Research Paper ■

Concepts for Integrated Electronic Health Records Management System

Miroslav Končar, Sven Lončarić

Abstract. Due to a very sensitive nature of medical information, Electronic health records (EHCR) management systems are faced with a number of stringent requirements. More precisely, security problem that affects all the levels of communication architecture as well as all the medico/legal and ethical issues has been recognized as the primary step towards integrated health computing environment. This paper presents the solution for a functional EHCR management system that meets these strict requirements, but also follows the initiative taken by the Next Generation Network (NGN) approach, that addresses the problems of modularity and flexibility of medical information systems.

■ **Infor Med Slov** 2003; 8(1): 27-37

Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia.

Contact Person: Miroslav Končar, Badalićeva 26, 10000 Zagreb, Croatia, email: miroslav_koncar@hotmail.com.

Introduction

Supported by the advances achieved in the computer science, communication technologies and especially by the growth of the Internet, medical information systems are becoming more and more present in physicians' practice. Telemedicine as the next step in medical care evolution has become possible in every aspect of its' essence. Distance in no longer a factor, and it is feasible to provide every person with high quality health care, independent of their current location.

However, when studying the requirements for medical information systems, the picture is somewhat different. Despite the fact that information systems used for different medical aspects raise diverse set of requirements and are evaluated by various performance factors, there are some basic issues that characterize practically every information and communication system used in medicine:

- Electronic health record (EHCR) management – every medical information system has to have either its' own implementation or a functional interface to the EHCR management.
- Security and data confidentiality – the system has to ensure that every piece of information is transferred, stored and retrieved in a secure way. This includes procedures like access control and the obligatory authorization at all levels in the health computing environment. Additionally, but not less important, the system has to respect patient's legal right to privacy, and ethical and legal policies required by the national regulations.
- Open system architecture – integration of different levels of medical care that would overcome today's boundaries is one common final goal set for medical information systems.

Security issues in medical information systems and EHCR management represent the starting point in the system design. Encryption of the communication channels, identification and authorization of users etc, solve just part of the problem. Confidentiality and privacy issues, legal, ethical and moral aspects of patients' personal and medical data as well as the integrity and professionalism of physicians' practice has to be preserved and supported by the medical information system management. EHCR management system is not just a computer science, and many other human disciplines take part in defining system requirements.

This paper describes the EHCR management system that successfully addresses all the issues mentioned above, and follows the ideas summarized in Next Generation Networks (NGN). Original software solution that supports the framework is also presented.

It is organized as follows: In Methods section basic set of requirements for the logical schema of the EHCR is presented; status and characteristics of information systems currently deployed for various medical purposes are discussed; communication architecture principles of the developed EHCR management system are introduced; the most important open R&D middleware issues are addressed; and details of the experimental laboratory implementation of EHCR management system are described. In Results section the performance results of developed encryption/decryption module are presented. Conclusion gives some final remarks as well as our plans and ideas for future development.

Methods

Open development issues for EHCR architecture and management systems

Health information systems today suffer from a number of significant problems.[1] Challenges that need to be met by the systems of tomorrow include:

- support for a life-long health record
- interoperability among all the parties and systems used in patient care
- intelligent decision support
- domain size and rate of change
- systems obsolescence
- multi-contact healthcare system and mobile patients
- multiple medical cultures
- support for domain experts to have direct control over the information design and change management of their systems

Current work in health standards, notably by HL7, CEN, ISO and the OMG attempts to address some of these problems, as does implementation-based work including a number of policies-funded efforts around the globe. Very first efforts of EHCR architecture evolution were compromised by a number of factors that strongly influence the functionality and performance of the developed systems. Most of the organizations today agree on the basic concept, which is to separate context from the content even if the data is brought out of its original context,[2,3] in order to cope with a huge diversity between data recorded in the different departments of medical care. A clear context/content separation provides the users with medical data transfer without any loss of information by straightforward extract of the parts of patients' EHCR.

One of the cornerstones of the functional EHCR system is the security and confidentiality of patients' medical data. In the soul definition of EHCR it is stated, "the record is under control of the consumer and is stored and transmitted in the secure way",[4] which includes patients' ethical and legal rights to privacy and data confidentiality. Security includes obligatory authorization at all levels of the system, as well as the secure transfer of information between the end points of communication. Furthermore, the developers are advised to implement access-logging routines, which store all the transactions and data flows and are retrieved for auditing and legal purposes only.[5]

When considering the construction or review of good health information standards, insufficient attention was typically paid to the consequences for software construction and runtime systems. Many of the mayor problems of the past for information-intensive systems, including most EHCR and related systems, have to do with the inability to deal with change. This has led to an important turning point in the architecture design, which than significantly influences the development of the EHCR management systems. The EHCR specifications recommended by the standardization bodies are primarily focused on the logical health record architecture, i.e. the developers are provided with the formal model of the framework and generic features of the EHCR and there is no restriction regarding data formats in which the record are stored. More precisely, it is up to system architects decision to develop optimal EHCR management system that would suite their needs and requirements.

Today there are number of associations and standardization bodies that have organized task forces for developing EHCR architecture standards, some of which that were already mentioned above. In our case CEN standards and recommendations[6] have been the referral point when developing the EHCR management system. ENV 13606 recommendations with the title "Electronic Healthcare Record Communication" provide the principles, structures, terms, rules and formats for open and safe communication of EHCRs. Since management system framework and logical structure of health records are two separate problems, and although our focus was not on the CEN recommendations them self, we have respected the specifications and the developed system offers a straightforward implementation of the ENV 13606 standard.

Communication platform for EHCR management system

The communication architectures and software solutions for medical information systems depend on number of parameters, such as the vendor of the hardware and software, requirements specification set for the particular example, the complexity of the services, type of processed information etc. Advanced, large-scale telemedicine applications are usually very performance sensitive, which could influence the developers decision for specific hardware solutions and programming techniques. As the result of these facts, at present most clinical software systems are “closed” with little or no interoperability between them.[7] Similar problem arise with the communication infrastructure solutions, which tend to be quite diverse. There are number of examples of teleconsultation or telesurgery systems that are based on communication protocols like ISDN or ATM.[8,9] Although these communication architectures fully satisfy their performance requirements, the services provided by the system are usually not transparent to the user, in sense that without specific equipment one is unable to use the application. In that case the application is not portable and cannot be used in other medical institutions without additional investments.

Integrated EHCR management systems should be able to manage patient information originating from various sources, and that is accessible independent of the users’ current position and terminal. In that sense we have followed the guidelines of the communication networks convergence summarized in the NGN framework. The basic approach taken for NGN is one common network platform for transferring and serving different types of information, services and media. In this way it is intended to handle different media types and to use different services at the same time, with possible selection of well-defined Quality of Service (QoS) parameters. Today’s concept of separate fixed and mobile network needs to be changed; it is assumed that a user is mobile within the system, and should be able to use all the provided services in a personalized and user-friendly way. The services developed for NGN tend to be inherently transparent, by which they assume IP based transfer protocol and are independent of a user’s current position and terminal. As the result of this approach, the developed EHCR management system framework adopts multi-tier communication architecture with IP-based transfer and middleware layer that is able to satisfy the requirements of the NGN ideology, and the user does not require any special network equipment to access the medical data repository.

EHCR management system framework

Development of EHCR management system is based on distributed network architecture and CORBA[10] communication platform. The two dimensional view of the system architecture is shown in Figure 1. There are a number of advantages offered by the CORBA platform, which are of great importance to the application developers. In a distributed computing environment (DCE), where all system components are introduced as objects, CORBA provides a standard mechanism and tools for definition and implementation of the interfaces between objects. Communication between the components is accomplished using object references in such manner that the strict client/server distinction no longer exists. Also, by taking advantage of the common distributed object computing (DOC) communication platforms, we are provided with very important features such as complete platform and language independence, error handling, memory management etc.

Multi-tier communication architecture based on CORBA middleware platform is highly flexible and modular. Introduction of new features and addition of new object or modules usually does not require changes in the system in general, which is very important in case of integration with other medical information systems. Since middleware communication layer contains most of the logic, potential upgrades of the system do not include changes and delivery of new client-side modules. The problems like diversity of data and media, localization based services and personalized delivery of information are addressed by classical middleware components in this communication model and comply with the concept of NGN architecture.

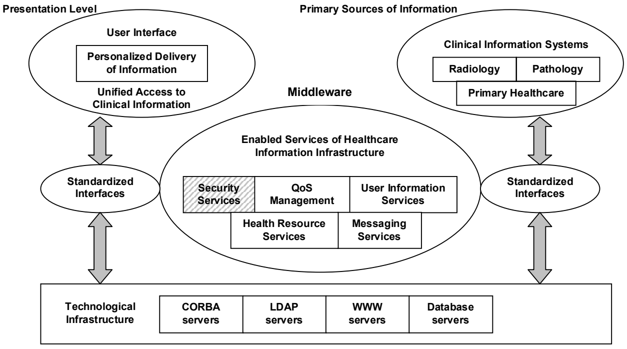

Figure 1 Multi-tier communication architectural framework for EHCR management system

In respect to sensitivity of medical information, close consideration has to be paid to the security framework offered by the CORBA platform. Implemented in the form of the CORBAservices, OMG among other things provides additional capabilities for security routines. This framework includes features like identification and authentication of users, authorization and access control, auditing, secure communication, non-repudiation and administration of various security policies. Undoubtedly, these functionalities are of great importance to performance sensitive applications such as EHCR management. However, they do not offer a complete solution in our case. Services provided by the standard DOC platforms cannot fully satisfy the legal and ethical rights of the patient and his/her medical data, and some additional measures have to be taken in order to meet those requirements.

In connection to middleware layer shown in Figure 1, framework for NGN communication architecture also includes some common functions such as registration, profile management, usage recording etc, which are also not CORBA's core functionalities. Those modules can be separated based on their orientation towards network transport layer or service layer, and together comprise a fully functional communication system for NGN architecture. Research in this area has been a subject of separate efforts conducted in our laboratory.[11]

Open R&D issues of standard DOC communication platforms

Employment of CORBA middleware communication architecture in medical information systems provides the application developers with number of advantages, especially in reference to classical client/server communication architectures. However, it still does not provide a complete solution for large-scale distributed applications. There are still some very important open R&D issues that are the subject of research in many laboratories and interest groups around the globe, two of which are of high importance for medical systems.

Communication overhead – traditionally, performance results of communication between CORBA objects and the application based on the ORB core were inferior to time requirements for client/server communication in two-tier network architecture.[12,13] Caused by the substantial progress in the standard middleware platforms, the performance results have significantly improved over the last couple of years,[14] however they still do not outperform classical client/server applications.

QoS management – first-generation DOC middleware was not targeted for performance sensitive applications with stringent QoS requirements. Not surprisingly, its efficiency, predictability, scalability and dependability was problematic. Over the last couple of years, however, the use of CORBA-based DOC middleware has increased significantly in high performance distributed systems with real-time QoS requirements. Advancements of CORBA architecture model include Massaging[15] and Real-time[16] specifications that provide the control of many end-to-end ORB QoS policies such as timeouts or priority queuing, and implement standard interfaces for managing ORB processing, communication and memory resources. As a result, some of the focus of overhead, non-determinism, and priority inversion problems has shifted to the commercial operating systems and networks, which are once again responsible for the majority of end-to-end latency and jitter.[17] However, in respect to quality solutions introduced by these specifications, there are additional requirements set for QoS management framework like dynamic resource management, portable network QoS APIs, and multiple QoS property, which together comprise guidelines for future research and development efforts.

Beside common QoS parameters like predictable latency and jitter control it is important to keep in mind that the term QoS also includes a wide range of system properties like scalability, security and dependability. Common middleware solutions still do not provide a complete solution for those issues, and the improvements in this area has been the subject of work for number of research teams around the world, some of which have achieved high level of performance and usability.[18,19]

EHCR management system design

Following the principles and the requirements summarized in the previous sections, we have designed an experimental laboratory EHCR management system based on the communication architecture framework shown in Figure 1. The focus of attention has been paid to the middleware services that are targeted to satisfy very strict demands set for EHCR system implementation. Figure 2 depicts the laboratory system schema.

The module that requires special developers attention is preserving security of patients' personal and medical data. Like stated before, one of the basic requirements for EHCR management system is to ensure privacy, medico-legal and ethical needs of all persons known to the system.[7] The basic principle used in medicine is that the access to patient's information is granted to a very limited group of people, which posses the legal right to retrieve and edit patient's data.[20] In most of the cases that means that only general practitioner (GP) chosen by the patient is allowed to edit the medical record of the particular patient. In every other case the medical staff, other GPs or specialists have to acquire explicit patient's permit to access his/her information. Also, it is a common practice that all the data used for scientific research has to be used anonymously, except when the process itself requires personal information. Again, in that case the project has to acquire the permit of the subjects used in the study.[21]

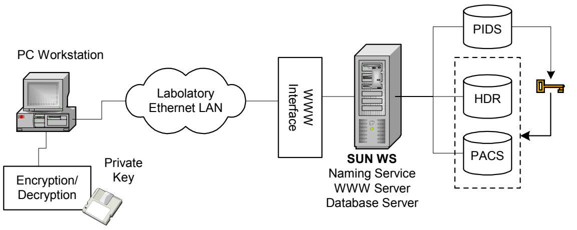

Figure 2 Laboratory System Infrastructure

Third part of the ENV 13606 recommendations called "Distribution Rules" addresses the problems of legal rights to view, edit and transfer a part of or a complete patient's medical record.[5] By adopting these proposals it is possible to define very detailed conditions when an access to patients' data can be granted, and what operations are permitted for different cases. Again, this represents only a mechanism to implement access rules at the data level, defined by the local users and national guidelines, and does not address logical and semantic security problems.

The solution implemented here provides the developers with the possibility to adopt all these specifications, but also introduces additional security measures against possible illegal and unauthorized access to the data repository. The basic concept of the EHCR management system is strict separation of patient's personal and medical data.[22] More precisely, the EHCR system consists of two completely separated databases: Person Identification Service (PIDS), which contains personal and demographic information, and Healthcare Database Repository (HDR), which contains medical data only (Figure 3). The connection between those two databases is achieved through Master Patient Index (MPI), which is stored in the PIDS database in encrypted form, opposite to HDR where it is kept as plain text. The encryption and decryption processes are following the concepts of the asymmetric cryptography,[23] in which one key, called "public" is used for data encryption and the other, called "private" for decryption process. When a new account for a physician is opened in the system, the administrator creates at least two pairs of key (one pair for encryption and decryption of data, and the other for digital signatures), and digitally signs them. Public keys are added to the public keyring and published on the key server that in general could use LDAP service to manage public keys, but this is not mandatory . Private keys are transferred on floppy discs or CD-ROMs that also have a copy of the fingerprint of the administrators' signing key. These portable discs act as smart cards, without which one is theoretically unable to use the service. When encrypting data, every key first has to be checked for the administrator's signature. If the fingerprint on the physician's public key matches the one on the floppy disc, key is used. Otherwise, the key is treated as untrustworthy, revocation certificate is published on the key server, and the key is no longer used.

The administration of the patients goes as follows: when the patient is introduced to the system for the first time, his/her personal information including MPI is entered in the PIDS database. At the same time the patient chouses the GP, and the administrator selects corresponding public key for the first entry in the HDR database. Moreover, if the patient wants to enable more than one physician with the access rights to his/her medical information, theoretically there is no limit of public keys that can be used in encryption process. Also, if the patient during lifetime changes the GP, which usually happens a couple of times, the soul procedure that needs to take place is to replace the old encrypted MPI in the PIDS database with the new one. In this sense the EHCR framework completely follows and fully meets the demand that the consumer, in this case the patient, is the legal owner of the health record content.[1] In combination with the selected physician's public key the encryption process automatically also uses Master public key. The purpose of this key is a "safety net mechanism", which is used in special situations like the loss of a private key, i.e. when there is no other way to decouple the connection between PIDS and HDR archives. Since Master private key is able to unlock all the records, the size of these keys should be much bigger than standard key size and therefore harder to break. It is also very important that the private key of the pair is kept in a high security location like a safe .

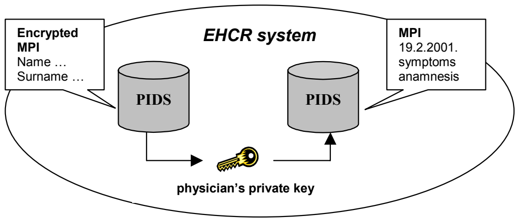

Figure 3 Configuration and logical architecture of EHCR system

With this model we have accomplished some very important features. First, because of the fact that all the relevant data is stored as plain text within both modules, PIDS module can serve as the primary interface to all the other modules defined on the system. It can be opened for access not only to physicians, but also to other groups of users like nurses, hospital administration staff etc. Furthermore, by storing medical data as plain text in the HDR data repository, this archive can easily be used for education or research purposes. The logical structure of the HDR database system is not limited by any means and can adopt specifications proposed in ENV 13606 document, including the distribution rules that comply with the generic standard.

Developed security module resides on client side of the application (Figure 2). This partially steps out of the classical middleware networks framework, where the clients don't require special additions in order to be able to use the service. It is insecure to encrypt data on the server side, since the automation takes away all the control about the keys that are used in the process. Possible intruder could compromise some of the keys in such way that the server logic is unable to locate the problem. If the encryption is connected to the client side, the client has the ability to autonomously check every public key that is used in the process. Comparing the fingerprints of the public key used in the current process and the value stored on the floppy disc, the user is certain whether the public key is trustworthy or not. Decryption is even more insecure if it would be placed on the server side. In such case the server would need to have some kind of an access to physicians' private keys, which is inherently a security leak.

EHCR management system is based on CORBA's middleware architecture, which is responsible for object localization, naming service and communication between server and client components. By default clients access the application through their WWW browsers, i.e. using HTTP or HTTP/SSL communication protocols (Figure 2). System that adopts this type of communication architecture is straightforward and can be mapped to a wide variety of network access, which makes the application transparent to the details and characteristics of the client terminals. Especially if the system is being accessed from within the hospital LAN, clients can theoretically use raw CORBA's IIOP communication protocol, but its' efficiency from the performance point of view is rather questionable.

Finally, the question that is quite expected is how secure actually are we? Unfortunately, the answer to this problem is not completely unambiguous. Implementing CORBA security services and additionally employing SSL communication protocol, all the information is transferred in the encrypted form and therefore hidden from eavesdroppers. Local hospital networks are usually protected by the firewalls, and even if an attacker breaks into the system, without the possession of the private keys he is unable to compromise the medical data repository. Regular database backups as well as the use of digital signatures for data integrity check would easily diagnose possible misuse of the system. The last potential security gap are the keys used in the encryption/decryption process. In the recent years there has been a lot of discussion and research in this area that tried to find the answer to what level of security Public Key Infrastructure (PKI) offers. The results of empirical studies have shown that PKI can provide extremely high level of security. The size of used keys directly influence the complexity of the possible break. Private keys use additional security measures in such way that they are kept in the encrypted form on the floppy discs and protected by the passfrase. Bottom line, the consensus of developers and researchers is that this type of security infrastructure is more profound, sophisticated and qualitative than the standard measures used in paper health record management.

Results

Laboratory prototype performance results

To support the system architecture illustrated in Figure 2, we have built a laboratory prototype of the encryption/decryption module. Also, in order to simulate a real situation environment, we have designed an interface to the image management system that was developed during our previous work,[24] which among other characteristics featured a diagnostic images database repository. These images complied with the DICOMv3 standard and were taken using different image modalities. Prior to the integration the system needed some changes, because its' data archive contained parts of patients personal information. That information was directly deleted from the database, and replaced with the newly created MPIs.

Details of laboratory devices, servers and terminals are as follows:

- Client terminal is a PC with a Pentium II processor and 256 MB RAM, and private keys are stored on floppy discs.
- WWW, CORBA and database servers are implemented on a single SUN Ultra 5 WS running on 400MHz RISC processor and 256 MB RAM.
- LAN is based on Ethernet 100BaseT technology.
- Asymmetric and symmetric keys used in encryption and decryption process are 1024 and 128 bits of size respectively.
- CORBA and database modules were implemented using Java™ Programming Language.

The encryption/decryption module is fully implemented using C/C++ Programming Languages. Encryption algorithms were provided by the GnuPG[25] application, and using provided APIs and Java Native Interface we have programmed a Dynamic Loadable Library (DLL) that interfaces Java GUI in WWW browser and controls the use of GnuPG application (Figure 4). Dynamic library also performs various security routines such as validation of the public/private keys and integrity check of the GnuPG application and Java Security File.

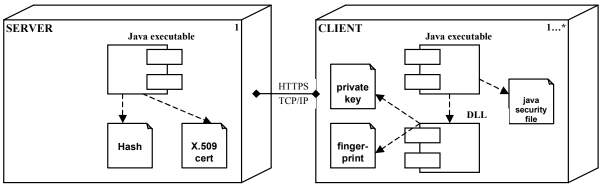

Figure 4 UML Component/deployment diagram of application modules

In order to gain a prospective about the performance characteristics we have conducted some basic measurements of time needed for different processes. The idea behind this work is to find out which module or process is most time consuming and in future could cause bad performance results. Our hypothesis was the encryption/decryption module could be rather sensitive procedures, since both processes need to access data stored on the floppy disc. Table 1 illustrates the measurements results.

Table 1 Security module performance results

Procedure	Time interval (sec)
1 thread ORB context initialisation	0.317
100 thread ORB context initialisation	2.173
Decryption	0.091
Encryption	0.364
US image retrieval	1.624
MRI image retrieval	1.861
CT image retrieval	2.381

ORB initialisation threads are used to simulate more than one connection at the same time, which is usually the case in a real situation. Second column depicts average time for 20 iterations.

Time needed to initialise the context or to retrieve and transfer images is highly dependant about the network conditions and number of clients accessing the service, whereas that does not influence the neither encryption nor decryption, since those are client-side processes. Image retrieval was measured from the time the user sent a request for an image and until that image appeared on the screen. Every image before being sent to client terminal must be additionally processed, since common WWW browsers like Netscape Communicator or Internet Explorer do not support DICOM image format. In this particular case images were formatted to PNG (Portable Network Graphics) format, which is supported by all of the standard browsers. Furthermore, at this point the laboratory prototype supports rendering only one image at the time, and therefore no image compression was used.

The comparison of the results shows that our assumption the encryption/decryption of patient IDs will strongly influence the time performance of the system was not confirmed. The use of GnuPG's implementation of crypto algorithms and DLL control has shown no disadvantages apart from being platform dependant. It is especially useful because the control of modules is distributed, i.e. Java module controls DLL and GnuPG and vice versa. This makes the application robust, since possible attacker would need to compromise both modules in order to do the damage. Table 1 also illustrates the complexity of QoS problem for image transfer. Namely, studies within imaging departments have shown that clinicians find it acceptable for studies to appear at workstations within 2 seconds of the images being requested,[26] which in our case the results for CT image retrieval do not satisfy this boundary.

Conclusion

Medical information systems require an increasingly broad range of features, which impose number of research questions on the computer and telecommunication scientists. Large-scale integrated EHCR systems are faced with many very strict requirements such as security and privacy, sensitivity and diversity of data and media types that need to be processed, support of various QoS aspects etc. Our goal was to make the EHCR management system secure from the unauthorized access from both outside and inside local hospital network, and at the same time to meet the demand of legal patients' ownership of their own medical data. The EHCR management system presented here successfully copes with the requirements and provides the developers with key performance factors such as flexibility, modularity and scalability. It also solves the necessity of controlling very strict access rights to patients' medical data, and fully respects the recommendations and proposals of CEN standardization body.

Our plans for further development include the design and research of the system modules according to the framework shown in Figure 1. We are planning to further investigate the performance issues of IIOP opposite HTTP/SSL communication protocol stack, based also on the results of some other research teams that show clear advantage of server-based applications and latter type of access. Parallel to that another research team in our laboratory is working on communication architecture for NGN. We are especially interested in the standard and healthcare specific middleware components, which would introduce important new features like personalization, profile management, terminology services etc. All of these address different issues of the QoS properties, which is of paramount importance to EHCR management system.

References

1. T. Beale, “Health Information Standards Manifesto”, rev 2.5, 2001.
2. Torleif Olhede, PhL: “Archiving of Care Related Information in XML-format“, Proceedings of MIE2000, pp. 1146-1150, Hannover, Germany.
3. F.H. Roger France, Cl. Beguin, R. van Breugel, et.al. “Long Term Preservation of Electronic Health Records. Recommendations in a large teaching hospital in Belgium“, Proceedings of MIE2000, pp. 1146-1150, Hannover, Germany.
4. National Health Records Task Force, Australia, “The Health Information Network for Australia”, 2000.
5. CEN/TC 251 Health Informatics, ENV 13606-3:1999, “Health Informatics – Electronic healthcare record communication – Part 3: Distribution Rules”.
6. European Standards in Health Informatics official URL: http://www.centc251.org.
7. P. Schloeffel, T. Beale, S. Heard, et.al. “Background and overview of the Good Electronic Health Record”, openEHCR Fundation, 2001.
8. I. Klapan et.al. “Our Tele-3D C-FESS remote surgical procedures: real time transfer of live video image in parallel with volume rendered models of surgical field”, SoftCom 2001 proceedings, pp. 967-979, 2001.
9. Irfan Pyarali, Timothy H. Harrison, Douglas C. Schmidt: "Design and Performance of an Object-

Oriented Framework for High-Speed Electronic Medical Imaging", Computing Systems Journal, USENIX, Vol. 9, No. 3.

10. Jeremy Rosenberger: “Teach Yourself CORBA In 14 Days“, SAMS Publishing, Macmillan Computer Publishing.
11. "Mobile Multimedia Portal – Role In UMTS Services", D. Šimić et.al. SoftCom2001 proceedings, Vol. II, pp. 529-535.
12. A. Gokhale and D. C. Schmidt, “Measuring the Performance of Communication Middleware on High-Speed Networks,” SIGCOMM’96 proceedings, (Stanford, CA), ACM, 1996.
13. A. Gokhale and D. C. Schmidt, “Performance of the CORBA Dynamic Invocation Interface and Internet Inter-ORB Protocol over High-Speed ATM Networks,” GLOBECOM’96, (London, England), IEEE, 1996.
14. G. Coulson, S. Baichoo, “Implementing the CORBA GIOP in a High-Performance Object Request Broker Environment”, ACM Distributed Computing Journal, vol. 14, 2001.
15. CORBA Messaging Specification, OMG Document orbos/98-05-05 ed., 1998.
16. Realtime CORBA Joint Revised Submission, OMG Document orbos/99-02-12 ed., 1999.
17. D.C. Schmidt, M. Deshpande, C. O’Ryan, “Operating System Performance in support of Real-time Middleware”, in Proceedings of WORDS’02, San Diego, 2002.
18. Yamuna Krishnamurthy, Vishal Kachroo, David A. Karr, et.al. "Integration of QoS-enabled Distributed Object Computing Middleware for Developing Next-generation Distributed Applications", ACM SIGPLAN Workshop on Optimization of Middleware and Distributed Systems (OM 2001), Snowbird, Utah, 2001.
19. D.C. Schmidt, D.L. Levine, S. Mungee, “The Design and Performance of Real-Time Object Request Brokers”, Computer Communications, vol. 21, pp. 294-324, 1998.
20. Reglementation applicable aux banques de donnes medicales automatisees, Recommandation No. R(81)1 adopte par le Comite des Ministres du Conseil de l'Europe, Strasbourg, 1981.
21. Recommendation on the Protection of Medical Data R(96) of the Council of Europe, Strasbourg 1996.
22. Hans Schuell, Volker Schmidt: “MedStage – Platform for Information and Communication In Healthcare“, Proceedings of MIE2000, pp. 1101-1106, Hannover, Germany, 2000.
23. Phil Zimmerman: "Introduction to Cryptography", copyright© 1990-1999 by Network Associates, Inc.
24. M. Končar and S. Lončarić: "WWW-based image management system", MIE2000, Hannover, Germany, 2000.
25. Gnu Privacy Guard Official WWW Site, http://www.gnupg.org.
26. CEN/TC 251 Health Informatics, “Quality of service requirements for health information interchange”, Technical Report, 2002.