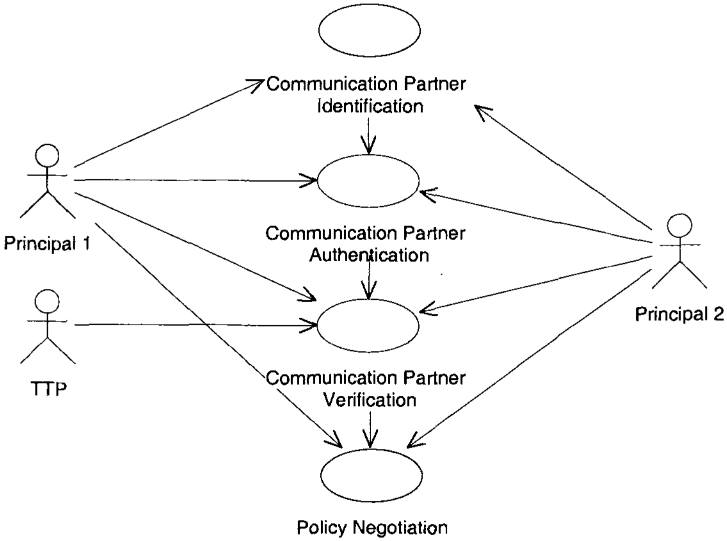
Communication Partner Identification
Principal 1
Communication Partner Authentication
TTP
Principal 2
Communication Partner Verification
Policy Negotiation

Fig. 5. Abstract Use Case "CommunicationInitialisation"

4.3.5 Information Request

After the initialisation of any communications and co-operations, the information requested has to be specified.

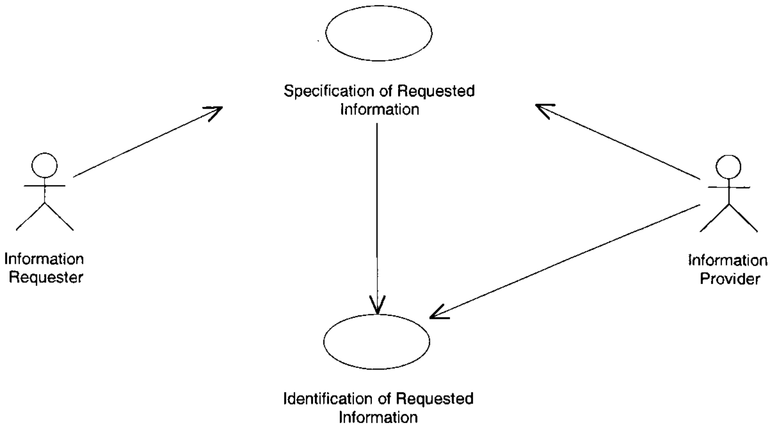
Specification of Requested Information
Information Requester
Information Provider
Identification of Requested Information

Fig. 6. Abstract Use Case "InformationRequest"

4.3.6 Access Control

Fulfilling the need to know principle and the privacy rights of the patient, the access to and the use of patient's information must be restricted and controlled according to the underlying mandatory and discretionary access control models. On that way, the functional and data access rights of the different user or user groups respectively in correspondence to their functional and organisational (structural) roles are defined and decided according to the rules agreed.

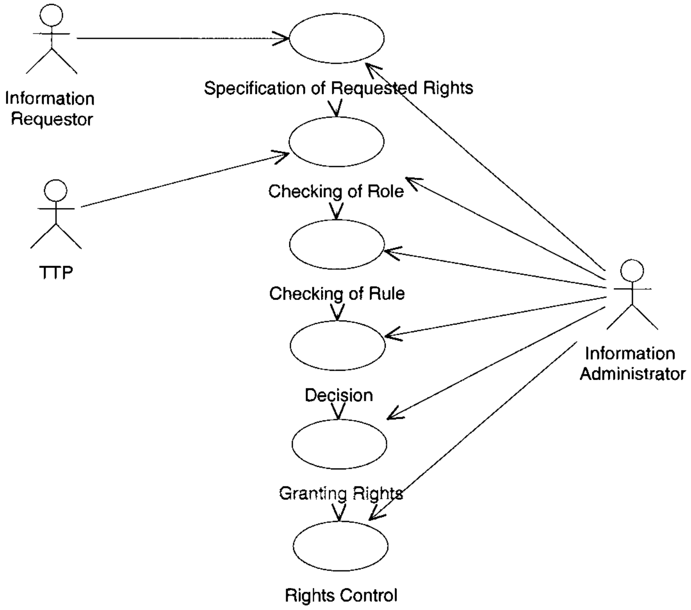

Fig. 7. Abstract Use Case "AccessControl"

4.3.7 Information Provision

According to the security policy and its access control decision, the permitted information can be provided and finally transferred.

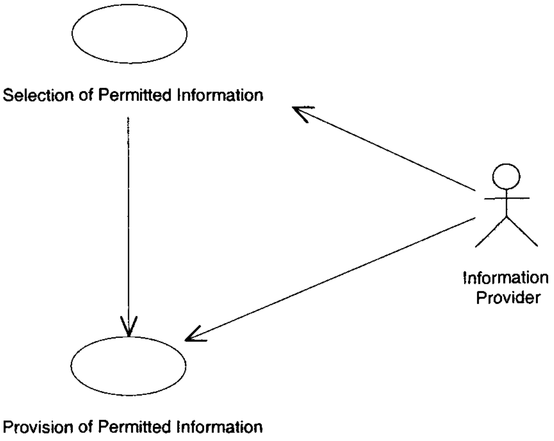
Selection of Permitted Information
Information Provider
Provision of Permitted Information

Fig. 8. Abstract Use Case "InformationProvision"

4.3.8 Information Transfer

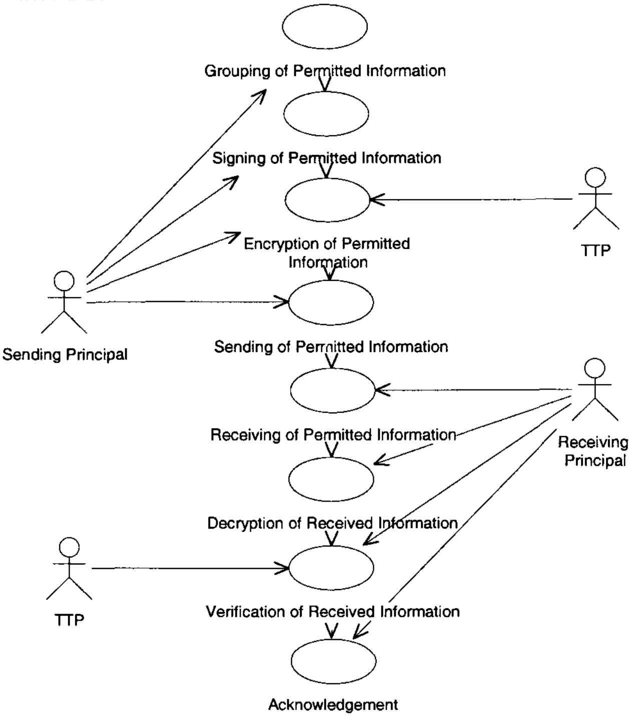
Grouping of Permitted Information
Signing of Permitted Information
TTP
Encryption of Permitted Information
Sending Principal
Sending of Permitted Information
Receiving of Permitted Information
Receiving Principal
Decryption of Received Information
TTP
Verification of Received Information
Acknowledgement

Fig. 9. Abstract Use Case "InformationTransfer"

The abstract use case “InformationTransfer” is defined in an very generic way also including the record of information and its transfer between user and system. Therefore, both application and communication security services dealing with integrity, confidentiality, and accountability (in the context of communication security also dealing with non-repudiation of origin and receipt) are reflected in the model presented.

To fulfil the policy agreed, beside the users also the information has to be classified and grouped.

5 The Layered Security Model

Based on the definition of a general security model within the „ISHTAR“ project funded by the European Commission in the Fourth Framework “Telematics Applications Programme” context, a layered extension of this model has been developed. It allows the selection of appropriate concepts-services-mechanisms-algorithms-data relationships according to the analysis and design results for the health information system under consideration [6, 7]. Interacting with the UML approach results partially presented in this paper, the complex and generic methodology supports the comprehensive analysis, design and implementation of secure health information systems. Within the EC „TrustHealth-2“ project, the methodology developed is also successfully used by the demonstration sites of the different participating countries. The complete results will be presented on other places [7].

6 Acknowledgement

The authors are in dept to the European Commission and to the Ministry of Education and Science of the German Federal State Saxony-Anhalt for funding as well as to the partners of both the „ISHTAR“ and the „TrustHealth-2“ project for kind co-operation.

References

1. Blobel, B.: 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. Springer, Berlin (1997) 39-56
2. Blobel, B, Bleumer, G., Müller, A., Flikkenschild, E., Ottes, F.: Current Security Issues Faced by Health Care Establishments. Deliverable of the HC1028 Telematics Project ISHTAR, October 1996
3. Blobel, B. and Pharow, P.: Results of European Projects Improving Security of Distributed Health Information Systems. In: Cesnik, B, McCray, A.T., Scherrer, J.-R. (eds.) MEDINFO ’98. IOS Press Amsterdam, Berlin, Oxford, Tokyo, Washington DC (1998) 1119-1123

4. Blobel, B., Pharow, P.: Security Infrastructure of an Oncological Network Using Health Professional Cards. In: Broek, L. van den, Sikkel, A.J. (eds.): Health Cards '97. Series in Health Technology and Informatics, Vol. 49. IOS Press, Amsterdam (1997) 323-334
5. Blobel, B., Pharow, P., Spiegel, V.: Shared Care Information Systems Based on Secure EDI. In: Moorman, P.W., Lei, J. van der, Musen, M.A. (eds.): EPRiMP – The International Working Conference on Electronic Patient Records in Medical Practice. IMIA Working Group 17, Rotterdam (1998) 164-171
6. Blobel, B., Roger-France, F.: Healthcare Security View Based on the Security Services Concept. ISHTAR Project HC 1028, Deliverable, August 1998
7. Blobel, B., Roger-France, F., Pharow, P.: A Systematic Approach for Secure Health Information Systems. (submitted to the International Journal of Medical Informatics)
8. Committee of Ministers: European Recommendation (Draft) No. R(96) of the Committee of Ministers to Member States on the Protection of Medical Data (and Genetic Data). CJ-PD (96). Strasbourg (1997)
9. Council of Europe: Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Strasbourg (1995)
10. Laske, C.: Legal Issues in Medical Informatics: A Bird's Eye View. In: Barber, B., Treacher, A. and Louwerse, K. (eds.): Towards Security in Medical Telematics – Legal, and Technical Aspects. Studies in Health Technology and Informatics, Vol. 27. IOS Press, Amsterdam (1995) 53-78
11. Eriksson, M., Penker, S.: UML Toolkit. Wiley Computer Publishing, New York (1998)