Case Study: Using Digital Signatures for the Archival of Medical Records in Hospitals

Sebastian Sageder[1], Johannes Sametinger[2], Andreas Wiesauer[3]
Johannes Kepler University Linz
Dept. of Business Informatics – Software Engineering
http://www.se.jku.at
[1] sebastian.sageder@gmx.at, [2]johannes.sametinger@jku.at, [3]andreas.wiesauer@jku.at

Abstract

Even in medium-sized hospitals, thousands of medical records are created every day. These documents have to be archived over many years. This is important for having access to information for later treatments of patients and for potential legal disputes. The latter makes signing of medical records important. The process of getting rid of paper in hospitals is quite challenging for many reasons. Using digital signatures is definitely one of these challenges. This article will report on this process and on experiences made in an Austrian medium-sized hospital.

1 Introduction

Most IT investments in healthcare have been driven by payment issues rather than by clinical needs [1]. Healthcare has invested at least 50% less of its gross revenues in IT than other information-intensive industries. Banking, for example, has international standards for the exchange of data. This is still unthinkable in healthcare. In many industries excellent information technology is a competitive edge. This is not yet true for healthcare.

An Austrian Communities Hospital, in short AKh, is a medium-sized hospital that is operated by the city where the hospital is located. It has about 2,500 employees; about 360 of them are medical doctors. The hospital is able to medicate about 1,000 patients at a time. For each patient, a number of medical records have to be created. These records contain information about patients' diseases, their treatments, their medication and therapies. They are signed by medical doctors to confirm their validity. And, for legal reasons, they get archived for up to 30 years. Archived documents are typically used for later treatments of patients and for any legal disputes. In this hospital, an average of over 6,000 medical records is being created every day.

The process of creating, maintaining, signing, archiving and retrieving the records is time-consuming for all involved parties (medical doctors, nursing staff and administration) and therefore accounts for high costs. Medical records are created by doctors in most cases. Once, the creation process is complete, the doctor and maybe other persons, e.g., the supervisor, check and sign the record. After the signing process, medical records are at first archived at the department where they have been created. After a few weeks, they get transferred to the department's archive. After three years, the records reach their final destination, the optical archive system (OAS). For the OAS, records are scanned and stored as tiff documents. The paper documents are not available any longer from that time on. Retrieving a medical record involves finding out where it is being stored. Paper records will be handed out directly and have to be archived again later. Records in the OAS, of course, are handed out as copies.

The need to reduce costs has sparked the idea of replacing paper records by electronic records. One of the major challenges in replacing paper by electronic records has been the fact that paper records can have a personal signature on them. A personal signature confirms authorship or agreement with the content of a document and is therefore a legal requirement in many cases. Over the last years, many products have been developed in the area of digital signatures, which aim on providing similar authenticity for electronic documents as personal signatures do for hard copies.

The goal of this paper is to give an experience report about the use of digital signatures in a medical environment. The paper is structured as follows: In Section 2 we will give an overview of medical records. In Section 3 we will present the basics of digital signatures. We will also shortly report on a market analysis done to evaluate potential products to be used in our environment. In Section 4 we will describe the conceptual solution, including business processes that have been improved by the introduction of electronic archives. Section 5 will evaluate the implementation of the archive. In Section 6 we mention related work. Finally, we will conclude in Section 7.

2 Medical Records

For each medical treatment of a patient, a hospital or doctor has to create several medical records, e.g., diagnostic findings or surgery reports. The information that has to be archived in these records is clearly defined by law (§ 21 OÖKAG in Austria). At least it has to contain the name and birthday of the patient and her social security number, start and end date of hospitalization, anamnesis, condition of patient at start and end, date of hospitalization, course of disease, and medical attendance as well as surgeries and care procedures.

Medical doctors confirm the correctness of any documents they create or modify by their signatures. The administration of medical records is rather complicated. It involves many persons in several processes and workflows. These processes include retrieving all relevant records about a medical case from the archive, creating and adding relevant medical records during a patient's hospitalization and archiving all medical records after a patient's hospitalization.

Medical records have to be archived up to thirty years, depending on the nature of the attendance. The archival consumes much time and many resources. This is due to the large number of medical records, the huge amount of collected data, the archival over a long period of time, as well as many involved persons.

In the US, there is also a growing national effort to bring medical records into the 21st century by converting paper records to electronic records [2]. In 2004, a plan had been outlined, to have electronic health records for most Americans within a decade [3]. The main challenge is that sensitive medical records must not bee seen by anyone outside of a few trusted people who take care of patients. Centralized electronic records can be analyzed much easier than paper records that are spread over many doctors' file cabinets.

An electronic medical record of a patient simply is the medical record compiled into a digital format. The goal of our project is to replace all medical records in a specific hospital by electronic records and to further improve the archival process. We will focus on technical aspects including digital signatures. Privacy concerns are outside the scope of this paper. We consider the archival of records within one institution, rather than among hospitals, physicians, health insurances, etc.

3 Digital Signatures

Digital signatures are used to simulate the security properties of personal signatures that are handwritten on paper. They provide authentication of any documents like contracts or medical records.

3.1 Technical Aspects

Digital signatures are based on asymmetric cryptography. The idea of asymmetric cryptography is having separate keys for encrypting and decrypting – a public key for decrypting and a private key for encrypting. Public key algorithms are designed to resist chosen-plaintext attacks. They gain security by using hard-to-solve problems, e.g. factoring large prime numbers. Unfortunately, many public key algorithms are susceptible to chosen-cipher-text attacks [4].

Asymmetric cryptography can be used to sign documents. To sign a document, the sender usually applies a hash function on it, e.g. SHA-1. The signature of the document is calculated by executing the decryption algorithm using the private key of the sender on the hash values. The result of the process is the signature of the document. The signature can be distributed together with the document. This procedure of creating digital signatures is called the hash-then-decrypt paradigm [5]. In order to verify the authenticity and integrity of the document, the recipient of the document can first calculate the hash values of the document. Afterwards she applies the encryption algorithm using the public key of the sender on the signature received together with the document. As a result, she gets the original hash values of the document, which she can compare with the hash values calculated by her own. If they do not match, the document was signed or altered by anybody else or the private and public key do not correspond.

As just shown, it is important to assure that a public key belongs to a certain person. For this purpose, certificates are used. A certificate is issued by a certificate authority, which proves and guarantees the authenticity of a public key [6]. Thus, digital signatures need a public key infrastructure where public keys are tied to users by digital identity certificates.

Common reasons for applying digital signatures are authentication and integrity. Digital signatures can be used to authenticate the source of documents. As ownership of secret keys is bound to specific users, valid signatures guarantee that a document was signed by that user.

Readers of documents want to have the confidence that the document has not been altered after the signing process. If a document is digitally signed, any change in the document has to invalidate the signature. There must not be an efficient way to modify a document and its signature to produce a new document with a valid signature. This is still considered to be computationally infeasible by today's cryptographic hash functions.

One of the major drawbacks of digital signatures is the fact that there is no inherent certainty about date and time at which a document was signed. A signer may have included a time stamp with the signature. The document itself may also have a date mentioned on it. However, later readers cannot be certain the signer did, for example, backdate date and time of the signature. Trusted time stamping in addition to digital signatures is needed to prevent such cases of misuse. Missing time stamps and loss of control over a user's private key make all digital signatures with that key suspect.

3.2 Legal Aspects

Legislation concerning effect and validity of digital signatures is quite complex and differing in various countries. In the US, the Uniform Electronic Transactions Act brings differing State laws into line over areas as retention of paper records (checks in particular), and the validity of electronic signatures, thereby supporting the validity of electronic contracts as a viable medium of agreement. The Electronic Signatures in Global and National Commerce Act is a federal US law to facilitate the use of electronic records and signatures by ensuring the validity and the legal effect of electronic contracts.

Directive 1999/93/EC establishes the framework for electronic signatures in the European Union [7]. It distinguishes simple electronic signatures and advanced electronic signatures. Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. Advanced electronic signatures have to be uniquely linked to the signatory, be capable of identifying the signatory, be created using means that the signatory can maintain under his sole control and linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The directive also distinguishes between certificates and qualified certificates. Certificates are electronic attestations which link signature verification data to a person and confirm the identity of that person. Qualified certificates must contain (excerpt):

- an indication that the certificate is issued as a qualified certificate
- the identification of the certification service provider and the country in which it is established
- the name of the signatory or a pseudonym, which shall be identified as such
- signature verification data which correspond to signature-creation data under the control of the signatory;
- an indication of the beginning and end of the period of validity of the certificate
- the advanced electronic signature of the certification-service-provider issuing it
- limitations on the scope of use of the certificate, if applicable

Certification service providers must demonstrate the reliability necessary for providing certification services, ensure the operation of a prompt and secure directory, ensure the precise determination of date and time when a certificate is issued or revoked and verify the identity of a person to which a certificate is issued.

In Austria, the signature law (*Bundesgesetz über elektronische Signaturen*) implements the Directive 1999/93/EC of the European Union [8]. As the case study had been carried out in Austria, this law had to be considered for digitally signing medical records. Austrian's signature law defines simple digital signatures, advanced signatures, and qualified digital signatures. Austria's simple and advanced digital signatures correspond to the 1999/93/EC directive. Austrian qualified digital signatures correspond to European advanced digital signatures but additionally have to be based on qualified certificates.

3.3 Requirements

It is not feasible for a health care institution to develop its own archival solution supporting digital signatures. Therefore, a first step towards such a solution is to check available solutions on the market. Requirements to such a solution were:

*Integration with SAP is-h*med:* The AKh is using the clinical system SAP is-h*med, which supports documentation, planning and controlling of service processes and communication in hospitals [9]. The system combines patient administration with SAP standard systems for patient management, medicine and nursing, controlling and accounting and human resources management. One basic condition given by the AKh was that archival of medical records had to be integrated with SAP is-h*med.

Efficiency: One further basic requirement was user-friendliness and efficiency. This is especially important, because doctors in hospitals typically run out of time, frequently switch computers and therefore do not accept any time-consuming signing process. It was agreed that signing a document should not take longer than 0.5 seconds. It is not unusual that doctors have to sign many documents at a time. It is therefore important, that they can sign many documents within a single signing action.

Strength of digital signatures: It had been decided to use at most advanced digital signatures. The reason for this decision is that qualified certificates are difficult and expensive to accomplish with hundreds of doctors and a certain degree of fluctuation. If a new doctor gets employed, she should be able to sign documents from the very first day. The city, which is the owner of the hospital, does provide certification services, but does not fulfill all requirements by law in order to be regarded as a qualified certification service provider. In addition, advanced digital signatures were considered to be sufficient for the signing process of medical records in the AKh.

PDF documents, time-stamps: It had been decided to sign PDF documents and to include time stamps, i.e., the time of signing a document. Also, the digital signature has to be validated, recognized and displayed by Adobe's Acrobat reader.

Smart card infrastructure: The AKh already uses a secure user authentication solution based on smartcards by LOGiCO. The Secure Smart Card (SSC) software portfolio consists of a comprehensive client product, a central administration and an issuing tool. The creation of a digital signature is supposed to be based on this infrastructure.

3.4 Market Analysis

The requirements listed above are definitely specific to the AKh, but it is rather common that digital signatures have to be integrated in existing infrastructures. Based on these requirements, the following digital signature solutions were considered to be potential candidates for integration in the AKh:

Xyzmo Seal: Xyzmo Seal is a server-based digital signing procedure developed by Xyzmo [10]. Its focus is on simplicity and on replacing conventional rubber stamps. Xyzmo Seal supports simple, advanced and qualified digital signatures. Documents signed with Xyzmo Seal additionally include a worldwide unique document number and a tamper-proof creation time-stamp.

XiCrypt eInvoiceGuard: XiCrypt eInvoice Guard is a digital singing solution similar to Xyzmo [11]. Additionally it offers an interface for connecting it to SAP is-h*med.

E-Sign for SAP Solutions: E-Sign for SAP Solutions was originally developed for automatically signing documents occurring in business accounting [12]. It allows the signing of documents and invoices with advanced digital signatures. E-Sign is a full SAP application. It should therefore be easily possible to integrate it in SAP is-h*med.

*EPA Befundserver with CABARet and SignLive!***:** EPA Befundserver is a product developed by Siemens Medical Solutions. EPA Befundserver is an add-on tool for SAP is-h*med which provides document management functions for medical records. EPA Befundserver uses CABAReT, a tool developed by CABAReT Solutions AG [13] for displaying and editing PDFs. SignLive! [14] is a CABAReT add-on which provides digital signature functions. It enables signing documents with simple, advanced and qualified digital signatures from within CABAReT.

We have developed a catalog of requirements in order to come to a decision for one of these products. For each requirement we gave two points to a product which fully fulfills the requirement, one point for partially fulfilling it, zero points if we were not sure, and -1 point if the product definitely did not fulfill the requirement. Our results are shown in Table 1.

System transparency (requirement 11) means that users should not recognize that digital signature software is launched. Free signature field definition (requirement 12) means that it should be possible to freely define the position and the appearance of the signature field on the document, e.g., a picture showing the scanned signature of the user. The results have been based on interviews, technical documentation, product presentations and tests. The EPA Befundserver, which delivered the best results, had been chosen to be tested in the AKh.

Requirement	Xyzmo	XiCrypt	E-Sign	EPA
SAP i.s.h.med integration	1	1	2	2
Document archive integration	1	2	2	1
PDF signature	2	2	2	2
Timestamp service	2	2	1	2
Mass signature	1	1	1	1
Smartcard or software certificate	-1	1	1	2
Terminal server support	2	2	2	2
Advanced digital signature	2	2	2	2
Product support	2	2	1	2
Signing duration < 0,5 s	1	1	1	1
System transparency	0	0	0	2
Free signature field definition	2	1	1	2
PDF/A support	1	1	1	2
Printing of signed documents	1	0	1	2
Total	**17**	**18**	**18**	**25**

Table 1: Requirement catalog

4 Conceptual Solution

As mentioned above, whatever the solution will be, it is important to have it integrated with the current IT infrastructure of the AKh. This infrastructure consists of the following components:

*SAP is-h*med:* A hospital information system by SAP, a provider for a comprehensive range of software applications and business solutions for almost every aspect of different businesses [9].

MS Windows Server 2003 Active Directory: This is the central directory for the administration of users and also serves as basis for the certification process [15].

Certification Center: The administration of user certificates is provided by the owning city. The Active Directory is used to store these certificates.

Citrix XenApp: It acts as terminal server and is hosting the signature software CABAReT and the SAP Graphical User Interface (SAPGUI), which serves as an interface to the hospital information system. The signing process is supposed to run on this server.

Smartcard Infrastructure: Each employee already has a smartcard which is used for the login at XenApp.

In order to find the most efficient process for digital signatures, prototypical implementations of the following architectures had been tested. All of the architectures have in common that they support advanced digital signatures, see Section 3.2. The unique linkage to the signatory and the capability of identifying the signatory, as required by advanced digital signatures, will be provided by the use of certificates. Every user has its own certificate. The certificates are maintained by the certificate authority of the owning city. Forgeries or changes of signed documents are detected by using SHA-1 hash algorithm and RSA encryption algorithm with a key length of 1024 bits.

4.1 Client-based signature with smartcard

The doctor's smartcard is used to store the certificate for the signing process. The certificate gets stored on the card during the first login in the domain. Later, a login causes the certificate to be stored in the Windows certificate storage of the current user session. The private key remains on the card. The signing process starts simply by selecting a document and clicking a button, which starts the automatic creation of a PDF document of the original document, e.g. a Microsoft Word document. The PDF document is then presented to the user for review. If the user decides to actually sign the document, she has to click another button. The system then presents available certificates to the user and asks for a PIN code in order to access the private key on the smartcard. The hash value of the PDF document gets encrypted with the private key and embedded in the document. Then the validation process starts for the certificate which ends at the certification authority of the city, see Fig. 1. The signed document can then be transferred to its final destination, the department's or hospital's archive.

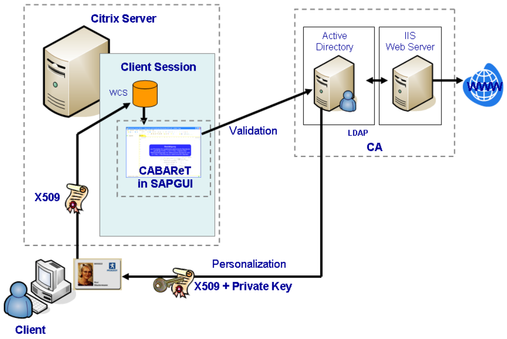

Fig. 1: Client-based signature with smart-card

4.2 Client-based signature with Active Directory synchronization

In this architecture the smartcard is not used for signing. Instead, the Active Directory is used for storing users' certificates. The main difference between the first architecture and this one is the method of loading the certificate into the Windows certificate storage.

The certificates of each user are stored in the Active Directory object corresponding to the user. On login, the Active Directory server checks to which groups the user belongs and requests the certificate authority, if certificates for members of these groups exist. If a new certificate for the user is found, Active Directory retrieves the new certificates (“synchronizing”) and stores them in the user’s Active Directory object.

The same procedure happens if a certificate has to be renewed. Afterwards, the certificates together with the user’s private key are loaded from the Active Directory object into the Windows certificate storage of the current user session. On logout, the certificates and the private key are removed from the session, in order to prevent other users from obtaining and misusing the certificates. This process is illustrated in Fig. 2. Signing of documents works similar as in architecture one.

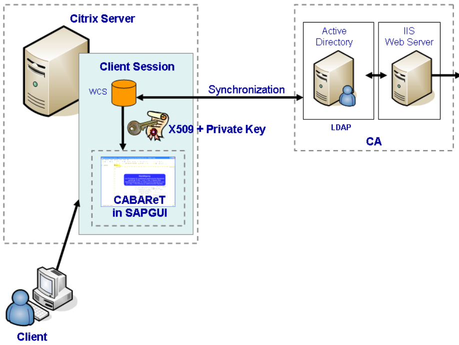

Fig. 2: Client-based signature with Active Directory synchronization

4.3 Server-based signature with personalized SSL certificate

A separate signature server is used for the signing process. This server creates both time stamps and digital signatures. The server needs two certificates per user, one for the signing process and one for the authentication of the user. Both certificates are retrieved via LDAP from the certificate authority, see Fig. 3. In order to select the correct certificate for the signing process, a user has to be authenticated. For this purpose, an SSL certificate is used and stored on the Citrix server. This certificate is used to securely connect to the signature server. When signing a document, a user has to select one of his personalized SSL certificates in the Windows certificate storage. This SSL certificate is unique for each user and can therefore be used for authenticating users by the signature server. The hash value of the PDF document to be signed is securely transmitted to the signature server by using this SSL certificate. The signature server connects to the certificate authority and retrieves the appropriate signing certificate and the private key for the user. The PDF document’s hash value is encrypted with the private key and a unique timestamp is added. The encrypted hash value is the digital signature, which is returned to the client. The signature is embedded into the PDF document and saved locally.

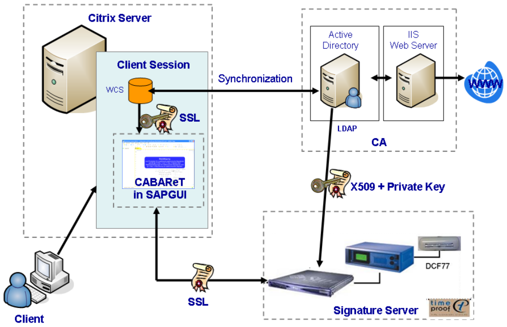

Fig. 3: Server-based signature with SSL certificate

In this server-based architecture, it would also be possible to let the user enter a PIN code, rather than to use an SSL certificate for user authentication. When singing a document, a user enters her username and her PIN code. A system-wide SSL certificate is used to securely connect to the signature server. This simplifies the certificate administration, because it is not required to maintain a personalized SSL certificate for each user. This modified architecture is shown in Fig. 4.

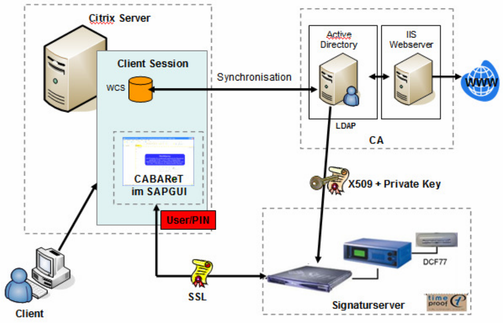

Fig. 4: Server-based signature with PIN code

The signature server takes the user name and the PIN code and retrieves the appropriate certificate and private key from the certificate authority. The rest of the process works similar as server-based signature with personalized SSL certificates.

5 Evaluation

We have implemented prototypes of each of the architectures presented in the last section. In this section we will present our results of testing those prototypes and we will outline the advantages and disadvantages we were able to identify.

All tested systems have in general worked satisfactorily, i.e., they were robust and reliable. From a legal point of view, the first architecture – client based signature with smartcard – would be preferable. This architecture would allow two-factor authorization as requested by the Austrian signature law. Unfortunately, our testing results showed that the signing process suffers from bad performance. The signing process took 5 seconds on average, which is clearly too long in our environment. Our tests showed that users simply did not accept this waiting time. The reason for this performance issue was the smartcard, which had high access times.

The second architecture – client based signature with Active Directory synchronization – showed better performance results. The signing process took about one second on average, which, as our tests showed, was acceptable to users. Additionally, this architecture could also be based on existing hardware. Furthermore, administration and distribution of certificates could be fully automated. One potential disadvantage of this architecture was the low security level when omitting PIN codes for accessing the private key of certificates. Without PIN codes, the requirement of the Austrian signature law for qualified digital signatures (Section 2, Number 3a SigG) cannot be fulfilled, because the private key is not under sole control of the user [8]. Therefore, without PIN codes, only simple electronic signatures can be implemented.

The third architecture – server-based signatures with personalized SSL certificates – was the best solution from the performance point of view. The signature server (Timeproof Server) could create even advanced electronic signatures faster than the client-based methods. But the organisational efforts of this architecture were high. At first, only smartcards which are confirmed by a special authority could be used. Further, the Timeproof server only supported eight smartcards, whereas in the hospital about 360 smartcards existed. This fact prevented from creating advanced electronic signatures, leading to a security level which was not higher than in other architectures.

A secure timestamp cannot be created, because there is no infrastructure for receiving secure time signals. The time signal which is used as an alternative is the time from internal NTP servers. This is nothing else than the system time, which is also used in the other architectures and therefore does not bring any advantage. Additionally, the efforts of administrating SSL- and signature certificates are high. Those certificates must be created and assigned to each other manually. These efforts and costs for new hardware are disadvantages of this solution.

Given these test results, the AKh chose the second architecture – client-based signatures with Active Directory Synchronisation, because this architecture causes low efforts, offers acceptable performance and has low acquisition costs. At the time of this writing, the AKh does not use PIN codes as recommended, because of the apprehension, that users may not accept this solution. Nevertheless, even the legal requirements are satisfied, because special legal statutes for the internal treatment of medical records are still missing. Therefore, simple digital signatures are currently sufficient.

It has to be mentioned at this point, that a lower level of security than possible had intentionally been chosen both from a technical point of view and also from an organizational point of view. For example, a smartcard could be left behind in an emergency situation. Social engineering leading to misuse can also be done easier without the use of PIN codes. However, in case of stronger legal requirements, the obligatory use of PIN codes can easily be added to the solution at a later time. Also, the certificates may get upgraded to qualified ones, if needed.

6 Related work

LENUS is an enterprise content management system specialized for medical and administrative processes in hospitals, which also includes digital signature functionalities [16]. This product has not been considered in our environment, because it is a complete solution for content management. We were looking for a solution that integrates in the AKh's technical infrastructure seamlessly and not for replacing solutions already in use.

wHospital is a web-based application for drug dispensing management [17]. Its focus is on mobile usage, i.e., doctors and nurses use tablet PCs and PDAs for drug dispensing. Due to legal requirements, digital signatures have to be used. The concept of mobile usage sounds promising, but was not a requirement in our environment. Additionally, the solution is focused to drug dispensing, whereas we were looking for a solution which covers the whole medication process.

Brandner et al. tried to determine user-oriented and legal requirements for a public key infrastructure for electronic signatures for medical records [18]. Depending on their results, they developed a prototype, which was integrated into the existing infrastructure of a German hospital. Although their goals were similar to ours, the resulting solution depended heavily on the existing technical infrastructure and the workflows in hospitals. It is therefore nearly impossible to take an existing solution and establish it without any or minor changes in the given environment.

7 Conclusion

The use of digital signatures will become more widespread, mostly in the areas of e-business, e-government, and e-health. Both legal and technical prerequisites are available today. However, as our case study has shown, the implementation of a digital signature solution is far from being simple and easy. Several issues have to be tackled in the run-up, especially legal aspects like the required strength of the signature, e.g., simple, advanced, qualified. Performance considerations play an important role also. A weaker signature typically leads to better performance, but may not be an option due to legal constraints.

Stronger signatures not only make demands on the technical infrastructure, but also provide a challenge to the organizational structure. For example, the administration of certificates is not an easy task when many users have to digitally sign and when these users have a high fluctuation. And even though digital signature solutions are available out of the box, it is still not an easy task to integrate such solutions in existing technical infrastructures.

8 References

[1] D. W. Bates, "The quality case for information technology in healthcare", *BMC Medical Information and Decision Making*, vol. 2, October 2002.

[2] "At risk of exposure: In the push for electronic medical records, concern is growing about how well privacy can be safeguarded", *Los Angeles Times*, June 26, 2006.

[3] P.G. Goldschmidt, "HIT and MIS: Implications of health information technology and medical information systems", *Communications of the ACM*, vol. 48, no. 10, pp. 68-74, October 2005.

[4] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd ed., John Wiley and Sons, New York, 1996.

[5] H. Delfs, H. Knebel, *Introduction to Cryptography - Principles and Applications*, 2nd ed., Springer, Berlin, 2007.

[6] S. Oaks, *Java Security*, 2nd ed., O'Reilly & Associates Inc., Sebastopol, 2001.

[7] Directive 1999/93/EC of the European Parliament and of the Council of 13 Dec. 1999 on a Community framework for electronic signatures.

[8] Austrian Signature Law: Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999, http://www.a-sit.at/pdfs/SigG.pdf [April 2, 2008].

[9] IS-H*MED Clinical System, http://help.sap.com/saphelp_ish471/helpdata/EN/94/8cae395b0ae361e10000000a11402f/content.htm. [March 18, 2008].

[10] Xyzmo Seal, http://www.xyzmo.com. [April 22, 2008].

[11] XiCrypt eInvoiceGuard, http://www.xicrypt.com. [April 22, 2008].

[12] E-Sign for SAP Solutions, http://www.esign.at. [April 23, 2008].

[13] CABAReT Stage. A flexible software for your daily work with PDF-Documents, http://www.cabaret-solutions.com/en. [April 18, 2008].

[14] Intarsys. Innovations for Electronic Documents. http://www.intarsys.de/d?set_language= en. [April 22, 2008].

[15] Microsoft Windows Server 2003 Active Directory, http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.msp. [April 23, 2008].

[16] D. Krechel, M. Hartbauer, K. Maximini, "LENUS - The Hospital Content Management System", *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems (CBMS'06)*, Salt Lake City, 2006, pp. 9-14.

[17] L. Rossi, L. Margola, V. Manzelli, A. Bandera, "wHospital: A Web-based Application with Digital Signature for Drugs Dispensing Management". http://embc2006.njit.edu/pdf/1281_Rossi.pdf, [April 18, 2008].

[18] D. Brandner, M. van der Haak, M. Hartmann, R. Haux, P. Schmücker, "Electronic Signature for Medical Documents – Integration and Evaluation of a Public Key Infrastructure in a Hospital", *Methods of Information in Medicine*, vol. 41, no. 4, 2002, pp. 321-330.