# Security Requirements for Telemedical Applications Regarding DICOM-image-management in a PACS[1]

Lutz Vorwerk, Chunyan Jiang, Christoph Meinel
Institut fuer Telematik, Trier, Germany
*Lutz Vorwerk, Instutit fuer Telematik, Bahnhofstrasse 30-32, 54292 Trier (Germany),vorwerk@ti.fhg.de*

*Standards are required in order to exchange data between applications of different retailers. A standardization of health care applications with provided security due to the DICOM-standard's current status of DICOM - PKI proposal(2). The specification of security profiles within DICOM is a first step performed to secure medical applications. We examined, if either a directory service or a "web of trust" is appropriate to implement a PKI. The infrastructure given by the DICOM standard decides which approach will be used. Regarding DICOM, applications are not able to decide if they trust other applications or not. Data can be protected during transfer according to requirement of healthcare by using an adapted PKI for healthcare. To extend a picture archiving and communication system (PACS) for integration in a PKI, the internal scheme of a directory service must be adapted to the definition of that PKI as well as the PACS has to be modularized into components.*

## INTRODUCTION

Securing the infrastructure of telemedical networks is important in order to protect privacy of patients. IT Security is traditionally divided into the concept of confidentiality, integrity and availability (1) and includes the classical computer science data process taxonomy of transport, storage and processing. Encryption helps to provide confidentiality.

You can integrate encryption in an algorithm which uses wavelets to compress data. Wavelets are more useful in image compression  than other methods. This is because the definition about which data should be left out is more flexible. This adaptation of wavelets to specific features of images leads to acceptable results. The use of computers in image transfer will increase further and it will therefore become necessary to transfer image data quickly. In addition, a protection of the image against unauthorized access will become necessary. Image compression increases the amount of time needed for transferring an image. Regarding the area of telemedicine, there is a demand for the protection of images. The reason for this demand is the need to prevent the relationship between patient data and an image from being determined. Therefore, the approach intends to describe a combination of  image compression by using wavelets and to integrate encryption into the wavelet-transform and -compression procedure. Another method to provide confidentiality is to integrate digital data in other digital data. Furthermore, the case of a pre-existent database which contains objects describing the owner of a multimedia element and image's features will be examined. A trusted party adds this information to an entry in its database and performs a hash over the data of the multimedia element. Additional operations will be performed to extract the main features of the multimedia element.

These definitions are independent from the kind of implementation or use of programming languages. We use an implementation which integrates a secure transfer of data in an existing system by using the transport layer security (TLS) and Java.

In the age of digital medicine, a growing need for secure transfer and storage of patient data is obvious. In medical science, the design of a PACS (picture archiving and communication system) is essential for storing digital images. We describe an alternative method of integrating encryption as a DICOM(digital imaging and communication in medicine)-conform mechanism in a PACS and via a DICOM-conform directory service in a HIS (hospital information system)/RIS (radiological information system). It is useful to integrate these systems in order to be able to merge existing patient data with DICOM images (3). In order to sign, mark, encrypt data you can use certificates. A certificate bind data important for identification to the public key. The next section will describe one method to manage certificates.

## WEB OF TRUST

As a signature and cryptography solution, you can have it very early in a program. PGP certification locations are not concurring with the signature law and they have some security problems in the newer ADK (additional decryption key) functionalities. The newer and the older versions of GnuPG are freeware and without ADK and 'Klima Rosa problems'. PGP is the abbreviation of "Pretty Good Privacy". The standard RFC 2440 defines all important conventions of the elements of PGP which are to describe. PGP and GnuPG (a related form of PGP) make it possible that messages can be exchanged without lost of privacy, authentification and comfort. To be able to send messages, they will be coded with the corresponding public key of the addressee. Then the adressee can  decipher the secret key.
The advantages of PGP are secure communication between persons who did not have to have meet yet. A bug-proof channel for the exchange of keys is not needed because of the asymmetric coding procedure.

Moreover PGP is fast, enables digital subscribes, offers a very well key-administration, compromises data and slits it if necessary to send the e-mail faster. PGP can be used nearly on every operating system. PGP combines two coding procedures: a symmetric procedure and the public-key-procedure. By coding the message with the private-key of the sender, the recipient (who possesses the public-key) can say with security that the message comes from the sender (provided that no one else possesses the private-key of the sender). So the recipient can determine the hash-code of the message, decode the message (with the public-key) and compare both hash-codes. In addition to the name and the e-mail address each PGP-key has a code which is derived from generated key data of the program. This code uses PGP internally (that means without the knowledge of the user) to distinguish between the keys. PGP (version 5.x/6.x/7.x, OpenPGP, GnuPG) uses the last 62 Bit of the public-key, from which only the last 32 Bit are shown, e.g. 0x6ce93239. That is because an attacker could calculate the next keys which will be generated by PGP or the last keys which were generated by PGP. The keys are stored in so called "key certificates" which have in addition to the key a short text with name and e-mail/netid (user-ID, unicode characters are usable since version 5) of the possessors and a notice of the date when the key was created. So more entertaining keys with a longer valid key (master key) can be subscribed. Distinguishing algorithms can be used in different keys for subscription and coding. There is an innovation since the version 6.5.1i of PGP. Such as noticed before, the subscription of a key expresses the trust in the validity of the key and the possessor. Well-known (only partly banned) security-problems of PGP are the "ADK-Gau" (documented on 23/24.08.2000). ADK/CMRK-K means Additional Decryption Key and is an additional key on which will be coded (inevitably) in addition to the recipient.

In the following more application fields will be mentioned. PGPdisk is a PGP application with which CAST-128 coded container-data can be used which are remained as an additional drive. PGPfone enables the coded phoning via internet (not in PGP 7.0.3). PGPnet is a more or less efficient firewall-implementation with PGP. In the „Web of Trust", on which PGP (Pretty Good Privacy) is based, each user is responsible for himself which certificates he trusts or not. He fixes it by confirming trustful certificates by his digital subscription. Other users can look in each certificate who subscribed this certificate before. If a user decides that he trusts every certificate which are subscribed from a certain person, a position of trust occurred. As each user can decide this position of trust for himself, a web like structure will be created which is called Web of Trust.

In the following PGP will be compared with the X.509 standard. X.509 uses an directory orientated procedure to administer the certificates while PGP uses a flexible (easier reproduction of a structure of a company) internet-orientated (network like) but a difficult to use procedure (→ figure 1).

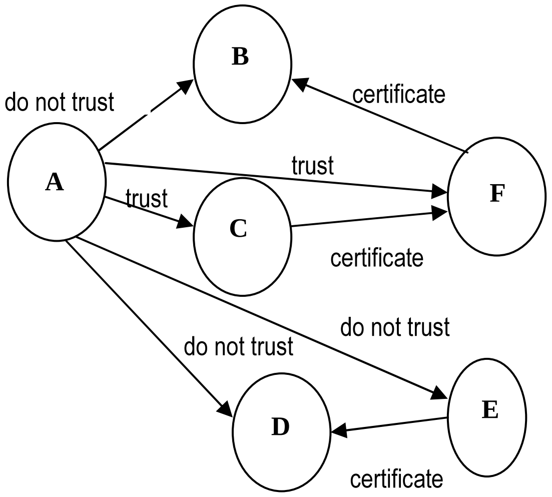

Figure 1. Example of a PGP-trust-security

In contrary to X.509 PGP uses nested signature procedures by using a certificate chain.

## HIERACHICAL PUBLIC KEY INFRASTRUCTURES (PKI)

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, like the web of trust. 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.

A trustcenter uses a registration position in which all personal data which are important for the content of a certificate will be took up. (The diagram on the next page shows the scenario which will be described now.) The person who considers to the data, that is the applicant, will be identified and proofed in the RA. That can be done with the help of his identity card or in a different proper way such as for making certificates for employees of a concern, only a confirmation of the personnel office is needed that all for a certificate needed data are there. The applicant receives the general terms of trade and an explanation about a responsible treatment with his certificate. For the attention the applicant subscribes the document.

The trustcenter has now the task to create a secret key which no one knows, the applicant not either. Preferably the creation of the secret key occurs together with an appropriate public key on the card. So the card as a "standard service" has to offer this key creation for the usage in a trustcenter.

In the following course the public key remains in the trustcenter. Out of the public key a digital certificate will be created together with the personal data of the applicant. That certificate will be made accessible for the applicant so that he can save the certificate on his card on which the secret key is and which was send to him by the trustcenter. Now the applicant can decide who should get his certificate in addition to the trustcenter.

The applicant can use the certificate now to sign and/or to code data. The checking, whether the certificate is valid, will be took over from the directory service of the trustcenter which issued the certificate. In the ideal case there is a worldwide directory service which has got the Certificate Authority as directory. A certificate guarantees certain access rights in this directory. In reality there are more directory trees which are linked by "cross-certificates". In the case of "cross-certificates" the (policy-) certificate instances of the trustcenters exchanges certificates so that the access to their directories are guaranteed for another policy-certification-instance and so that the other directories can be added to themselves. An example is the merger of two companies.

It is conceivable that one person made applications at different trustcenters. The secret keys and certificates could be saved on one card. As "cross-certificates" are not the rule, multi-function cards offer an alternative.

To be able to proof the validity of the certificates and so that the directory service of the certificate instance which issued the certificate will not be overloaded, sub-certificate-instances will be created by certification. These sub-certificate-instances contain all necessary information about that user group which have to administer them.

To be able to proof the validity of the certificates, so called Certificate Revocation Lists or shortly CRL were introduced. The idea to administer directory services out of browsers was favoured by the LDAP (Lightweight Directory Access Protocol). LDAP is based of DAP (Directory Access Protocol) which is a simplification for the standard X.500 [X500]. The following diagram shows an example how LDAP can be used. By adding TLS (Transport Layer Security) which is based on the standard X.500 [X500], the connection between client and server is guaranteed. To be able to fix the group affiliation of a person by login and password, this person has to apply a certificate at a certificate instance. An example for a certificate instance is Verisign. This certificate instance put a free certificate for 60 days at disposal with the help of which e-mails can be signed (digital subscription) and coded. The condition for the coding is the S/MIME (Secure MIME)-mechanism.

In the same way the certification-administration takes the role of a certificate instance. The certificates of persons, directory service and certification administration contain all the distinguished name (dn) of their possessors. This dn helps to put the enrolled server or person into the hierarchy of the directory service and is composed of knot identifier in the directory tree. By the dn the role of the possessors of the certificate will be defined.

The directory service is not only used for the administration of the certificates but additionally for the administration of user rights. So in the case of the registration with the help of a multifunctional card, it is proofed first if the certificate which is on the card is valid and after that if the resources are free on which the possessor of the card has access. The construction which is shown in the diagram is based on the components of Netscape Suite Spot. For configuration in this system the administrative component such as a component serve for the scaling and adaptation of the system to a certain purpose. The directory service administers internet clients which make applications for resources allocation with the help of multifunctional cards.

## USE OF A PKI IN HEALTHCARE

In health care environments, PKI uses authentication, encipherment, and digital signatures to facilitate confidential access to, and movement of, individual health records to meet both clinical and administrative needs. Interoperability of PKI technology and supporting policies, procedures, and practices is of fundamental importance if information is to be exchanged between organisations and between jurisdictions in support of health care applications.

The technical specification for a health care PKI applies to the health care industry both within and between national boundaries. It is intended to cover public health authorities, private health care providers across the entire range of settings including hospitals, community health and general practices. A PKI should also apply to health insurance organisations, health care educational institutions and health related activities (such as home care). The aim is to develop a framework where health professionals, health care organisations and insurers can securely exchange health information. The new part of DICOM's security enhancement is also intended to provide consumers with the ability to securely access their own health care information.

Major security threats that need to be addressed in health care information and communication systems are unauthorised access gained through stealing the private key of a legitimate relying party and then masquerading as that relying party. Public key cryptography uses two different keys, one public and the other private. Competent private key management is therefore critical to the successful functioning of any PKI within the health industry. If the private key is compromised, the PKI is no longer effective in protecting information communicated and stored using that particular public/private key pair. PKI describes the relation between a key holder and a relying party, including a Certification Authority (CA), which allows a relying party to use a certificate relating to the key holder for at least one application using a public key dependent security service. A PKI consists of a:

- **Certificate Policy**

Certificates based on a certificate policy, which are specifically designed to meet the needs of health care Information, support services such as authorisation, access control and information integrity.

- **Certification Practice Statement (CPS)**

This is a statement of the practices that a certification authority employs in issuing certificates to implement the Certificate Policy.

- **Certification Authority (CA)**

A Certification Authority (CA) is a trusted entity that verifies the identity of a relying party, allocates a Distinguished Name to that relying party, and verifies the correctness of information concerning that relying party by signing the data and in doing so verifying the binding between names or identities and public keys, which constitutes the digital signature for that relying party.

- **Registration Authority (RA)**

An RA is an entity that establishes the identities of relying parties and registers their certification requirements with a CA. [ISOTC215/WG4 Glossary of Security Terms]. An RA may also verify a relying party's role, rank or employment status for information that may be stored on an attribute certificate.

- **Attribute Authority**

An Attribute Authority is an entity that establishes the attributes of relying parties and certifies these attributes by issuing attribute certificates. Certificate Distribution (and Revocation) Systems Establishing Identity Using Qualified Certificates Establishing Specialty and Roles using Identity Certificates Patients/consumers may use different physicians for different health issues. As a result, a decision to grant a health professional access to particular parts of a patient/consumer's health record is usually based on that health professional's specialty.

## PREPARE THE PKI FOR APPLICATIONS USED IN HEALTHCARE

As an example for emergency department access to records in conjunction with a PKI serves the access of patients health plan site over the Internet by using the information on the health plan card in presenting digital certificate identification of current role as an physician. In Tele-Imaging the physician accesses during viewing the images on her workstation also the health care institution's clinical information system over the Internet to review other medical information on the patient.

Attribute Certificates are used for Authorisation and Access Control. Detailed authorisation information is appropriately supplied by using an attribute certificate that is bound to the health professional's public key. A health professional may have many attribute certificates that reflect multiple roles.
In order to provide a modular PACS system with the features of a PKI, we have to modularise the PACS.
Each module contained a certificate and is signed. If two modules want to communicate the modules exchange and verify its certificates and signatures at the system which provide these modules. Afterwards, the modules establish an encrypted communication line. If the number of modules increase the "web of trust" is not suitable, because the certificate chains become to large.

## CONCLUSION

Regarding DICOM, applications are not able to decide if it trust other applications or not. Therefore, the directory service is a better choice than a "web of trust" to implement this PKI. To extend a picture archiving and communication system (PACS) for integration in a PKI, the internal scheme of a directory service must be adapted to the definition of that PKI as well as the PACS has to be modularised into components. Each component is considered as a certificate owner which is able to communicate with other components of the PACS by using encryption and digital signatures. Digital signatures are used for logging purposes. The X.509 specification which defines the structure of certificates has to be extended by attribute certificates in order to implement a certificate which meets requirements of DICOM when using current standards. The confidence of certificates will be granted only by the user, signing the certificates.

## References

1 Charles P. Pfleeger, Security in Computing, 1989, Prentice-Hall International.

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

3 Constructing a secure HIPACS with Structured Reporting, Vorwerk L., Losemann F., Engel T., Meinel Ch., Medical Imaging 2000, PACS Design and Evaluation: Engeneering and Clinical Issues, G. James Blaine, Eliot L. Siegel, Sandiego, USA, SPIE, p. 335-342, Volume 3980, 2000.

[1] Europacs 2002 , Oulu Finnland, Niinimäki J., Ilkko E., Reponen I., Oulu University Press, p.66-69, 2002.