Architecture of Secure Portable and Interoperable Electronic Health Records

Bernd Blobel

Otto-von-Guericke University of Magdeburg, Medical Faculty, Institute of Biometry and Medical Informatics, Leipziger Str. 44, D-39120 Magdeburg, Germany
bernd.blobel@mrz.uni-magdeburg.de

Abstract. Electronic Health Records (EHR) are moving towards the core application of health information systems. Enabling informational interoperability of shared care environment including EHR, structure and function of components used have to follow open standards and publicly available specifications. This comprises includes also methods and tools applied. After shortly introducing general aspects of open interoperable component architectures, actual approaches for EHR systems are discussed distinguishing between the one-model and the dual-model paradigm. The emerging activities for a harmonised multimodel openEHR as well as its implementation are presented. Special attention is given to security requirements and solutions. Based on standardised Public Key Infrastructure (PKI) and security token such as Health Professional Cards (HPC), policy-defined application security services such as authorisation, access control, accountability, etc., of information recorded, stored and processed must be guaranteed. In that context, appropriate resource access decision services have to be established. As the European HARP project result, a component-based EHR architecture has been specified and demonstrated for enabling open, distributed, virtual, and portable EHR implementation with enforcing fine-grained security services by binding certificates to application components, by the way enforcing policies.

1 Introduction

For establishing efficient and high quality care of patients, comprehensive and accurate information about status and processes directly and indirectly related to patient's health must be provided and managed. Such information concerns medical observations, ward procedures, laboratory results, medical controlling, account management and billing, materials, pharmacy, etc. Therefore, health information systems within healthcare establishments (HCE) converge to Electronic Patient Record (EPR) systems as a kernel enabling the management of all the other business processes as specific views on the EPR and building the informational basis for any communication and co-operation within, and between, healthcare establishments (HCE). By that way, inter-organisational vir-

P.M.A. Sloot et al. (Eds.): ICCS 2002, LNCS 2330, pp. 982–994, 2002.

tual electronic healthcare records (EHCR)[1] are built. This virtual EHCR has to met shared care requirements of providing any information needed and permitted at the right time to the authorised user at any location in the right format including mobile devices. In that context, it has to fulfil all the needs of the HCE and its principals involved reflecting all the views defined in ISO/IEC 10746-2 "Reference Model – Open Distributed Processing", such as enterprise view, information view, computational view, engineering view, and technological view [9]. These views are different in different HCE with their different scenarios for meeting different requirements under their specific conditions and restrictions. For providing information and functionality needed, EHCR must be structured and operating appropriately.

First, some definitions related to EHCR should be introduced:

- An EHCR is a repository of information about the patient's health available in a computer-readable format.
- An EHCR system is a set of components establishing mechanisms to generate, use, store and retrieve an EPR.
- An EHCR architecture describes a model of generic properties required for any EPR for providing communicable, comprehensive, useful, effective, and legally binding records, which preserve their integrity over the time independent of platforms and systems as well as of national specialities.

Following, different approaches and an optimal way for meeting the requirements and characteristics mentioned is described in more detail by focusing on the architectural and modelling aspects of EHCR.

2 The Generic Component Paradigm for EHCR Architecture

Regarding EHR in general, we have to look for structure and domain knowledge related concepts, but also for the concepts of security, safety and quality. Considering security issues, the concepts of communication security can be distinguished from application security. Quality and safety are related to the latter one. Within one concept, different levels of granularity and abstraction can be defined forming a layered model of services, mechanisms, algorithms, and data [2].

$$\text{object} = \text{attributes} + \text{operations} \qquad (1)$$

However, objects require knowledge about object-to-object interactions to be completely useable, reusable, and interoperable on all the different levels of the ISO RM – ODP. Such requirements and conditions of interactions concern pre-conditions, post-conditions, constraints, group behaviour, etc. Within the object-oriented world, the management of object-to-object interactions can, e.g., only be provided at the CORBA COSS level, whereas the healthcare vertical facilities need the specification of this

[1] If the record includes also issues beyond patient's care such as, e.g., social aspects and health prevention of citizens, an electronic health record (EHR) is created. In the paper, the EHCR view will be used knowing the validity of the statements also for EHR, however.

knowledge about conditions, relationships, and framework at the business object component architecture level [11].

Figure 1 presents the conceptual schema of the original approach of CORBA. This CORBA conceptual schema enabled already grouping, multi-interfacing, etc.

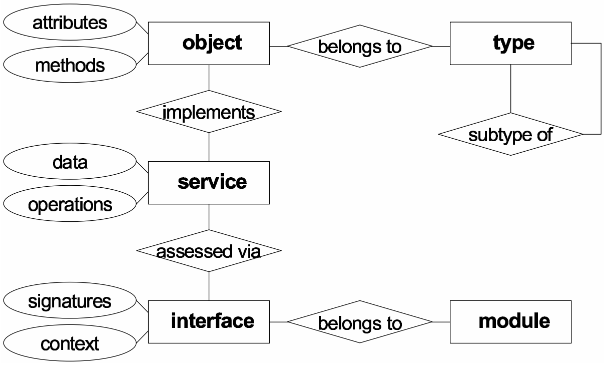

Fig. 1. The CORBA Conceptual Schema

To overcome these problems, a generic component architecture paradigm has been developed by the Magdeburg Medical Informatics Department at 1995. Contrasting to objects, a component is defined as shown in equation (2). The conceptual schema of such generic components is given in figure 2.

component =	attributes + operations + structural constraints + operational constraints + events + multi-interfaces * scenarios + safety + reliability + security + ...	(2)

3 Available EHCR Architecture Models

An EHCR has to meet requirement, that are already investigated e.g., in the context of several EHCR projects. Managing objects, an EHCR arises as dynamic process from clinical practice. It manages a complex workflow connected with medical acts. The EHCR is based on, and supports, electronic communication between all parties involved. It documents any diagnostic and therapeutic measures in a standardised structure. Reducing or avoiding redundancy, an EHCR facilitates an optimised unambiguous presentation of medical concepts, preserving the original context and enabling new ones. It reflects chronology and accommodates future developments and views. For managing an EHCR system, the architecture of such distributed and highly complex component system as well as its behaviour (functionality, set of services) must be designed appropriately.

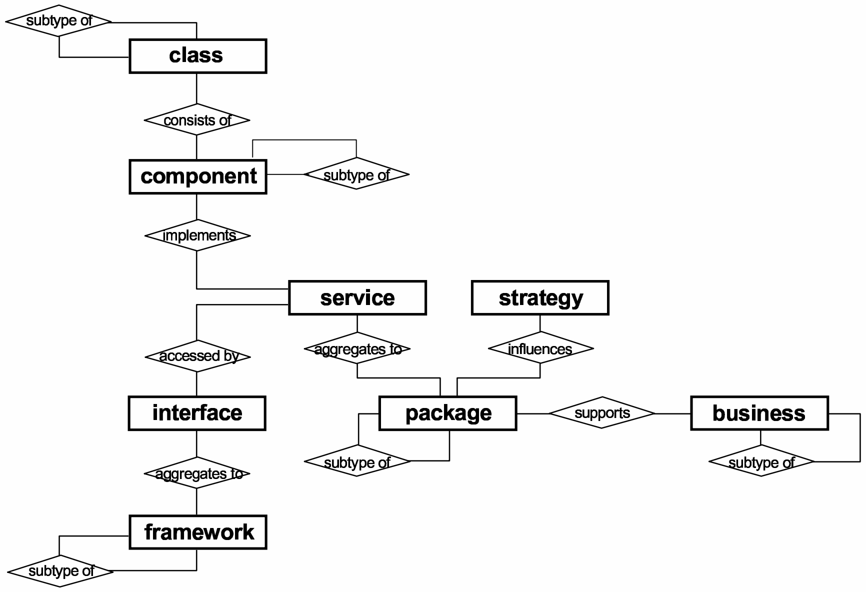

Fig. 2. The Conceptual Schema of the Generic Component Model [2]

Replacing the old relation paradigm of some architecture models for health information systems such as, e.g., the Distributed healthcare Environment (DHE) architecture, the actual EHCR architecture standard models follow the object-oriented or even component-oriented paradigm. However, they are distinguished by a fundamental difference in their approach of establishing the EHCR model. One group intends to develop the complete EHCR architecture within one comprehensive model of structures, functions, and terminology in the classic way covering all the concepts known at the development time. Such an one model approach however reveals some essential weaknesses and problems related to technical, complexity, and management issues which are now shortly resumed [1]:

Considering the technical problems of the one model approach, the mixture of generic and domain-specific knowledge concepts with their own expressions, but also weaknesses in basis class stability must be mentioned.

Regarding the complexity problems, the size of the resulting model leads to difficulties in managing so many concepts in parallel, in completing the model which might be unachievable, in standardising such models and in providing interoperability due to the needed agreement on a huge number of aspects and details.

Related to the management of the one model approach, different developer and user groups dealing with their own concepts expressed in their specific language must be managed, combined and harmonised. The generic part of the EHCR concepts concerns the grammar of the IT-system domain which is specified by computer scientists. The health domain specific concepts representing the domain knowledge are specified and maintained by medical experts. Both groups are characterised by their own terminology and their specific way of thinking. The dependency of both groups results from the fact that there is only one common development process using one formalism.

The other group provides a dual model approach establishing a generic object or component model and a set of specialised models reflecting organisational, functional, operational, contextual, and policy requirements presenting the knowledge about the detailed circumstances of practical EHCR instances overcoming the one model approach's problems.

An example of the first group is the CEN ENV 13606 "Electronic Healthcare Record Communication". HL7's version 3 models and the Australian GEHR approach belong to the second group, despite of the differences explained in detail in the next chapters. By that way, the component characteristic of equation (2) is established which has been completely realised by the GEHR approach.

3.1 EHCR One-Model Approaches

3.1.1 The CEN "Electronic Healthcare Record Communication" Standard

The CEN ENV 13606 "EHCR Communication" defines in its Part 1 an extended component-based EHCR reference architecture [3]. Such an extended architecture is mandated to meet any requirements through the EHCR's complete lifecycle. According to CEN ENV 13606, an EHCR comprises on the one hand a *Root Architectural Component* and on the other hand a *Record Component* established by *Original Component Complexes* (OCC), *Selected Component Complexes*, *Data Items*, and *Link Items*. OCC consist of 4 basic components, such as folders, compositions, headed sections, and clusters. These OCC sub-components can be combined in partially recursive ways. Beside its Part 1 "Extended Architecture", the CEN ENV 13606 offers the Part 2 "Domain Term List", Part 3 "Distribution Rules", and Part 4 "Messages for the Exchange of Information".

3.1.2 The Governmental Computerised Patient Record Project

Launched by a consortium formed by the US Department of Defense, the US Department of Veterans Affairs, and the Indian Health Service, the Governmental Computerised Patient Record (G-CPR) established a model and tools for implementing and managing an proper business as well as technical environment to share patient's information [5]. The main goals concern

- the establishment of a secure technical environment for sharing sensitive personal information,
- the development of a patient focused national information technology architecture,
- the creation of common information model and adequate terminology models to ensure interoperability between disparate systems.

The solution should be based on advanced national and international standards. Using object oriented specifications for interoperability, the approach was rather service oriented than architecture based.

3.2 EHCR Dual-Model Approaches

3.2.1 The GEHR Approach

Based on the European Commission's Third Framework Programme project "Good European Health Record (GEHR)", but also acknowledging the results of other R&D projects and efforts for standards around the globe, the Australian Government launched and funded the Good Electronic Health Record (GEHR) project [6]. The basic challenge towards GEHR is knowledge level interoperability.

The GEHR model consists of two parts: the *GEHR Object Model* (GOM), also called reference model, delivering the EHCR information container needed on the one hand, and the GEHR meta-models for expressing the clinical content on the other hand (figure 3).

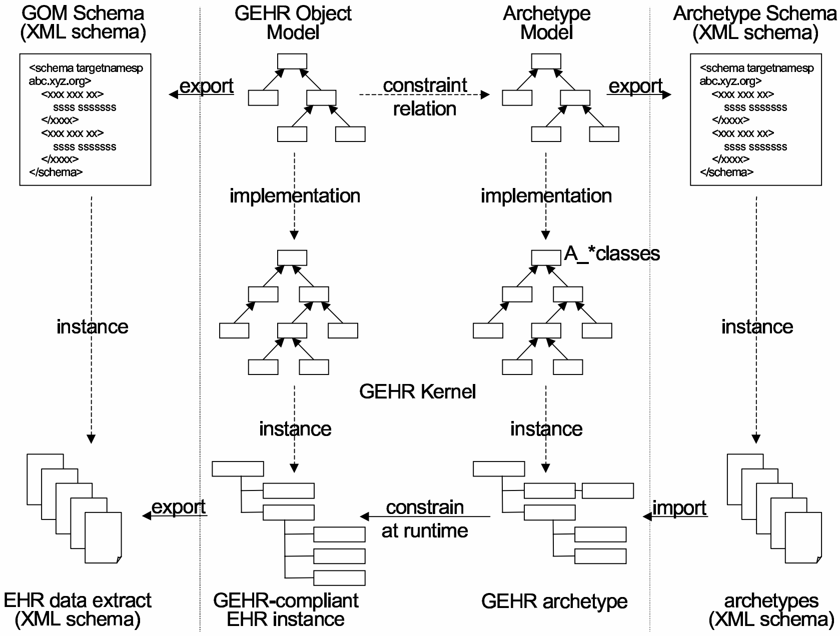

Fig. 3. GEHR Architectural Schema (after T. Beale [1])

Bearing the medical knowledge in the sense of healthcare speciality-specific or the organisation-specific, department-specific or even person-specific views and restrictions, the meta-models are commonly called *Archetypes*. Therefore, the corresponding model is also called archetype model. Because the archetypes are separately developed, they can be instantiated step by step at the technical model level until the complete medical ontology has been specified. In summary, the GEHR approach consists of small flexible pieces like LEGO® bricks which can be combined in a proper, health domain specific way following construction plans defined in archetypes. Summarily, the reference model is the concrete model from which software can be built, and of which EHR data are instances. The archetype model establishes a formalism whose instances are domain concepts which are directly processable by health information systems.

3.2.2 The HL7 Reference Information Model and its Clinical Document Architecture

Within its Version 3 *Message Development Framework*, the well known health industry standard for communication HL7 specified a comprehensive *Reference Information Model* (RIM) covering any information in the healthcare domain in a generic and comprehensive way [8]. The HL7 RIM deals with the associations between the six core classes *entity* (physical information object in the healthcare domain), the *role* the entity can play (competence for action), *participation* (performance of action), the *act* as well as *role relationship* mediating interaction between entities in the appropriate roles and *act relationship* for chaining different activities. HL7's RIM and vocabulary provide domain knowledge which is exploitable, e.g., for knowledge representation (representation of concepts and relations) in the GEHR Object Model and archetypes discussed before.

The specialised model for Clinical Document Architecture (CDA) has been specified for developing appropriate messages to support EHR communications. It is based on the generic RIM and its refinements as *Refined Message Information Model* (R-MIM) and *Common Message Element Types* (CMET) for EHR related scenarios. It establishes a dual model approach analogous to the GEHR approach.

The HL7 approach reflects solely the information viewpoint of ISO RM – ODP. Within information models, it describes classes, attributes and their specialisations for developing messages. Therefore, HL7 provides interoperability at data level but not at functional level.

3.3 EHCR/EHR Architecture Model Harmonisation and Emerging Projects

Establishing formal and informal liaisons, organisations engaged in EHCR or EHR specification and implementation intend to improve the existing standards. In that context, several activities have to be mentioned especially such as

- the recently started improvement of CEN ENV 13606 now called "Electronic Health Record Communication",
- the refinement of G-CPR in the sense of emphasising HL7 communication instead of CORBA service orientation,
- the establishment of the European Commission's EUROREC organisation, and
- the openEHR approach.

Collaborating with HL7, both CEN and openEHR will narrow and harmonise their approaches. Establishing a (initially funded) national EUROREC organisation in all the European Union member states, the EuroRec initiative concerns the improvement of awareness for, and the wider implementation of, EHR in the European practice. In that context, a European Electronic Health Record institute has been founded at November 2001.

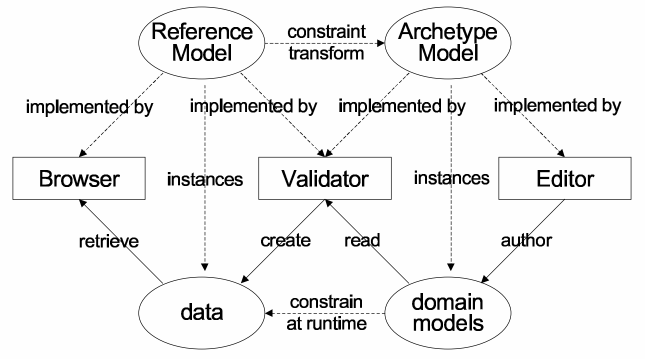

Fig. 4. Meta-Architecture for Implementing and Use of OpenEHR

Regarding implementation and use of the openEHR approach, the model components and system components needed can be presented as shown in figure 4. Based on the models introduced in section 3.2.1, editors are needed to author the domain knowledge in domain models. Read by the openEHR kernel, this information is used to create the object model instances, i.e., the data the principal is interested in to be retrieved and presented by a browser.

4 OpenEHR Package Structure

For implementing openEHR, several system components or packages have to be established. The EHR basic structure is the *Record*. Its sub-packages describe the compositional structure of an EHR. The *Record* package contains the packages *EHR* (incl. EHR extracts), *Transactions* (incl. audit trail), and the related content. The latter contains the *Navigation*, *Entry*, and *Data* packages, whose classes describe the structure and semantics of the contents of transactions in the health record. The *Path* serves for item location. The basic package defines the core classes used in the openEHR approach. *External* refers to external packages providing interoperability with non-EHR systems. The *Party* package addresses the principals involved such as users, systems, components, devices, etc.

Figure 5 presents the package structure of an openEHR system as described.

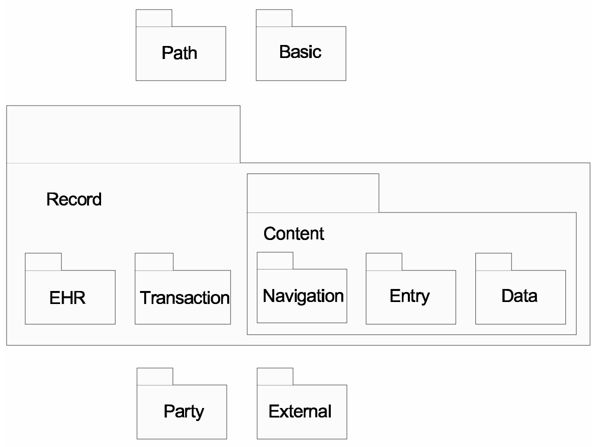

Fig. 5. Package Structure of the openEHR Reference Model

5 The HARP[2] EHR Implementation

According to the generic component model [2], all views, information content, functionality, implementation environment, and underlying technology but also the proper level of granularity might be modelled in a consistent way. In this way services and the complexity of the running application component can be defined according to the application environment and the user needs. Services concern entry, processing, and presentation of data but also the enforcement of underlying policy for communication and co-operation. The generic component model enables claims change management (viewpoint of the system) and the resolution of the component's complexity by the transition to less complex sub-components as shown in figure 6. Each specific model in the abstraction-granularity space reflects one specific archetype. A theoretical consideration on consistency for state transitions within the generic model have been provided in [2].

The description of the components according to equation (2) is established in archetype schemas using the XML (Extensible Markup Language) standard set. Related to granularity and technology viewpoint, mobile computing has to meet special requirements which are easily enabled by this dynamic selective approach of the proper state of the a complex system.

Within the HARP project, partners from Greece, Germany, Norway, United Kingdom, and the Netherlands specified, developed and implemented the HARP Cross Security Platform (HCSP) for Internet based secure component systems as well as the development methodology and the development tools needed have been specified.

[2] The HARP (Harmonisation for the Security of Web Technologies and Applications) project (Project Number: IST-1999-10923) was funded by the European Commission within the Information Society Technologies (IST) Programme Framework

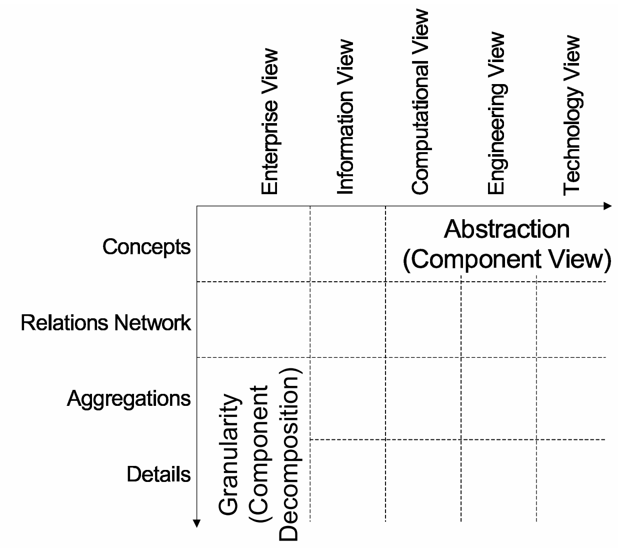

Fig. 6. State Transitions within the Abstraction-Granularity Matrix of Component Systems

5.1 Security Services in the OpenEHR Context

As already mentioned, the archetypes describe conceptual, contextual, organisational, functional, but also legal and ethical framework of the EHCR system and its behaviour. Such framework is also called policy. Archetypes define the domain-specific constraints to be established. Therefore, archetypes enable the description of policies. By refining archetypes, detailed specifications for security services such as authorisation and access control management can be specified and at runtime instantiated. Following the GEHR approach, the overall policy as well as its refinements in special policies and detailed security services sense should be specified in archetype models and expressed in XML schema. The generic meta-models have to be specified using the XML Schema standard.

5.2 The HARP Cross Security Platform

The HARP project's objective is building up entirely secure applications in client-server environments over the Web. Real interoperability leads to a closer connection of both communication and application security services. Communication security services comprise strong mutual authentication and accountability of principals involved, integrity, confidentiality and availability of communicated information as well as some notary's services. As a result of the authentication procedure, authorisation for having access to the other principal has to be decided. Application security services concern accountability, authorisation and access control regarding data and functions, integrity, availability, confidentiality of information recorded, processed and stored as well as some notary's services and audit.

To provide platform independence of solutions in HARP as a real three tiers architecture, the design pattern approach of developing a middleware-like common cross platform (HCSP) has been used. In HCSP, platform-specific security features have been isolated. Using an abstraction layer, communication in different environment is enabled. According to the component paradigm, an interface definition of a component providing a platform-specific service specifies how a client accesses a service without regard of how that service is implemented. So, the HCSP design isolates and encapsulates the implementation of platform-specific services behind a platform-neutral interface as well as reduces the visible complexity. Only a small portion has to be rewritten for each platform The solutions concern secure authentication as well as authorisation of principals even not registered before, deploying proper Enhanced Trusted Third Party (ETTP) services [7]. Especially, it helps to endorse policies by mapping them on processing components. For that reason, HARP components follow the specification of equation (2).

HARP's generic approach implements several basic principles. HARP's solution of embedding security into any application to be instantiated over the web-based environment outlined above is based on object oriented programming principles. It is based on Internet technology and protocols solely. The trustworthiness needed has been provided by applying only certified components which are tailored according to the principal's role. In fine-grained steps, it establishes its complete environment required, avoiding any external services possibly compromised. After strong mutual authentication based on smartcards [4] and TTP services [10], the security infrastructure components are downloaded and installed to be used for implementing the components needed to run the application as well as to transfer data input and output. The SSL (Secure Socket Layer) protocol deployed to initiate secure sessions is provided by the Java Secure Socket Extension API. The applets and servlets for establishing the local client and the open remote database access facilities communicate using the XML standard set including XML Digital Signature. Because messages and not single items are signed, the messages are archived separately for accountability reasons meeting the legislation and regulations for health.

Policies are dynamically interpreted and adhered to the components. All components applied at both server and client site are checked twice against the user's role and the appropriate policy: first in context of their selection and provision and second in context of their use and functionality.

Applet security from the execution point of view is provided through the secure downloading of policy files, which determine all access rights in the client terminal.

This has to be seen on top of the very desirable feature that the local, powerful, and versatile code is strictly transient and subject to predefined and securely controlled download procedures. All rights corresponding to predefined roles are subject to personal card identification with remote mapping of identity to roles and thereby to corresponding security policies with specific access rights.

For realising the services and procedures described, an applet consists of the subcomponents GUI and interface controller, smartcard controller, XML signing and XML processing components, communication component applying the Java SSL extension, and last but not least the data processing and activity controller. Beside equivalent sub-components and an attribute certificate repository at the server side, policy repository, policy solver and authorisation manager have been specified and implemented as a "light weight" Resource Access Decision service (CORBA: RAD).

After exchanging certificates and establishing the authenticated secure session, servlet security is provided from the execution point of view through listing, selecting and finally executing the components to serve the user properly. By establishing an authenticated session that persists for all service selections, a single-sign-on approach can be realised.

HARP enables the implementation of openEHR in a convincing way. Using the open environment of certified Java™ components, portability of the HARP solution to any platform is guaranteed.

In the server-centric approach, a web-accessible middleware has been chosen based on its support of basic security functionality, e.g., MICO/SSL., Apache Web server with mod_ssl, Apache JServ, and Apache Jakata Tomcat.

Combining the server-centric approach of HCSP, its server-centric approach and the network-centric VPN behaviour, the completely distributed HARP Cross Security Platform has been designed.

5.3 Harmonising the HARP Approach and OpenEHR

The HARP approach enables the implementation of any EHR component following constraints defined in archetype models and expressed in XML schema. The HCSP facilitate the instantiation of those components by combining both specifications in the sense of certified components. So, any granularity, any constrain in the sense of domain knowledge, organisational structure, underlying policy, technological requirements for structure and presentation providing portability, etc. are supported properly. The development of HARP rules underlying the XML messages which establish the HARP components (servlets and applets) is based on UML models. Within the HARP project developed independently from openEHR, these models reflect archetypes. For enhancing the current openEHR specification by security archetypes, a harmonisation in concepts and especially terminology used must be performed.

6 Conclusions

EHR architecture and subsequently specified and implemented EHR systems have to meet the shared care paradigm establishing openness, interoperability, scalability, and portability for providing any needed and permitted information to any authorised user at time, location, and format required, including mobile devices. Furthermore, EHR systems have to comply with comprehensive security solutions solely based on available and emerging standards. Actual EHR architecture standards comparably presented in the paper move in the direction requested. Emerging common projects harmonise the different approaches towards an "global" openEHR.

The European HARP project specified and implemented open portable EHR systems enriched with enhanced TTP services and comprehensive development strategies for establishing fine grained application security services. Constraints specified can be bound to components at runtime, enabling different views or supporting specific domain knowledge concepts. By binding attribute certificates to components appropriate policies can be enforced. These constraints such as, e.g., certificates are interpreted at both server and client sides using authorisation services. The HARP Cross Security Platform is solely based on standards including the XML standard set for the establishment of EHR clients and servers as well as their communication.

7 Acknowledgement

The author is in debt to the European Commission for funding and to the EHR community as well as to the HARP project partners for their support and their kind cooperation.

8 References

1. T. Beale: An Interoperable Knowledge Methodology for Future-Proof Information Systems, 2001
2. B. Blobel: Application of the Component Paradigm for Analysis and Design of Advanced Health System Architectures. *International Journal of Medical Informatics* **60** (3) (2000) 281-301.
3. CEN ENV 13606 "Health Informatics – Electronic Healthcare Record Communication", 1999
4. CEN TC 251 ENV 13729 "Health Informatics - Secure User Identification – Strong Authentication using Microprocessor Cards (SEC-ID/CARDS)", 1999.
5. G-CPR Project: www.gcpr.gov
6. GEHR Project: www.gehr.org
7. The HARP Consortium: http://www.ist-harp.org
8. Health Level Seven, Inc.: www.hl7.org
9. ISO/IEC 10746-2 "Information Technology – Open Distributed Processing – Reference Model: Part 2: Foundations".
10. ISO DTS 17090 "Public Key Infrastructure, Part 1 – 3", 2001.
11. Object Management Group, Inc.: CORBA Specifications. http://www.omg.org
12. Object Management Group, Inc.: The CORBA Security Specification. Framingham: Object Management Group, Inc., 1995, 1997.