Medical Infobahn for Europe
A. Hasman et al. (Eds.)
IOS Press, 2000

MedStage – Platform for Information and Communication in Healthcare

Hans Schüll, Dr. Volker Schmidt
Siemens AG Medical Engineering, Erlangen, Germany

Abstract. This application report describes the technologies and strategies used by MedStage, an open infrastructure for secure telemedical internet applications. The infrastructure includes several technical and application frameworks including a public key infrastructure for providing professional security solutions, like certificate-based authentication, secure transport protocol, strong data encryption and digital signature. The key components are an universal healthcare data repository based on the work of CEN TC 251 with extensions for the storage of multimedia data, an exchangeable authorization management, an exchangeable patient index service based on CORBAmed PIDS and a set of XML-based import and export modules. Additionally there are prototype applications for home-monitoring, telereporting and personal health passport.

1. Introduction

In the past five years the Internet has started to change communication and workflow processes through almost every industrial and service sector. With the ability of transmitting data to every location in the world within seconds, it is possible to establish new forms of collaboration, where the availability of information is no more limited to the places where the information was gathered. But the past years have also shown, that it is not enough to be technically in the position of accessing information remotely. There is a strong need to define, implement and improve communication protocols, coding systems, terminology and concepts to keep the quality of information that is shared in a network.

In 1996 the basic research and development department of Siemens Medical Engineering started to work in the area of *telematics*, a new field of work, born to achieve synergies from the rapidly developing communication and information technologies. The project named *MedStage* was initiated to research and examine different technologies and strategies to provide a telecommunication platform designed for the special needs of healthcare. In contrast to existing healthcare application systems, that are often designed for only one group of care providers, MedStage is intended primarily to be a platform for all participants within care processes. The main requirements were

- creating an open platform based on commonly available Internet technologies,
- being usable for all care providers (hospitals, GPs, specialist, pharmacies, mobile home care services) and patients,
- considering existing standards for import, export and storage of medical data,
- fulfilling the strong demands for security, confidentiality and data privacy,
- being able to offer the functionality as a service provider with additional conditions to ensure proper ownership of the stored data.

2. History of MedStage

The project was started as a set of experimental solutions using different information and communication technologies in the new areas of telemedical applications [1]:

- Teleconsultation (Telereporting, Second-opinion) and Telescreening
- Telemonitoring
- Electronic Referral Support
- Patient Data Repository

Beside research and development, the MedStage team was always trying to find partners for implementing pilot projects in different medical areas. So the application models and the corresponding software was proven stepwise in existing environments.

2.1 Screening for Diabetic Retinopathy and Glaucoma

The first pilot project, a telescreening application, was initiated 1998 together with the department of ophthalmology of the University of Erlangen-Nürnberg. The goal was to show how telecommunication can be easily used for early diagnosis of eye diseases. A GP uses a special camera to generate images of the eye background and sends them to the MedStage server via Internet using HTTP upload. The specialists in the ophthalmology department retrieve the images from special mailboxes, evaluates them, prepares *multimedia diagnosis reports*, and return these reports to the GP. The used multimedia reporting tool, also used in the SIENET PACS product line of Siemens, was developed as an *asynchronous electronic whiteboard*, that allows the reporting physician to add text-, drawing- and voice-annotations onto raster images or video sequences using the recorder component of the tool. The ordering physician uses the playback component to view the diagnosis and treatment proposals. The software itself is available as a browser plugin or a Java Bean component.

2.2. Home-Monitoring for Glaucoma

In May 1998, a first home-monitoring project, called "*Telematic Self-Tonometry*", was established in cooperation with the department of ophthalmology of the University of Erlangen-Nürnberg. The patients participating in this project all suffer from glaucoma, and using a portable measurement device, they test their intraocular pressure several times a day at home. The patients record the results using a special user interface for a PalmPilot. The PalmPilot is transmitting the data automatically after connecting it to a modem. As a more simple alternative the patients can use a touch-tone telephone with the telephone number of a *software-based call center* where they receive voice instructions for entering their data with the telephone keyboard. The controlling ophthalmologist is able to access this data at any time using a standard web browser. The results are prepared using a Java chart applet, where different viewing options may be set. The second generation of the home-monitoring application will be available this year with additional features of configurable alerts, deputy rules and a broader range of transmission channels, e.g. FAX, E-Mail, SMS and WAP.

2.3 Used technology

The described teleconsultation/telescreening and home-monitoring framework is based on nowadays wide-spread technologies: HTTPS communication with SSL encryption, HTML pages, JavaScript or Java applets at client side and server technologies like CGI, ASP, JSP or Java Servlets together with application-centric storage of the information in file systems or relational database tables. The first generation of this framework had to be used with limitations concerning data privacy. All data stored at the MedStage server was unencrypted, but pseudonymized. The information about the concerned patient was known only by the physician, who has entered the data, so he was able to maintain his duty for confidentiality.

3. MedStage 2nd generation

With the experience from the pilot projects and a lot of discussions with different participants, the MedStage team started to design and develop a second software generation. The ideas for the new generation where driven by both new application requirements and new available technologies. The main goal for the new generation was to provide a universal *telemedical service center* for a larger application area, where

- the mapping of patients and pseudonyms cannot be handled manually,
- the potential receiver of the medical data may not be known at the time, when the data is entered, e.g. due to free choice of a specialist by the patient in a referral process or due to emergency cases,
- the user groups will be enabled to define their own authorization policies, security levels and workflow processes.

3.1 Security

The following security requirements are considered to be essential:

- *Encrypted transmission* of all client server communication (SSL/TLS).
- *Logging* of all access to the system (audit trail).
- User *authentication* based on strong cryptography (SSL/TLS with client authentication based on certificates including revocation lists).
- Configurable role-based *authorization.*
- *Non-changeable data storage* – entered data cannot be deleted or overwritten. If changes are necessary a built-in version management has to create new versions.
- *Non-repudiation* of entered data – for every data item added to the repository the data itself or a textual representation of the performed operation may be digitally signed.
- Data *encryption* of all person-identifying data using hybrid encryption (symmetric encryption of data with asymmetric encryption of the symmetric key) at client side.

To achieve these goals a Public-Key-Infrastructure (PKI) is part of the new architecture. All users receive two asymmetric key pairs (one for data encryption and one for digital signature) either using floppy discs or smart cards. The user management is performed using the *registration authority* interface of the PKI. Different policies for key lifetime or automatic key update may be set. All public keys are stored within a directory service (LDAP). Compromised certificates can be locked and *certificate revocation lists* are published on the LDAP server. As mentioned above all person-identifying data is encrypted within the data repository. To access patient lists, a separate patient index based on the CORBAmed *Person Identification Service (PIDS)* [2] is used, where patient identifying data (name, birthday, address, security number) is stored together with an encrypted identifier for the root medical record in the data repository.

3.2 Healthcare data repository

To be able to provide a storage framework for the very different telemedical applications it was decided to implement a generic *Healthcare Data Repository (HDR)* based on the data model of the *"Electronic HealthCare Record Architecture" (EHCRA)* [3] of CEN TC 251, see Fig. 1. All medical data is structured into folders, link items and medical data items. Every component within the model is versioned, each version object holds information about the creator, a start time, when the version was added, a digital signature of a pseudo-text describing the operation in which the version was added and an optional end time, when the version became invalid.

For the hierarchical structuring currently only the *Folder Original Component Complex* of EHCRA is used. The folder item mainly consists of a code to specify the type of the folder, a symbolic name, a display name, an access control list and the link to the parent folder. Link items are used to provide additional relationships between folders and data items. A link holds the information about the source and target object, a role, specifying the relationship of the target object to the source object, e.g. "*related-to*", "*evidence for*", a display name and an access control list. The medical data item base class consists of a code to specify the kind of the data item, e.g. "*ct-scan.liver*", "*xray.chest*", a type to specify the presentation component, e.g. *image/jpeg*, an identification of the subject of care, e.g. a *patient id*, a display name and an access control list. Data items can be reached either using vertical navigation through the folder structure, following links or direct horizontal queries on data items, e.g. "*find all ECG results of patient 4711 of the last 6 month*".

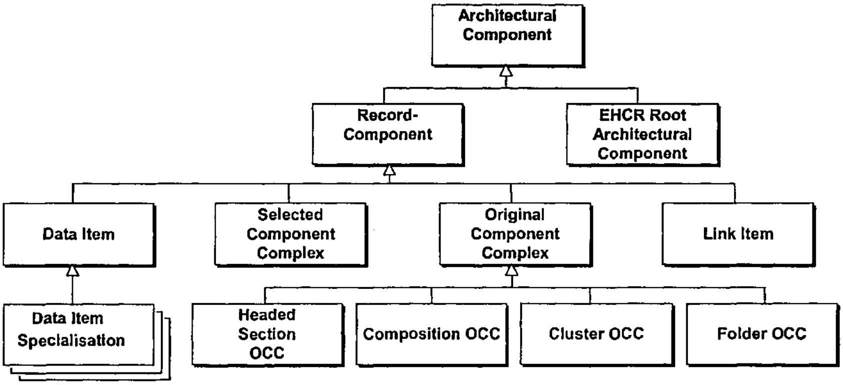

Fig. 1. Data model of EHCRA.

For the information stored within the data items, there are several predefined data item specializations, that hold the different data:

- lists of key value pairs,
- references to multi media files stored as BLOBs (*binary large objects)*,
- references to one or more records in a flat database table within the HDR,
- references to structured data using parsed or unparsed XML,
- references to external medical objects.

Beside the digitally signed pseudo-text within each version object, there can be also a law conformant digital signature on the data item's information itself, e.g. a digital signature on a referral letter stored as a BLOB.

3.3 System architecture

The frameworks of the new MedStage system are designed using object-oriented modelling and implemented using the latest versions of Sun's Java Development Kits on both client and server side. The primary focus is not to build another monolithic electronic patient record, but an open architecture of frameworks and modules, that are attached using platform-independent and language-neutral CORBA and HTTP communication channels together with the rapidly growing XML technologies for data exchange. Additionally the architecture tries to simplify the management of the different security modules by using a professional PKI solution as the central unit for all necessary security administration purposes.

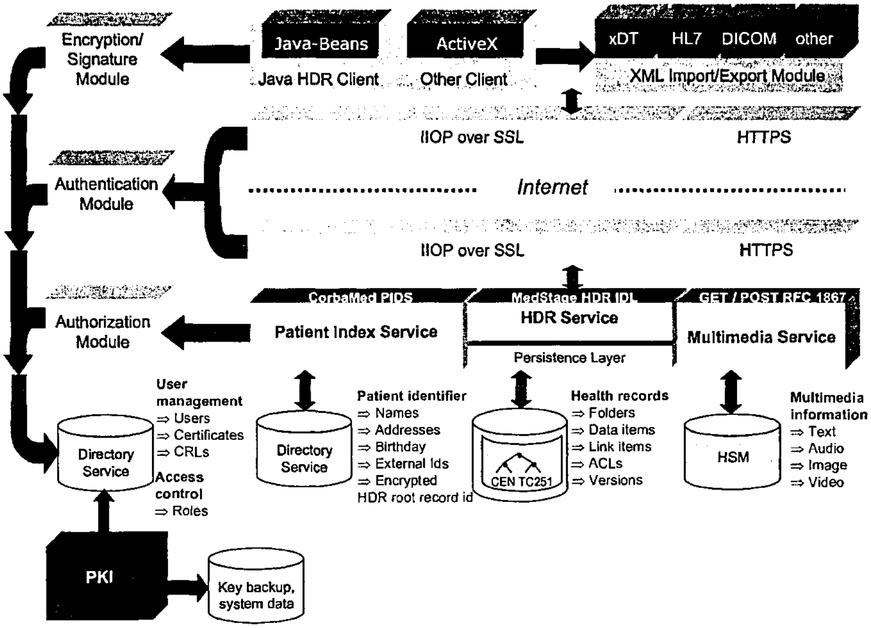

Fig. 2. System architecture.

In cases, where open medical standards, like CORBAmed PIDS exist, we use these standards whenever possible. Future versions of the HDR will also integrate the new standardisation efforts of HL7 PRA (Patient Record Architecture), DICOM Working Group 8 (Structured Reporting) and CORBAmed COAS (Clinical Observation Access Service), CIAS (Clinical Image Access Service) and HRAC (Healthcare Resource Access Control).

References

[1] "Telematik im Gesundheitswesen Perspektiven der Telemedizin in Deutschland für Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie und Bundesministerium für Gesundheit, München, August 1997", Roland Berger & Partner GmbH International Management Consultants, München

[2] "Patient Identification Service", CORBAmed, htp://www.omg.org/cgi-bin/doc?formal/99-03-05

[3] "prENV 13606-1: Health informatics - Electronic healthcare record communication - Part 1-4", CEN TC251, http://www.centc251.org/ TCMeet/Doclist/TCdoc99/N99-0{40|41|43|43}.pdf