Lutz Vorwerk, Chunyan Jiang, Christoph Meinel:
Secure Transfer of Digital Images and Related Data
in Proceedings of the 11th International World Wide Web Conference (WWW 2002), W3C, Hawaii, USA, 5, 2002.

[i]Secure Transfer of Digital Images and Related Data

Lutz Vorwerk, Chunyan Jiang, Christoph Meinel
Institut fuer Telematik, Bahnhofstrasse 30-32, Trier, Germany

ABSTRACT

Communication in medicine and healthcare is very important. A standard used for communication is DICOM. It integrates medical images with patient related data. This data describes some attributes of the image and the patient whom the file belongs to. The interpretation of radiological images is a required procedure. It is hard to understand a report directly without a relationship to an image. So the structured reporting that ease the understanding of reports is preferable. During the transportation process, another important issue arises. It is security. In a DICOM application, the data of a patient should be read only by some specified persons or groups. It must provide a mechanism to guarantee the data can not be gained by other persons. There are several methods to realize encryption and decryption. We developed one system used to apprehend and transfer DICOM files, and extended this system to meet the requirement of security. In order to secure the data, this system adopts the PKI mechanism. It uses public key and private key to authenticate the identity. At the same time, there are still many other important information need to store in one device. So we design one health professional JAVA card. Our system include some elementary files to verify the patient's key (private key) and doctor or hospital's key (public key).

Keywords: DICOM, healthcare, structured reporting, security, smart card, PKI, authentication

Wordcount: 5491

INTRODUCTION

There are more than 22 million internet pages concerned with health and health related topics worldwide. In Germany about 630 000 web pages offer information on health and health care services. It seems quite obvious that "Online Health Care" will play an increasingly important role in doctor/patient relations and will highly influence how individual persons `manage` their personal health. Patients will have the possibility of obtaining online information about prescriptions and treatments. At the same time, they will be able to evaluate their local doctor's services in a broader context. Patients even could join online self-help groups. It is also highly likely that Internet pharmacies will start to sprout rapidly on the Internet in the near future. As for today, German law does not yet allow the electronic prescription or even the electronic ordering of medications. Actually, progress in the field of electronic health care is extremely slow in Germany. The existing technical potential is hardly even being exploited, because obsolete, inflexible standards and structures prohibit the use of these existing potentials. To counteract these setbacks which result in a falling behind of the German progress in telemedicine as compared to other parts of Europe, the German government is planning to develop a comprehensive platform of Telematics, aimed at regulating the integration of the various different health care services. Projects such as “Electronic Prescription”, “Secure Infrastructure”, “European Dimension” are mainly concerned with administrative and business considerations.

The need for laws regulating Internet health care is exceptionally urgent. Clear standards and regulations are needed as the basis for a not only rapid but also constructive development of electronic health care services. DICOM (Digital Imaging and Communication in Medicine) is one of those standards.

STANDARD OF DIGITAL IMAGING AND COMMUNICATION IN MEDICINE

DICOM is the abbreviation for digital imaging and communication in medicine. It defines protocols and mechanisms to manage and transfer medical data. The combination of patient data and image data those conform to the DICOM standard is called a DICOM image. There are some other elements of the DICOM standard like DICOM Worklist. They are not mentioned here because these elements are not relevant to this paper, yet. The DICOM protocol intend to negotiate the features of the DICOM standard supported by two DICOM applications which want to communicate. The subset of DICOM features supported by both applications decides if a communication is possible.

The use of computers in medical imaging and the development of applications that process images, which have been produced by imaging devices, creates the problem of how to exchange images with related patient data between devices of different manufacturers. A common interface has to be specified for the devices and applications. This interface, called DICOM, makes it possible to connect devices, PACS and databases that contain diagnostic data. The DICOM-standard is accepted and used by many manufacturers.

The status of the standard is represented by the core. This core consists of several parts which specify the required elements. These elements are needed to develop and to understand a DICOM-conform application. The required elements are: the definitions of attributes, the representation of these attributes, the transfer of a set of attributes and the storing of these attributes in a file. A statement declaring which attributes defined in the DICOM-standard have been used and how they are being represented, as well as additionally defined attributes that do not occur in the DICOM-standard, has to be written. The statement is important for a user who wants to buy a DICOM application or hardware with a DICOM interface. The statement may serves as information about the interoperability of two DICOM interfaces. Interoperability may not be guaranteed if the statement is indefinite, incomplete, imprecise or incorrect. Developers of DICOM-conform applications, as well as manufacturers of DICOM-conform devices, must be sure to describe the features of their products thoroughly in order to increase the interoperability and acceptance of products that conform to the DICOM-standard.

The core of the DICOM-standard may be extended by correction-proposals or supplements. The evolution of DICOM is achieved by the integration of accepted supplements that have reached a final status and by the acceptance of correction proposals. There are two supplements concerning the integration of security in the DICOM-standard. Both are vague when specifying the transfer of encrypted data. There are some basic elements like digital signatures and authentication. The definition, which describes the use of digital signatures in adding an attribute that contains the hash-code to a set of attributes called module in the

DICOM-standard, is clearer than the description of encryption and decryption. Therefore, the use of digital signatures is not considered here. A module in DICOM represents a piece of related information like the module ‘patient’ that contains all personal data of a patient. The problem for this solution of integrating digital signatures in the DICOM-standard is the modularity of the standard. An application without support for digital signatures may ignore the attribute that contains the hash code so that this attribute may get modified and the document may be transferred to a third application. This application contains a feature to verify digital signatures if they exist. It reads the document, estimates that there are no digital signature attributes and treats the data as unsigned. A problem of information getting lost is that it is dangerous for the transfer of data which must not be changed. The guaranteeing of a consistent exchange of data is one aim of digital signatures.

The other supplement of the DICOM-standard concerns the authentication of Service Object Pair (SOP) and the specification of security policies. An SOP is a combination of a set of modules representing a DICOM document, called ‘Information Object Definition’ (IOD) and a service that allows to work on the attributes of the modules and therefore, on the IOD.

Operations that move data from one point to another are an example of such a service. The authentication integrated through the supplement concerns the communication between two applications which support the service. This SOP itself is authenticated by the other application. This concept is very time-consuming because of the verification of the SOP that poses the request for authentication. The encryption of a connection between two applications is specified incompletely. There is no concrete definition of how to integrate encryption into the DICOM-standard. There are references for policies, but these policies require creativity from the developer. DICOM also offers an appropriate method to manage radiological reports.

DICOM CONFORMS RADIOLOGICAL REPORTS

The DICOM-standard was enhanced by a supplement called Structured Reporting (SR). This supplement is part of the core now. SR defines a way to produce medical reports of radiological image interpretations. In practice, the production of a report is achieved by using a dictaphone. The report recorded on tape is transcribed by a secretary. The secretary shows the transcribed report to the physician who recorded the tape. The physician verifies the report and signs it. To reduce the amount of text, the physician uses a medical code. The code is often a standard-code like logical observation identifier names and codes (LOINC) or systemized nomenclature of human medicine (SNOMED). Additionally, private codes of physicians are also used. Because the physicians may want their code to be understood only by themselves or by a group of people they trust. The supplement SR uses the supplements for coding medical data which are integrated in the core now in a pre-defined scheme. In the definition of SR, there are three pre-defined kinds of reports. The basic-text, the enhanced, and the comprehensive Information Object Definition (IOD).

The structure of a SR report is complex [Gehlen98], [Clunie00]. This structure is represented in DICOM as an IOD. In [NEMA00], there are three definitions for a report IOD. These three definitions will be described in the following:

- The simplest definition is the SR-Basic-Text-IOD. This definition possesses the features of reference images and other reports. The structure of a report in this definition consists of the following elements: a document content that contains information about the examiner, as well as information pertaining to the time the report was created and why the report was created. Medical Codes may be integrated. An observation context may be integrated by using relationships between predefined classes defined for the creation of a report.

- The SR-enhanced-IOD provides additional classes like coordinates to reference an area in an image. The coding scheme defined for these three IOD is the SNOMED DICOM micro glossary (SDM). This coding scheme is a medical coding scheme that assigns medical code words to their descriptions.

- The comprehensive IOD allows the specification of relationships by reference instead of using values like in the other two IODs. There are some implementations of SR which use SR to relate text to images.

Currently, SR is regarded as very complex. The complexity can let applications run into difficulties when interpreting SRs because too many variations of ways to construct a report exist. Nevertheless, it is a good decision to use SR because it provides the best way to relate images to reports. Some data has to be protected. Therefore standards for security are needed during transferring and storing medical data.

SECURITY IN HEALTH CARE

Regarding the area of telemedicine, there is a demand for the protection of images. The cause for this demand is the need to prevent the relationship between patient data and an image from being determined. This section describes some aspects that are necessary to understand what security means when transferring data from one destination to another. There are different modes to protect data from third persons who want to read this data.

One way is to hide the data in other data. This concept is called steganography and is used for example in digital watermarking. It is that data belonging to an owner of an image is integrated in the image and protected against modification by using a digital signature. A digital signature builds a hash over the data that has to be signed. The hash is an encryption that is not reversible. The hash is encrypted with a private key. The private key is a secret key that can only be assigned to one and only one public key. The public key serves as a helping tool to exchange data with the owner of the assigned private key. To verify a digital signature, the hash is first decrypted with the public key and then it is checked whether the decrypted data (hash) matches the hash that has been generated by the data to verify if the data is changed.

Another way is to encrypt the data. That means to protect the data against modification and against information retrieval. The first step of such a method is the generation of a key. An algorithm declared ‘secure’ is Rivest Shamir Adleman (RSA). This algorithm is based on the problem of factoring large integers. Another method is that of Diffie and Hellman. This algorithm computes discrete logarithms modulo a prime number. A third method is that of using elliptic curves to compute the keys. The keys are shorter than in RSA and evoke, therefore, a smaller bandwidth and memory requirements.

With the key generation, a key pair is created: the public and the private key. The public key is now used to encrypt the data that can now only be decrypted by the owner of the private key. This method is called ‘asymmetric encryption’ because of the fact that one key is used for encryption and another one is used for decryption. Another method is called symmetric encryption. This method uses one key to encrypt and decrypt the data. It is less time-consuming but also less secure because the key can get deciphered by a crypto-analyst.

In order to come true a system which finds the approval of most physicians, JAVA should be used. This programming language allows to connect to an order database where the physician can deposit her or his order. The order is then processed by the radiological department, which orders, in turn, existing images of the patient and decides if there are available images and if these images are sufficient to meet the requested order of the physician. If the answer is positive, the radiologists perform the findings by using these images and then send the report to the physician. If not, they tell the patient to make an appointment to produce new images. This procedure is beneficial to the physical health of the patient, because of reduction of radiation.

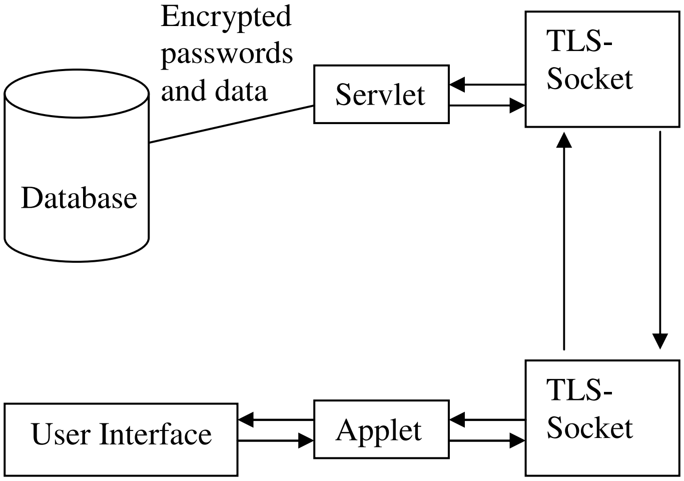

Figure 1: Model of integration of a TLS-mechanism into Engrane

There are some kinds of impediments. German regulations are very restrictive concerning the transfer of digital medical images and patient data.

Among the existing components of this system is Engrane (see next chapter for further information), which will be connected to a database via sockets. A socket is one end-point of a two-way communication link between two programs running on the network. These sockets provide a secure protocol mechanism capable to store physicians’ reports and order in a secure manner.

The system component presented here uses the javax - API (Application Programming Interface) to implement a secure transfer between two locations. One location has an applet (i.e. the multimedia-editor or a text editor) which uses the implemented TLS (Transport Layer Security) [Dierk97] to communicate with a servlet. This servlet operates on a database to store incoming requests and process them. Incoming requests are URLs that refer to objects which are to be processed. These URLs contain keys to decrypt the data of the referenced object.

The first thing which one must consider here is the TLS protocol definition. Afterwards, a transfer of the TLS protocol to the structure of the hierarchical ordered security classes, which form the javax-API, is necessary. To perform the transfer, we have restricted the used encryption algorithms to those which are actually considered to be highly secure[Menezes96, Teletrust 98]. The management of used algorithms will be performed by a database which stores the compiled Java classes. The database will be used by a Java servlet. The communication between the database and the servlet is handled in a secure manner to prevent interior attacks. Information sent to the database is encrypted by PGP (Pretty Good Privacy). The servlet governs a key table stored as an PGP encrypted object in the database. During initialization, the servlet asks the user for his or her login and password in order to be able to decrypt the key table. If the key table is available, the servlet is able to read and store objects in the database. New keys will be created for new objects. We use the Cryptix Java Security [Cryptix97] extension as a helping tool. It provides the majority of the encryption algorithms and is a valuable basis for our development. How to integrate a TLS connection in the system is shown in Figure 1. The Keys used to establish the communication are stored in certificates. The certificate allows an identification of the application. The application uses the Java library Cryptix in order to produce certificates. The application consists of two tools, one tool is for certificate creation and the other tool is for verifying the existing certificate. The certificate is used by the application in order to create the symmetric key pair for establishing an encrypted connection between the server and the client. The application works until the certificate is expired. If the certificate is invalid (wrong certificate issuer or certificate is expired) the application will not work. This procedure is developed first, because the use of the application should be as simple as possible. It is possible to transfer data by using encryption and you do not care about passwords. The application will be extended through a JAVA-card access mechanism. Certificates are stored in following format: Name, First name Organisation, Department, Email, Validation Begin, Validation End, Data of construction.

We implemented a system for presenting radiological images. The system is called Engrane and may be used in order to demonstrate findings made of radiological images. Those demonstrations can be performed local or remote. The component described above is integrated into this system in order to secure the transfer of patient data.

THE SYSTEM ENGRANE

The System Engrane integrates a DICOM Server and a user interface. Engrane display patient data according to DICOM Patient, Study, Series, Image hierarchy. Important values of attributes of each level are listed. On series level it is possible to choose two series and compare them. This feature is important to compare series of a patient that are made at different times. Image operations integrated at series level and image level are rotation, lenses, flipping, annotation, to adjust brightness and contrast and windowing. Second module is developed in order to manage presentations and organize them into a calendar by using drag and drop. Every presentation is represented as an icon containing the name of the patient, his or her birth date. A third module serves for the presentation. The presentation is started simply by a click on the corresponding icon. Afterwards, one may walk through the presentation by simply pressing a button. In order to manage different users and settings they made we think about to integrate smartcards to prevent time consuming log in by password. Additionally, it is possible to integrate a management of prescriptions. Let us assume the case of an physician who wants to refer to a radiological report in order to write a prescription and wants to refer to the medicine taken by the patient before. A model for writing, receiving a receipt describe the next section.

EXTENSION OF ENGRANE TO SUPPORT OF ENTRIES CONCERNING PRESCRIPTIONS

The process of authentication is the most important process in a public key infrastructure (PKI), because the verification of user identification is a process, that decides what access rights assigned to this person and if a person is allowed to use components of the PKI. An appropriate method to perform an authentication is to use a chip card like a Java Card. In this section we will introduce a special kind of health professional card (HPC) using a multifunction Java Card with a flexible verification for distributed subsystems of a networked system for healthcare. A flexible verification means that the sender of a signed mail could automatically be identified by scanning different directory servers of this system. We developed a concept for an electronic prescription of a patient. For a system of healthcare, it is important to proceed a standardized electronic patient record, which can be used in different national systems for healthcare of the world. Nowadays we have many different card systems. Almost all chip cards are shipped with implemented software using application programming interfaces (API) written in the programming language C, but there is an alternative: the Java Card. On a multiple application Java Card you may integrate several applications with the Java Card Virtual Machine. These applications must have a high secure architecture with the possibility to digitally sign.

Nowadays, the increasing development of internet applications for the transfer of private medical data forces a need of high secure mechanisms that protect the data to be transferred over the internet as well as infrastructures especially developed to provide authentication and authorization mechanisms. A PKI is used to assign the public key of a user with owner information. The public key together with the owner information represents a certificate. Certificates are managed in a certificate database, which provides services like certificate verification, request, enrollment and management. The private key is kept by the owner on a chip card preferably. The private key can not reconstructed from the public key, but the public key can be reconstructed by the private key. That is why this kind of key pair is called asymmetric. Two different keys are used to perform encryption and decryption. Here a first check will be done if the public key belongs to the private key.

There are many different card systems used in healthcare. Considering Europe, the importance of card systems for healthcare increases. There is a system for healthcare in Europe which consists of three levels. The first level is represented by the physicians, the second by the specialists and third by the hospitals and clinics [BfB97]. The communication between these levels is not standardized in the national and international system for healthcare. Most kinds of communications consist of the exchange of letters by post instead of using electronic communications. Only in some fields there are microchip cards. Nowadays, we use different cards for insurance and hospitals. In 1994 the insurance card of the duty health insurance substitutes the health insurance certificate [G&D00]. Patients with a private health insurance have a hospital insurance card. These cards are only for administrative purposes. Other health card systems are not widely known or not popular.

MULTIMEDIA STANDARDIZED, ELECTRONIC PATIENT RECORDS

The standardized, multimedia, electronic patient record depicted in figure 2 can help to improve the communication between the three levels doctors, specialists and hospitals. A secure electronic data exchange between the different groups simplifies the administration processes of this system. It can reduce costs and it can avoid faults caused by sending the wrong information. So we need an electronic communication platform for the system [JCAP99]. The infrastructure has to be modernized by new medical networks and trust centers. The medical network enables the electronic communications. Trust centers are needed for secure data transfer. All members of the health systems need different types of certificates, private and public keys, a symmetric key for ciphering, a hash function for computing the signature.

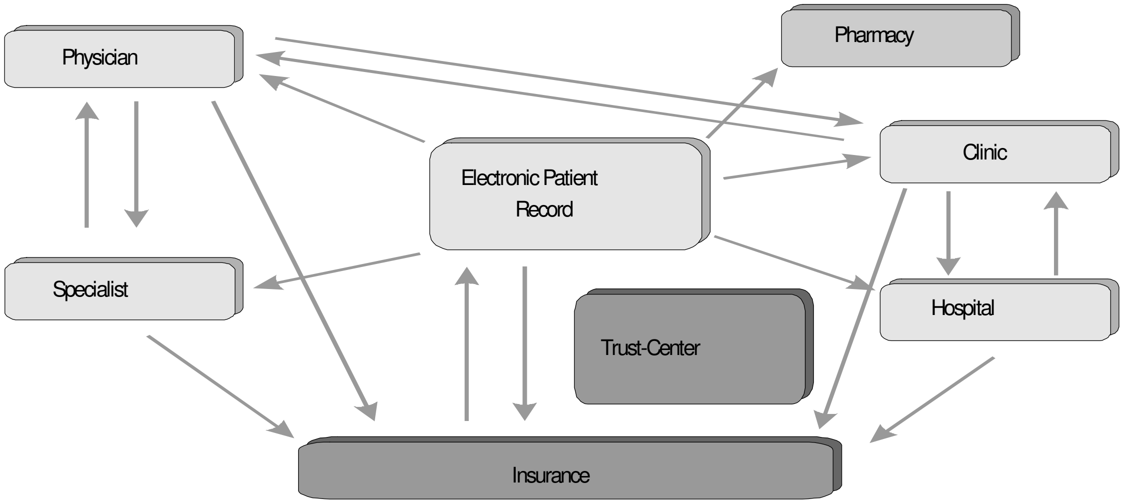

Figure 2: Patient-Oriented Model of Healthcare

For a healthcare system it is important to provide a standardized, multimedia, electronic patient record, which can be used in different national systems for healthcare in the world. Another requirement is to support a multifunction card. There are different possibilities to use a health professional card together with an electronic patient record. Some information can be stored encrypted on the card. Other applications can be used for authentication to get the electronic patient record from the server of a hospital or other institutions.

DESIGN OF A HEALTH PROFESSIONAL JAVA CARD (HPJC)

The solution for multifunctional smart card used in order to store important patient-related data needed for prescriptions is the Java Card. The Java Card standard is created in the Java Card Forum founded by the smart card producers Bull, Schlumberger and Gemplus [JCF00]. With a multifunctional Java Card it is possible to access several applications by using the Java Card Virtual Machine. An applet on the Patient Card can read information from the card. With the information it is possible to retrieve additional information from the WEB, if needed. We used the Java Card API 2.1. This API support cryptology, object sharing between applets and file system management.

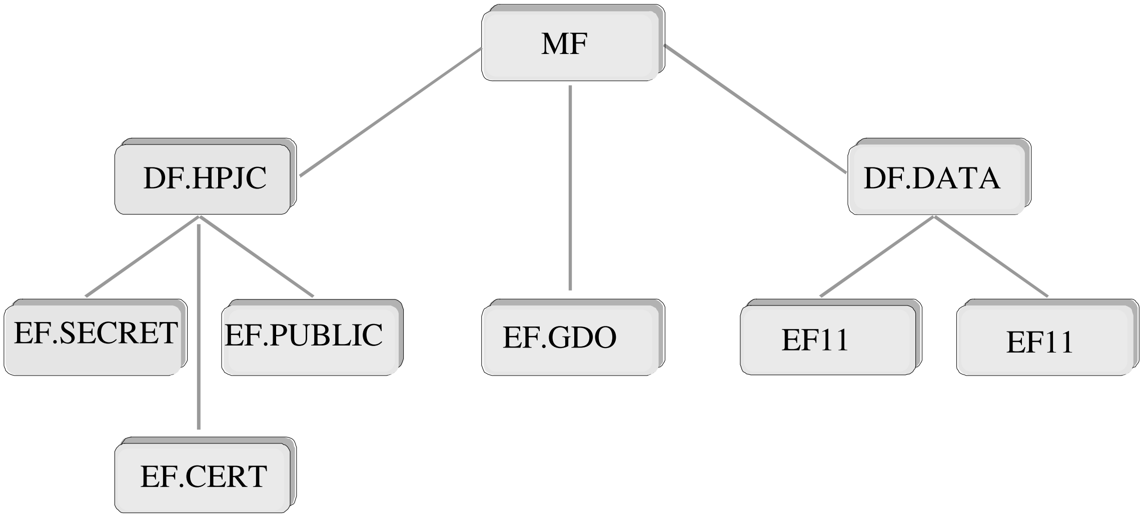

Figure: 3 File System Patient Card

A HPJC shall comply with ISO/IEC 7816, the standard of smart cards and with DIN NI-17.4, the standard of chip card with electronic signature application [ISO00], [Sch96]. In our application we use an ID-001 card. The other important card format is ID-000. The dimensions and locations of contacts are specified in accordance with ISO/IEC 7816-2. In our application the half-duplex asynchronous Block Transmission Protocol T=1 is used. For this protocol the node address (NAD) has to be set to '00'. The file structure is in accordance with ISO/IEC 7816. The file structure is hierarchically oriented (Fig. 2). The root of this hierarchy is the master file (MF). The MF-File contains elementary files (EF) and dedicated files (DF). The dedicated files consists of dedicated and elementary files, but the dedicated file in the last plain of the hierarchy containing only EF's. Below the MF as depicted in figure 3 we have the EF.GDO, the ground data object with the serial number of the chip (ICCSN) and the name of the card holder (CHN). The signature application is stored under the DF.HPJC. All applications have a DF with an application identification (AID). The DF.HPJC consists of three groups of EF's, the secret files, the public files and certificate files. The PIN-Number and private key are located in the secret files. The public key and the hash function are located in the public files. The certificate of authorization and the attribute certificates of health insurance, pharmacy, doctor and hospital are located in the certificate files. If you put the card in the card holder, the answer to reset (ATR) will start and initialize the card. Then the MF is selected.

The secure hash algorithm (SHA-1) is used [Sch96b] for hashing. Only the 160-Bit hash algorithms of MD4 family are suitable in Germany [BSI99]. Two conditions have to be fulfilled. The hash algorithms have to be free of collisions. The hash algorithms have to be one-way functions. After the computation of the hash the next step is to store the hash value together with the document on the disc of the PC. The hash value is written to an EF. With the standard command, select file and read binary the value could be transferred on the disc. The hash value of document is a suitable method to check, if somebody modified that document. The next important process is to read public certificates and their public keys. We stored this information in the EF.PUBLIC.x elementary files. For different applications the card checks, if the certificate of the doctor, of the pharmacist, of the hospital, or of the insurance is correct. We introduce only the process that the certificate is stored on the Java card and has to be checked. Provided that the actual X.509 certificate is downloaded by an X.500 directory server and stored in the EF.PUBLIC.CERT.PHAR. The verification can also be processed in a similar manner for data which is sent encrypted by the public key of the sender.

In order to demonstrate the usage of a Java Card configured in the way described above, an example which assumes a patient who has visited his doctor is described in the next section. The doctor send a prescription to the pharmacy of the patient as a digitally signed Email. Then he goes to the pharmacy to get his medicaments.

USAGE OF THE MULTIFUNCTIONAL PATIENT CARD FOR TRANSFERRING A MEDICATION LIST

It is possible for patients to use different levels of the healthcare system. We simulate the different levels by using different servers in a local network. We will introduce the transferring of prescriptions with a multifunctional patient card by using the example of a patient who receives his medication. The doctor, who has already been visited by his or her patient, has made a diagnosis. As a result of this diagnosis, he or she has written a prescription. It is assumed that the patient has told the doctor who his pharmacist is. The doctor uses a symmetric key for ciphering the document. The symmetric key is ciphered by the doctor’s asymmetric key. At this point, there are different possibilities of transferring the prescription securely and electronically to the pharmacist, due to the fact that the doctor may use the following different asymmetric keys.

1. private key of the doctor
2. public key of the patient
3. private key of the patient
4. public key of the pharmacists.

In the third case the patient has to be absent to check the ciphering with his private card. The patient may not give the PIN-number to the doctor. However, he can cipher the symmetric key of the doctor with his private key.

At this point, the patient goes to his pharmacist. For each of the four possibilities, the patient has different methods of deciphering the symmetric key of the doctor.

1. The patient verifies the X.509 certificate of the doctor. The certificate is stored in a LDAP Directory Server of a trust center. If the patient has the doctor ‘s public key on his card, he can decipher the doctor ‘s symmetric key with the doctor’s public key. If the patient does not have the doctor ‘s public key , he can read the public key from the certificate downloaded from the trust center. So he may decipher the symmetric key with that public key.
2. The patient deciphers the symmetric key with his private key. He may use his private key after authentication with his PIN-number.
3. The pharmacist verifies the certificate of the patient with directory server of the trust center. The first alternative is that the patient deciphers the symmetric key with his public key. As his public key is on his smart card, he can authenticate himself with his PIN-number. The other alternative is to read the public key of the patient out of his certificate downloaded from the trust center. The patient identifies himself with a identity card or a driver license.
4. The pharmacist uses his smart card to decipher the symmetric key. In doing so, he enters his PIN-number before using his private key.

After deciphering the symmetric key, the prescription can be deciphered with the symmetric key. In this process, the pharmacist must check the digital signature. He or she computes a hash value with the same hash algorithm used by the doctor. The pharmacist computes the hash value of the deciphered medication list. Afterwards, he compares that hash value with the sent digital signature. If these values are the same, the digital signature is the same as the original.

CONCLUSION

This paper presents the significance of the communication in healthcare. The standard used in this communication combines the medical image with related data. In order to be understand easily by different users, a system should offer a report to describe the attributes of the image and the related patient data.

The other important aspect of the communication is security. The data transferred between different terminals should be protected against illegal accessing. The data can be hidden in other data such as digital watermarking. It also can be protected by encryption by using a public key. The receiver of the data can decrypt it by using his or her private key. The system can authenticate and verify as far as the key is available. To store the private key and patient information, a smart card should be used. Using this device, all processes concerning authentication can be automatically.

We designed one system named Engrane which can satisfy the requirements, that means not only to communicate with DICOM files, but it is able to handle the security issues additionally.

REFERENCES

[JCAP99] Java Card Application Programming Interface 2.1, Version 1.0, 1999

[BfB97] Telematik im Gesundheitswesen - Perspektiven der Telemedizin in Deutschland -für Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie und Bundesministerium für Gesundheit, München 1997 http://www.iid.de/forschung/studien/telematik/ oder http://www.rolandberger.com

[G&D00] Application of Health Cards, http://www.gdm.de/index_0.htm G&D

[JCF00] Java Card Forum (JCF), Standardization workgroup of the Java Card. http://www.javacardforum.org

[ISO00] ISO7816 Standard, Teil 4 – vollständig http://www.fh-augsburg.de/~bossekr/iso7816_4.html

[Sch96] Specification of chip card interface with digital signature application/function, DIN NI-17.4, Version 1.0, 1998

[Sch96b] B. Schneier, Applied Cryptography, Second Edition, 1996

[BSI99] Geeignete Kryptoalgorithmen gemäß § 17 (2) SigV, Hrsg.: Bundesamt für Informationssicherheit (BSI), Bonn 1999 http://bsi.bund.de

[NEMA00] NEMA, 2000, Digital Imaging and Communications in Medicine, Part 1-15. NEMA Standards Publication PS3.X.

[Clunie00] Clunie, Dr. A. D., 2000, DICOM Structured Reporting, PixelMed Publishing.

[Gehlen99] von Gehlen, S., Vorwerk, L., Eichelberg, M., Jensch, P., 1999, A multimedia editor for radiological reports based on the DICOM Supplement Structured Reporting. In CARS `99, Computer Assisted Radiology and Surgery,(H.U. Lemke, M.W. Vannier, K. Inamura and A.G. Farman), 438-442, Elsevier, Paris.

[i] www2002, The Eleventh International World Wide Web Conference, Alternate Paper Tracks Proceedings (CDROM), T2 ,ISBN 1-880672-20-0,/alternate/T2/index.html, Honolulu, Hawaii, USA, 2002.