Paper

Tools for health professionals within the German health telematics platform

Bernd Blobel and Peter Pharow

Abstract— Shared care concepts such as managed care and continuity of care are based on extended communication and co-operation between different health professionals or between them and the patient respectively. Health information systems and their components, which are very different in their structure, behaviour, data and their semantics as well as regarding implementation details used in different environments for different purposes, have to provide intelligent interoperability. Therefore, flexibility, portability, knowledge-based interoperability and future-orientation must be guaranteed using the newest development of model driven architecture. The ongoing work for the German health telematics platform based on an architectural framework and a security infrastructure is described in some detail. This concept of future-proof health information networks with virtual electronic health records as core application starts with multifunctional electronic health cards. It fits into developments currently performed by many other developed countries. The paper introduces into the German health telematics platform and its tools based on smart card.

Keywords— health telematics, model driven architecture, electronic health record, smart cards, patient health card, health professional card, security, privacy.

1. Introduction

Any communication and co-operation between healthcare providers must be supported by intelligently interoperable health information systems. This challenge needs to be met especially for managed care and continuity of care concepts widely introduced in most of the developed countries to improve quality and efficiency of patient's care. In shared care environments – health professionals belonging to different healthcare establishments with different legal background, using different methods to perform different procedures, supported by different applications provided by different vendors and following different protocols, applied at different time – have to be deployed for co-operatively caring the same patient in an optimal way.

Interoperability might be provided at different levels. Those interoperability levels are ranging from simple data exchange and meaningful data exchange with agreed vocabulary to a functional interoperability with agreed communicating applications' behaviour, or finally to a service-oriented or semantic interoperability directly invoking the applications' services.

Health information systems enabling such advanced co-operation mentioned above in the managed care context are characterised by openness, scalability, flexibility, portability, distribution at Internet level, service-oriented interoperability, as well as appropriate security and privacy services. Finally, they have to be based on standards [1].

2. The German health telematics platform

As many other countries, Germany has launched a national programme for establishing a health telematics platform supporting seamless care [2, 3]. This platform combines card-enabled communication mediated by the patient with network-based interoperability between all actors involved. For the patient data card, called the German electronic health card, a multi-purpose microprocessor card is used. It will serve as a health insurance card, an immunisation and vaccination passport, emergency data and electronic prescription carrier, a carrier for pointers to the patient's electronic health record (EHR) components or related information such as drug information distributed on the net, and an information carrier for facilitating managed care and quality assurance.

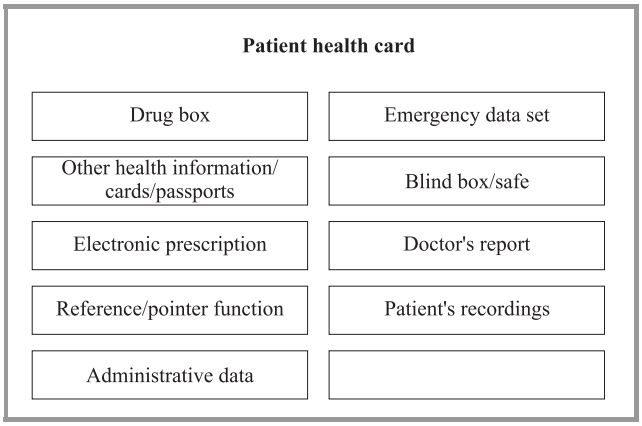

Fig. 1. Functional blocks of the electronic health card.

A specifically protected compartment contains information the patient likes to hide from reading by others. Additionally, the electronic health card provides basic security services based on cryptographic algorithms, such as strong authentication, integrity, accountability, and encoding/decoding services deploying the qualified electronic signature [4] and a related public key infrastructure (PKI). To support trustworthy interoperability between patients and health professionals, the latter use health professional cards (HPC) for adequate security services. For any access to data others than the emergency data set and the blind box/safe (the latter can only be opened by the patient as

mentioned above), the HPC as electronic doctor's license is required providing personal and role authentication. Security services support both communication and application security services for any principals such as users, devices, systems, applications, components, or objects.
The health card should be rolled out by 2006. It complies with the corresponding European health insurance card, which will be implemented in all EU member states until 2008. As important tool, the aforementioned HPC is a prerequisite for the health telematics platform and should be rolled out before 2006 too. The HPC is described in more detail in the following section.
Figure 1 shows the functional blocks of the German electronic health card. The blocks can be separately protected at different levels.

3. The German health professional card specification

Based on results of the European TrustHealth project [5] and the first HPC standard CEN ENV 13729 [6], the German HPC V 1.0 specification has been approved at 1999 [7], combined with political decisions setting up the legal and organisational framework in December 1997 already. The electronic physicians' ID is intended to completely replace the currently used paper based classical physicians' ID. For this reason the physicians' ID will have a distinctive card cover with the following general layout (Fig. 2).
The general structure and the dependency hierarchy for potential communication in the German health care system are indeed defined in an extremely heterogeneous manner (Fig. 3). There are many different players involved, i.e., medical associations, statutory health insurance (HI) administrations, physicians, hospitals, pharmacies, and insurers – only to name just a few. Definitely, a considerable number of communication pathways are already in place. However, the number of paths and the amount of information transmitted may easily be considered minor when compared to the potential needs of all of the other communication expected in health care. If just 10 000 physicians (of more than 380 000 registered in Germany) would possibly wish to exchange electronic data items of their patients among at least one another, this amount would completely surpass any of today's volumes by far. A well-established infrastructure is necessary to cope with the expected amount of information circulated among Germany's health professionals.

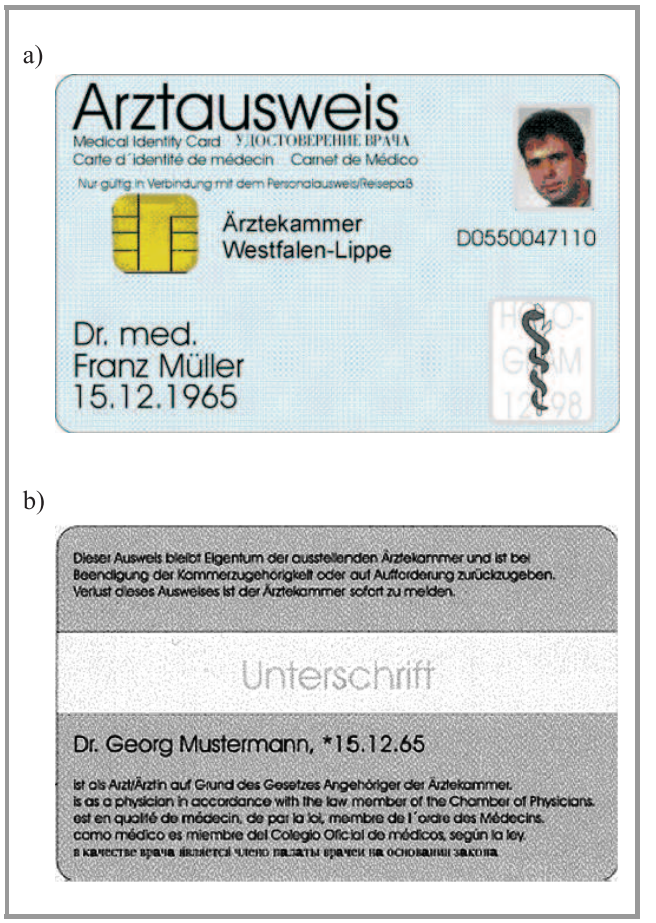

Fig. 2. Surface of the German health professional card for physicians (HPC). Front side (a) and reverse side (b).

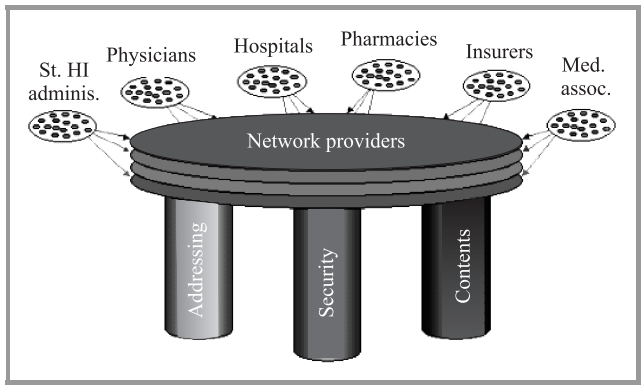

Fig. 3. Communication pathways.

It seems to be reasonable that at least three major factors need to work together, for any communication to work:

- basically, health professionals need to have a reliable method for addressing each other; this constitutes a nearly solved problem, since the majority of physicians already have some type of unique e-mail presence; the HPC will fill the remaining gaps by providing all health professionals with a distinguished name (DN);
- secondly, any communication in healthcare and welfare has to take place securely and confidentially; the participants must know and be able to prove who they are "talking" to; this is another major issue addressed by the German HPC development;
- finally, once health professionals can actually exchange data, this has to be done in a form which

allows them to really make use of the data transmitted; a basic consensus concerning content standards for verbal data, images, lab results, etc., has to be achieved for transmission to be interoperable; here, industry and standardisation initiatives like ISO, CEN, DICOM, HL7, IEEE, etc., play an increasingly important role.

All three factors need to work together, like the pillars supporting a platform. This platform itself consists of the interoperable connections between different network providers who offer their customers transmission facilities. A reduction of providers is neither feasible nor desirable and so interoperability on all of these levels becomes paramount.

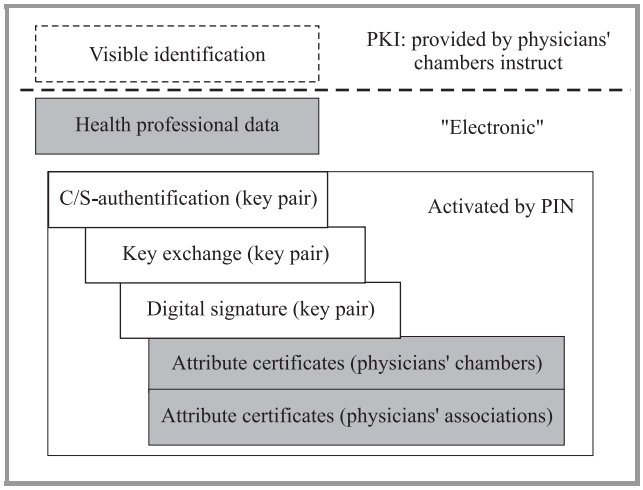

Fig. 4. Functional structure of German HPC.

Looking more closely at the details, the German physicians' ID contains a total of five different functions (Fig. 4).

1. The first function is that of a classic identification card which a physician can use in a number of different settings, e.g., when ordering prescription drugs in a pharmacy where he is not known. To this purpose the card is personalised with name and picture, completely replacing the classic paper ID which any physician can apply for today.

2. The first electronic function is that of a simple basic certificate providing authentication to any digital device this card is presented to. Here, a fast and simple method for easy identification was realised taking into account that this approach can only be used in an otherwise already secure setting, since there is no special security against theft. This trade-off between security and simplicity will certainly find its use, since it is intended as a direct electronic analogue to the physical presentation of the classic identification card.

3. The second electronic function is that of being carrier of an asymmetric key pair (more specifically, the private key of the key pair) for the strong authentication in a client/server environment. A public key infrastructure has to be put into place, where virtually any unit can look up or download the public key of a health professional and can then make use of it to check the private key of the person presenting his identification in any type of clinical setting. This enables the implementation of strong security in an otherwise untrusted environment.

4. The next major element is bearing another key pair (again, the private key of an asymmetric key is stored on the card) for the implementation of a hybrid (symmetric/asymmetric) transport encryption. This is where transportation protocols like HCPP, S/MIME, etc., can come into play by defining how the messages interchanged are to be encrypted and decrypted.

5. The final element of the HPC is the private key of an asymmetric key pair for the production of a legally binding electronic signature according to the German signature law (SigG). The specifics of the health professional are contained in a number of attribute certificates which he can append to his signature, specifying his role in medicine.

From a more technical point of view, the HPC is a contact-based smart card capable to process public key (PK) algorithms. The physical characteristics shall comply with ISO/IEC 7816-1 and related standards. An HPC is a normal size card (ID-001 card). Another card layout is the so-called institutional card (SMC) that could easily be considered a plug-in card (ID-000) for secure devices, e.g., in pharmacies.

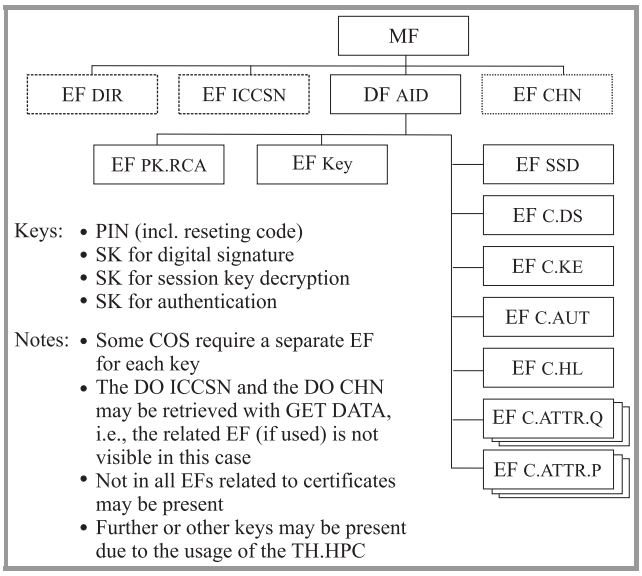

Fig. 5. Internal structure of German HPC.

As shown in Fig. 5, the HPC contains:

- some elementary files (EF) at the master file (MF) level for some general data objects and the card verifiable (CV) certificate;

- the HP application (HPA) providing the following services:
  - electronic identification of the health professional,
  - electronic signature creation,
  - client/server authentication,
  - document decipherment,
  - card-to-card authentication (HPC/eGK and HPC/SMC);
- the cryptographic information application (CIA) providing information for the primary system (e.g., a doctor's office system) to support the communication between the system and an HPC.

The HPC security mechanisms require different types of end user certificates:

- electronic (digital) signature certificate(s) (X.509 v3, type: electronic signature certificate(s), i.e., public key certificate and attribute certificate(s)), here called C.DS;
- authentication certificate (X.509 v3, type: authentication certificate), here called C.AUT;
- key encipherment certificate (X.509 v3, type: key encipherment certificate), here called C.KE.

In addition to the aforementioned certificate types all containing a key, additional certificates without a key (so-called attribute certificates) complete the card infrastructure. Attribute certificates in the context of the German HPC do rule certain aspects of permission (C.ATTR.P) and qualification (C.ATTR.Q).

4. The bIT4health project

To guarantee future-proof principles for designing and implementing common basic services of the aforementioned health telematics platform, an architectural framework and a security infrastructure have been defined and demonstrated as a proof of concept within the German project for improving the German healthcare system through the deployment of information and communication technology. This project has been called bIT4health (better IT for health) [8].
This architectural framework is characterised by different paradigms such as:

- distribution for openness;
- component-orientation for scalability and flexibility;
- interoperability at service level reflecting concepts and knowledge expressed through formal models for enabling conformance agreements;
- separation of platform-independent and platform-specific modelling separating logic and technologic views on system components as well as;
- installation of reference and domain models.

The latter properties enable openness, portability and future-proof investments for the solutions provided. The approach completely complies with the advanced paradigms including the model driven architecture presented in this paper.

5. Modelling systems

For describing systems and their behaviour in an appropriate way, real systems need to be modelled. A model might hide internal structural complexity, or might be focused on specific aspects of the system such as form or special functions. Beside this way of simplification of complex systems by modelling them, grouping elements of a system according to specific commonalities in structure and/or function makes system design, development, and maintenance manageable, realisable, and eligible for financing. The result are components which can be designed, manufactured, improved separately from other components, however keeping in mind and enabling reasonable interoperation between related components.
To reduce the complexity of the whole healthcare system consisting of many subsystems following the shared care paradigm, a single unrealistic comprehensive information system covering every thinkable procedure, fact and result will be realised by subsystems constraint to specific tasks, content, etc. In other words, we move from systems to components.
An information system is reflecting processes happening in the real world, by that way on the one hand establishing an information-related model of reality and on the other hand implementing a real system. Models are systems consisting of components, too. The component paradigm is a basic paradigm which is applicable to real systems but also to models of reality [1].

6. MDA-based architectural framework and security infrastructure

For keeping such complex national project's specification and implementation manageable, the architectural framework including the security infrastructure as its integral part is strictly based on the ISO 10746 reference model – open distributed processing (RM-ODP) [9]. This concerns all newly developed applications, common services components, but also analysis and migration of legacy systems.
The ISO RM-ODP considers every component in distributed interoperable systems from different viewpoints, thereby abstracting from complex reality to interesting constraints such as concepts, contexts, structure, or behaviour (Fig. 6). Thus, a component's purpose (business view, scenario, policy), the information needed to describe the content (attributes) and function (operations) of a component (information view), component's functional aggregation (computational view), physical distribution

(engineering view), and implementation and operation principles (technology view) have been specified.

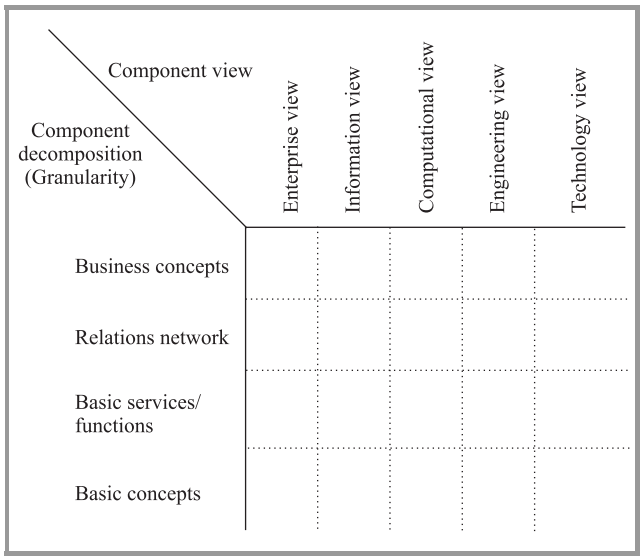

Fig. 6. Abstraction matrix of components.

Components can be composed/decomposed providing different levels of details or granularity. Starting from the granularity level of basic concepts of the corresponding domain, the complexity of aggregated components reflecting the application needed may be increased according to the users' needs. By that way, stand-alone applications, distributed applications or even highly complex networks can be implemented. In that context structural and functional complexity has to be considered as well. Components and their level of granularity can be selected according to the users' needs [1, 10].

In the first phase of modelling, the platform-independent specification of the components' properties is performed describing the business, the information, and the computational viewpoint of every component needed. Those models are portable to any environment with specific database models, operating systems' requirements, etc. This specification is transferred into the second phase of platform-specific modelling, covering the engineering and the technology viewpoint.

The separation of platform-independent and platform-specific models, distinguishing logic and technologic aspects is the core idea of Object Management Group's model driven architecture (MDA) for component-oriented information systems [11]. The specification of platform-independent models (PIM) is supported by appropriate tools. The transfer into platform-specific models (PSM) is automatically performed by tools. Both phases describe system components at meta-level using, e.g., the unified modeling language (UML) still abstracting from implementation details. The resulting graphical vocabulary can be transferred into verbal constraint models using the extensible markup language (XML). All models are developed starting from coarse description up to fine grained specialisation.

Thereby, the models follow the approach of the generic component model based on the ISO reference model – open distributed processing. For model management and the automatic development of running application at runtime, corresponding tools will be deployed. In a model driven architecture, the implementation is automatically performed using tools as demonstrated in the HARP project running at the Magdeburg Medical Informatics Department [12]. In the next section, this project will be shortly introduced.

Because different views can be described independently by domain experts, available knowledge can be exploited and specific terminologies can be applied correctly. For example, the concepts knowledge of medical doctors or procedural experience of administrators will be expressed in domain models referring to an information reference model established by IT experts. Beside agreed methodologies and tooling, accepted terminology maintained in a repository is a basic requirement. This terminology and ontology will be reused from SNOMED® with its extensions SNOMED_RT® and SNOMED_CT® as well as from the UMLS® created by the US NLM and meanwhile internationally maintained with important contributions by the British NHS. The outcome is transferred considering engineering aspects related to, e.g., the specific database model, which can be managed by DB experts.

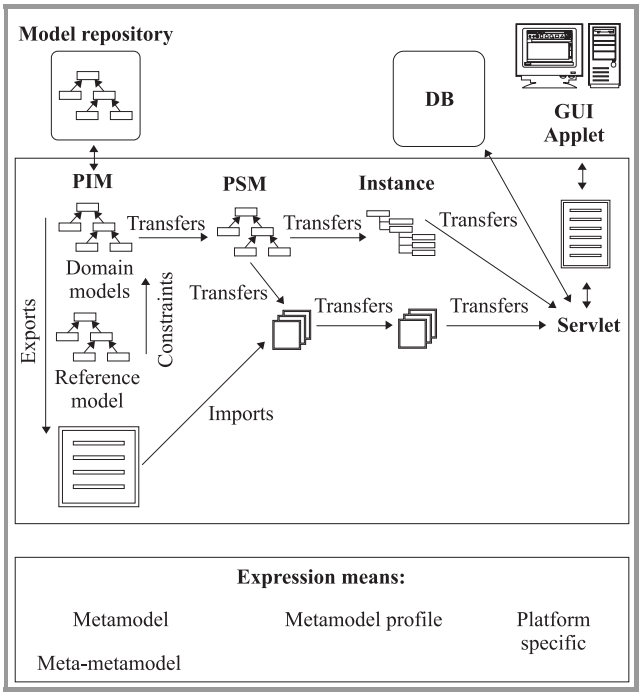

Fig. 7. MDA development nd expression means.

All different development phases from general requirements analysis over domain-specific views up to implementation and maintenance of any HIS can be described by MDA. Therefore, MDA allows also dealing with legacy systems to define interfaces and levels of interoperability. Figure 7 presents the MDA schema including the expression means used. As meta-languages, UML and XML have been introduced as mentioned already. Because of some weak-

nesses of the approved version UML 1.4, tools supporting the emerging UML version 2.0 have been used.

7. System integration and migration paths

Keeping in mind that systems consist of hierarchically built subsystems or capsules as shown in Fig. 8, at least three different levels of interoperability can be modelled and implemented starting at the highest level of service-oriented collaboration between directly related components (Fig. 9).

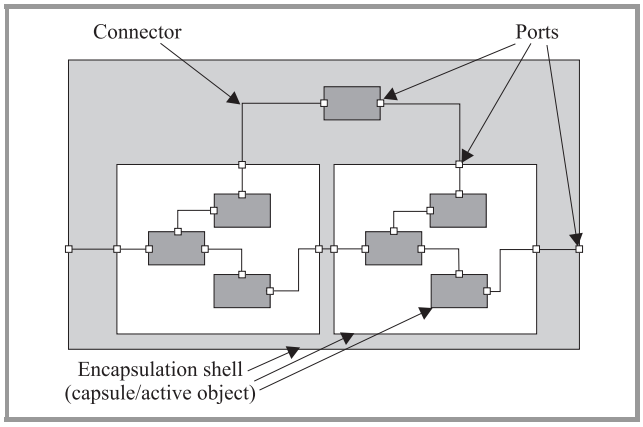

Fig. 8. Hierarchically built capsules.

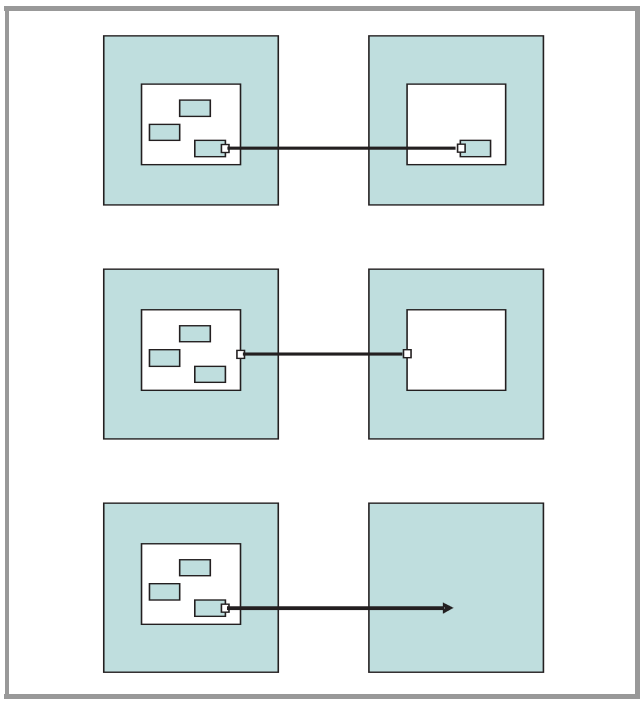

Fig. 9. Interoperability level.

The next level comprises aggregated services mediated either by super-component interactions or by the exchange of messages via architecture-independent interfaces (e.g., HL7 V2.x) [13]. Finally, proprietary communication or database import/export functions might be established. The aggregation of components and – by implementing them – services is mediated by components, in analogy to CORBA establishing horizontal or vertical services depending on the usability of those services by all domains or by a special one.

Platform-specific issues are kept out of scope as long as possible to enable a future proof HIS characterised by the aforementioned properties. For final implementation, they have to be realised, however.

8. Electronic health record

Because all facts directly or indirectly established during patient's care are needed for its optimised management, shared care information systems and networks have to be based on a comprehensive and lifelong virtual EHR system as the HIS core application. Therefore, the German health telematics platform must be completed by a modern EHR architecture, which is also open, component-based and model-driven, etc.

The EHR architecture deployed in the German health telematics project will be based on specifications provided by the revised CEN ENV 13606 "Electronic Health Record Communication" [14] and international projects and initiatives such as the openEHR Foundation [15]. Accordingly, the German electronic health card provides a tiny EHR extract. Furthermore, it establishes a tool (pointer facilities) for managing EHR systems in a patient-controlled way.

9. Architecture and security infrastructure implementation

Beside the definition and demonstration of an architectural framework and security infrastructure as German health telematics platform, the roll-out of that approach first manages the card-enabled environment, and second provides basics and migration path for a future-proof ICT supporting shared care.

In that context, the acceptance of the solution by patients and health professionals including responsible and influencing bodies within the German healthcare and social system is inevitable. For that reason, the creation of acceptance by public relation activities, support of the ministry in creation of positive opinions and resonance is an important work package. Additionally, the project management, quality assurance and quality management as well as an appropriate scientific accompaniment of the project are crucial success factors.

10. Conclusion

Modelled as a multi-model approach at meta-model level, the future-proof secure health information system (HIS) is

a virtual, at runtime self-organising architecture consisting of certified components which exchange digitally signed and attributed XML messages.
Reference model, constraint models, terminology, and methodology have to comply with international standards or must be standardised.
Following the challenging example of other countries such as Australia, Denmark, Finland, the USA, and certainly some others, Germany launched a programme for establishing a health telematics platform, which has to comply with the advanced paradigm of component-based MDA systems. First feasibility studies have been performed within the European HARP project the Magdeburg Medical Informatics Department being responsible for the modelling part has been involved in.

Acknowledgments

The authors are indebted to thank the European Commission and the German Federal Ministry for Health and Social Security for supporting their activities as well as the partners from the TrustHealth project, the GEHR/openEHR Foundation and the Object Management Group for collegial collaboration.

References

[1] B. Blobel, *Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems*. Series "Studies in Health Technology and Informatics". Amsterdam: IOS Press, 2002, vol. 89.

[2] German Federal Republic, Federal Ministry for Health and Social Affairs, http://www.bmgs.bund.de

[3] Aktionsforum Telematik im Gesundheitswesen, http://www.atg.gvg-koeln.de

[4] Council of Europe. Council of Europe 99/93/EC: Directive on Electronic Signatures. Strasbourg, 1999.

[5] B. Blobel, "The European TrustHealth project experiences with implementing a security infrastructure", *Int. J. Med. Inform.*, vol. 60, pp. 193–201, 2000.

[6] CEN ENV 13729 "Health Informatics – Secure User Identification – Strong Authentication Using Microprocessor Cards", 2000.

[7] HPC. The German HPC specification for an electronic doctor's licence, V 1.0, 1999, http://www,hpc-protocol.de

[8] Federal Ministry for Health and Social Affairs. BIT 4 Health, http://www.bmgs.bund.de/deu/gra/ministerium/ausschreibungen/index.cfm

[9] "Information technology – Open Distributed Processing – Reference Model", ISO/IEC 10746.

[10] *Advanced Health Telematics and Telemedicine. The Magdeburg Expert Summit Textbook*, B. Blobel and P. Pharow, Eds. Series "Studies in Health Technology and Informatics". Amsterdam: IOS Press, 2003, vol. 96.

[11] Object Management Group, Inc. CORBA Specifications, http://www.omg.org

[12] HARP Consortium, http://www.ist-harp.org

[13] Health Level 7, Inc., http://www.hl7.org

[14] Comité Européen de Normalisation, http://centc251.org

[15] openEHR Foundation, http://www.openehr.org

Bernd Blobel is Head of the Health Telematics Project Group at Fraunhofer Institute for Integrated Circuits (IIS) in Erlangen, Germany. He worked for more than 20 years as founder and head of the Medical Informatics Department at the Magdeburg University Hospital. His areas of interests are advanced health information systems architecture, electronic health records, modelling, knowledge representation, clinical guidelines, security, privacy, standardisation, and interoperability. Among others, he is chair of the CEN/ISSS eHealth Standardization Focus Group, chair of the EFMI WGs "Electronic Health Records" and "Security, Safety and Privacy", chair of HL7 Germany, co-chair of the WITFOR Healthcare Chapter. Associate Professor Bernd Blobel is strongly involved in the national health telematics projects, e.g., in Germany, USA, and Australia. He is author of several books and more than 270 scientific papers.
e-mail: bbl@iis.fraunhofer.de
Health Telematics Project Group
Fraunhofer Institute for Integrated Circuits IIS
Am Wolfsmantel 33
D-91058 Erlangen, Germany

Peter Pharow currently works as senior scientist within the Health Telematics Project Group at Fraunhofer Institute for Integrated Circuits (IIS) in Erlangen, Germany. His specific working areas are aspects of security, safety, and quality in health informatics, legal aspects, data security and data protection, security services, mechanisms, and infrastructures, security policy and policy templates, health professional cards, trusted third party infrastructures and related services as well as health networks and user behaviour. He is author of more than 70 scientific papers.
e-mail: phw@iis.fraunhofer.de
Health Telematics Project Group
Fraunhofer Institute for Integrated Circuits IIS
Am Wolfsmantel 33
D-91058 Erlangen, Germany