Medical Data GRIDs as Approach towards Secure Cross Enterprise Document Sharing (Based on IHE XDS)

Wozak F[1], Ammenwerth E[1], Breu M[2], Penz R[3], Schabetsberger T[1], Vogl R[3], Wurz M[4]
[1]Institut für Informationssysteme im Gesundheitswesen, Private Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik Tirol, Österreich
[2]Leopold-Franzens-Universität Innsbruck, Österreich
[3]Health Information Technologies Tirol GmbH, Österreich
[4]Icoserve Information Technologies, Österreich
florian.wozak@umit.at

Introduction The electronic processing of medical data which is expected to improve quality and efficiency of health care services [1] will lead to an increasing amount of medical data exchanged across institutional boundaries [2].

The greatest benefit is expected if concise medical data are available for the patient him-self as well as for medical institutions involved in the treatment process. Presently communication among institutions in the healthcare environment is based on directed data flow, implying that the intended receiver has to be known at the very beginning of the communication process, resulting in documents to be sent from the producing institution to each requester.

Based on an initial analysis of functional requirements for shared electronic health records technical requirements have been elaborated [3]. They mainly comprise security, scalability and high availability. Research revealed that distributed architectures seem to be most appropriate for this field of application since data and indices remain stored locally at the producing institution, which avoids single point of failure and attack. Thus without centralized data processing centers, scalability is expected to improve, particularly in a trans-regional context. A variety of architectures described in literature rely at least partly on centralized services and adequate approaches for distributed architectures seem to be missing. So the aim was to develop a network architecture completely based on distributed services. We decided to take the IHE-XDS (IHE cross document sharing) profile as basis for the exchange of clinical documents [4]. The proposed architecture we use for a shared electronic health record (SEHR) is designed to be highly scalable and to comply with both, the cross enterprise document sharing specification (IHE-XDS) and the Austrian federal law for health telematics [5]. For this reason an architecture following the blueprint of Medical Data GRIDs seem to be most appropriate [6]. Data handled by a shared electronic health record and their analysis and procession are specific to a medical domain such as laboratory results or radiological images. These specific requirements demand for adaptation of the data GRID architecture definition. For this work we extend the original definition to meet legal and organizational requirements of the environment they are operated in.

Methods In an initial step functional requirements for a SEHR have been analyzed. According to these requirements the implementation of the architecture was designed. Functional requirements are recorded along with security requirements of the trans-institutional workflows in a SEHR. A starting point is the document model that defines the basic objects that are managed and exchanged by the system. In parallel a role model is developed that reflects the permissions and capabilities of the users of the system. These models guide through the elicitation of security requirements.

IHE is an initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. The IHE cross enterprise document sharing profile (XDS) provides an architectural approach for document sharing in heterogeneous health care environments.

Results: The proposals from the Austrian e-Health initiative are the foundation for the implementation of the health@net [7] core architecture. Currently we are implementing an open source prototype architecture based on the IHE XDS specification. The architecture and specific modifications necessary to meet legal and organizational requirements are described as follows. To ensure greatest possible flexibility and scalability, a distributed approach following the above introduced paradigm of Medical Data GRIDs was chosen and implemented widespread Web service technology. The core architecture consists of independent services responsible for storing documents and corresponding meta data, security features, unique patient identification and service discovery according to the IHE XDS specification. To guarantee a high level of security beyond the application security covered by role based access control, well proved security concepts are applied.

Core functionality is provided by the three service groups. *Document Repository*, *Document Registry* and *Patient Id Source*. Medical documents remain stored in the organization where they have been produced in the Document Repository (DR). The *Document Clearing* service (DC) is responsible for converting documents from a proprietary format to the clinical document architecture CDA [8] and mapping of locally used patient identification to the internally used unique identification. The Document Registry service provides functionality for document search, per-document access permissions, a link to the physical location at the Document Repository as well as a service discovery unit. This service group comprises three services: *Document Meta Data Index* (DMDI), which holds search relevant meta data as well as document based access permissions. The *Global Index* (GI) is responsible for finding Meta Data Index services that hold document meta data for a specific patient identified by the unique patient ID. Document consumers are only permitted to access the architecture via a gateway with well defined interfaces, provided by the *Access Nodes* (AN), which generate queries to the architecture. The Patient Id Source service group provides for unique patient identification across institutional boundaries, independent form patient's nationality. The Austrian legal situation and the fact that a unique patient identification does no (yet) exist requires different services, partly provided by the Austrian government to be integrated in the architecture. A *Patient Lookup Index* (PLI) is used as interface for other services (mostly DC and AN) to obtain a unique patient identification based on demographic data. A *Patient Lookup* service (PL) is used to obtain this identifier transparently for the architecture from different governmental person ID sources.

Currently two different approaches are being evaluated for services which allow the patient to give fine grained permissions to physicians and institutions which allows them to access specific parts of the record:

1. Distributed services, which manage and enforce access permissions assigned by the patient using roles defined by the e-Health directory.
2. A permission management system based on attribute certificates, digital certificates issued for each permitted operation.

Due to the early stage of evaluation this service is not implemented in the first prototype. The privacy of patient related data is temporarily solved in a way that participating institutions are bound by contract to only access data relevant for the specific treatment case. A variety of work flows such as the adding, retrieval, version-save updates of documents and correction of misidentified patients are supported by the architecture. Their detailed description is beyond the scope of this work.

Diskussion The development of the network architecture follows an iterative approach which we have chosen to gradually adopt the architecture to evolving requirements of the major players. In this article the first prototype implementation is described, which of course lacks certain functionality and implements only simplified security requirements. To guarantee the highest level of data protection for patients, in the initial prototype phase physicians who test the architecture are conscientiously selected and will be bounded by contract to respect the patient's consent. The operators of the architecture commit themselves to prove the adherence to the contract by collecting random samples from logging.

Though the developed architecture follows the paradigm of Medical Data GRIDs, currently available GRID middleware such as the GLOBUS-Toolkit [9] is not used in this setup. The main reason is that requirements for Medical Data GRIDs as outlined above are currently not satisfactorily covered and only a subset of the provided GRID features would be used. Nevertheless, the evaluation of the GLOBUS-Toolkit version 4 revealed some useful concepts. Since they mainly rely on open standards defined by the OASIS working group [10] those concepts have been integrated in the architecture. Our implementation of the architecture follows the IHE XDS specification as closely as possible, nevertheless the Austrian federal law demands for specific modifications of the architecture as described above for patient identification and usage of the central e-Health register.

We expect to gain knowledge about the development of a shared electronic health record and how proprietary systems, particularly the clinical information system from the Innsbruck University Hospital can be integrated in this environment. Before the architecture can be used in productive environments technical and organizational issues have to be solved comprising extended security, financing and cooperation with other health care institutions.

Literature

[1] Maglaveras N, Chouvarda I, Koutkias V, Meletiadis S, Haris K, Balas EA. Information technology can enhance quality in regional health delivery. Methods Inf Med 2002;41(5):393–400.

[2] Haux R, Ammenwerth E, Herzog W, Knaup P. Health care in the information society. A prognosis for the year 2013. Int J Med Inform 2002;66(1-3):3–21.

[3] 1.Schabetsberger T, Ammenwerth E, Goebel G, Lechleitner G, Penz R, Vogl R, Wozak F. What are Functional Requirements of Future Shared Electronic Health Records? In: Engelbrecht R, Geissbuhler A, Lovis C, Mihalas G. European Notes in Medical Informatics (CD-Rom): Connecting Medical Informatics and Bio-Informatics; MIE2005; 2005 Aug 28-31; Geneve, Switzerland. Vol. I Nr. 1, 2005. ISSN 1861-3179.

[4] IHE Radiology Technical Framework Supplement Cross-enterprise Document Sharing for Imaging (XDS-I) [homepage in the Internet]. IHE.net; c2005 [cited 2005 Dec 19]. Available from: http://www.ihe.net/Technical_Framework/upload/IHE_RAD-TF_Suppl_XDSI_TI_2005-08-15.pdf.

[5] Gesundheitsreformgesetz 2005, BGBl. I Nr. 179/2004, (Dec 30 2004).

[6] Leoni L, Manca S, Giachetti A, Zanetti G. A Virtual Grid Architecture for Medical Data Using SRB. In: Inchingolo P, Pozzi-Mucelli R, editors. EuroPACS - MIR 2004 In The Enlarged Europe. vol. 1. E.U.T. Edizioni Universita' di Trieste; 2004. p. 475–478.

[7] Schabetsberger T, Ammenwerth E, Andreatta S, Gratl G, Haux R, Lechleitner G, Schindelwig K, Stark C, Vogl R, Wilhelmy I, Wozak F. From a Paper-based Transmission of Discharge Summaries to Electronic Communication in Health Care Regions. IJMI. In press.

[8] HL7 Clinical Document Architecture Release 2.0 [homepage in the Internet]. hl7.org;[cited 2006 Mar 19]. Available from: http://www.hl7.org.

[9] Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International J Supercomputer Applications 2001.

[10] OASIS [homepage in the Internet]. OASIS Open; c2005 [cited 2005 Dec 11]. Available from: http://www.oasis-open.org/.