# Secure and Cost-Effective Exchange of Cardiac Images over the Electronic Highway in the Netherlands

A Kleijhorst, E T van der Velde,
M H Baljon, M J G M Gerritsen, H Oon

University Hospital Leiden, The Netherlands
ICIN, Interuniversity Cardiology Institute of the Netherlands

## Abstract

*Today, in many catheterization labs the images are processed and stored in digital format. This creates the possibility to transfer the images electronically between an university cardiology centre and referring cardiology centres. Electronic exchange of images will reduce waiting time and costs involved with physically sending cine films or cd-roms to other centres.*
*However, the electronic exchange of images poses two big challenges:*
*- The safeguarding of the privacy of the patient-related information.*
*- The handling of large amounts of data.*
*These challenges can be met by using encryption algorithms and efficient data reduction methods.*

## 1. Introduction

As more and more catheterization laboratories change from cine films to digital storage, the possibilities grow to duplicate, send and store the images in a more efficient way. Several University Hospitals in the Netherlands are working together to develop an image server which will function as a (low-cost) PACS system (Picture Archiving and Communication System), which will also include the option to transfer images to other hospitals [1].

This project, called 'Escarin' (Electronic Superhighway for CARdiac Information in the Netherlands) is co-ordinated by the ICIN (Interuniversity Cardiology Institute of the Netherlands).

The image server consists of a large capacity hard-disk on which the images are stored in DICOM-3 format and a database with reference information to the files. This database is used to facilitate the search for specific image runs of a patient.

A client application has been developed to access the stored images. With this application the user can select runs on a CD and copy them to the image server. It is also possible to view the runs which are stored on the image server and to select runs to be sent to another hospital.

### 1.1 Transmission of the images

There are two important issues involved with the transmission of medical images over the Internet:

- How to achieve an acceptable transmission time
- How to maintain the patient's privacy

The transmission time is related to the large amounts of data that have to be transported, and the limited bandwidth of the Internet.

The second issue is related to the possibility of eavesdropping the communication lines and thereby retrieving personal information of the patient stored in the image file(s).

## 2. Methods

To deal with the issues raised above, the following solutions have been or will be implemented:

1. use of daemons,
2. data reduction and
3. data encryption.

### 2.1 Use of daemons

To avoid the sending user from having to establish the connection manually a send- and receive daemon have been developed. Both daemons take care of the complete transaction, so the sending user only has to issue the order to send and the receiving user can view the images a

0276-6547/97 $10.00 © 1997 IEEE

couple of minutes or hours later, depending on the bandwidth and the number of images sent. The send daemon sends the requested runs and will try to re-establish the connection when it gets lost. When all the runs have been received, the receive daemon updates the database and moves the files into the right place on the large capacity hard disk.

## 2.2 Data reduction

To reduce the amount of image data that has to be transmitted, the following data reduction options are available:

- The user can select and transmit only the runs that are relevant
- The user can select only part of a run; with these selected frames a new DICOM file is created which then is transmitted
- The image files can be compressed before transmission; compression can be lossless or lossy

## 2.3 Security

The three topics in security in the context of medical informatics are:

- confidentiality,
- integrity and
- availability.

In the Escarin project, confidentiality of the transmitted data has been secured by encryption of the data; integrity of the data has been secured by adding a digest of the original message and a digital signature of the sender. The availability of the data is taken care of by use of reliable hardware and database technology.

Data-encryption

During the transport of the DICOM files, non authorized people might try to eavesdrop and read patient related data. Proper encryption of the data can prevent these kind of attacks. Two important encryption algorithms have been implemented:

- DES algorithm (Data Encryption Standard)
- RSA algorithm (named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman)

The DES algorithm uses one key to encrypt and decrypt a message, so the sender as well as the receiver need access to this key. This means that there has to be a secret exchange of the key between the sender and the receiver.

With the RSA algorithm this need for secret key exchange has been solved by using a so-called key pair. This key pair consists of a public- and a private key. A message encrypted with the public key can only be decrypted with the corresponding private key.

The owner of the key pair has to distribute the public key and keep the private key secret. In this way everybody can send a message encrypted with the public key and only the owner of the private key can decrypt the message, so a secret exchange of a key is unnecessary.

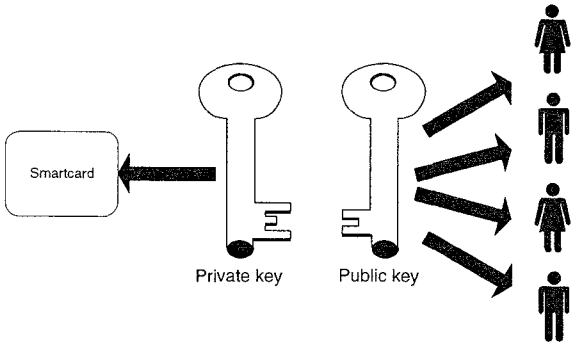


Figure 1. Public and private key distribution

However, because the RSA algorithm is fairly slow in comparison with DES, a mixed approach is taken: every time a message has to be encrypted, a DES session key is generated. This key is used to encrypt and decrypt the message. The DES session key itself is encrypted with RSA using the public key of the receiver. The result is attached to the message.

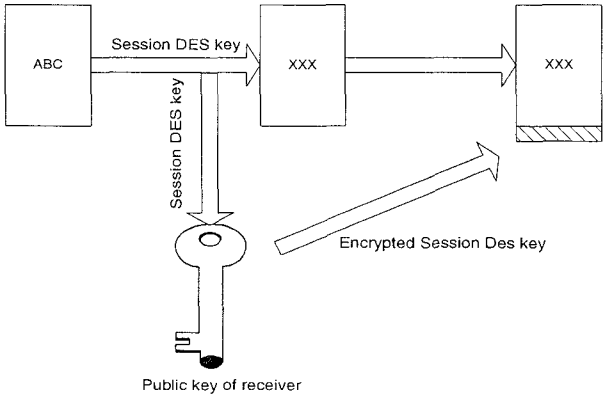


Figure 2. Encryption process

When the message is received first the attached RSA encrypted DES key will be decrypted with the private key. The resolved DES key will be used to decrypt the message itself.

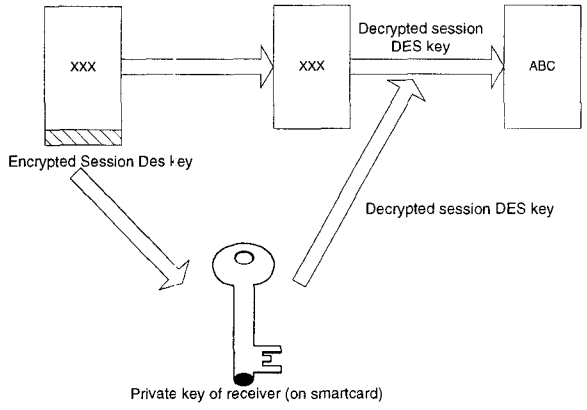

Figure 3. Decryption process

Data-integrity

The private key can also be used to sign a message. Suppose person A wants to send a message to person B. Person A uses the public key of B to encrypt the message and uses his own private key to sign the message. When person B receives the message he can check the digital signature with the public key of person A and decrypt the message using his own private key. In this way person B is certain that the message has been sent by person A.

The RSA algorithm also provides a tool to ensure the integrity of the file. It is possible to generate a fingerprint of a message. The receiver can verify the received file by calculating the fingerprint of the received file and comparing it with the supplied fingerprint. If they do not match it is evident that the file has been changed during transport.

So with RSA it is possible to both check the identity of the sender and to guarantee the integrity of the files.

## 2.4 Smart cards

There are several products available which support RSA in combination with DES encryption. There is a freeware product called PGP (Pretty Good Privacy) and a system which uses card readers and smart cards to encrypt and decrypt messages.

The management of keys has been organised differently between PGP and a smart card system. PGP stores the keys in files. These files can get lost, duplicated or corrupted. With the smart card system the private key is stored on the smart card and the public key can be stored in the database. In this way the user doesn not have to manage his own keys, he receives a smart card which can not be duplicated or corrupted.

Another important advantage of the smart card system that we have used is that it is implemented as a DLL, Dynamic Link Library, and not as an executable like PGP.EXE. In this way the encryption can be easily integrated in the send and receive daemons, just by calling some functions which are stored in the DLL. In this way it is not necessary to switch to another program.

## 3. Experiences

The Escarin system is in the process of becoming operational. During demo's and acceptance sessions to the prospective users the functionalities have been accepted quite well. Escarin seems to offer a good solution for practical problems related with the handling of cine films. Cine films may get lost when shipped to another hospital and the film can be needed in both hospitals, but copies can not be made. That the Escarin exchange of images over the Electronic Highway solves these problems can be made clear to the users easily. The data reduction functionality was less appreciated.

Some cardiologists appreciated the possibilities to send only a selection of the relevant image runs to prevent unnecessary delay. However other cardiologists or thoracic surgeons were concerned to miss some runs if not the full study would be sent, and therefore would prefer to send all images. This is of course possible but may take a lot of time.

## 4. Discussion

Presentation of the Escarin concept in the Netherlands gave rise to two main discussion points:

- The data reduction option to cut a number of frames out of a complete run is thought to be illegal in a DICOM conformance setting, because it may mislead the clinician who views the incomplete run.
- Internet is thought to be inherently insecure since any encryption method can be decoded.

## 4.1 Data reduction debate

When transporting cardiac images over the electronic highway there are three possibilities to deal with the throughput limitations.

The first option is patience, start the communication in the evening and expect the images to have arrived the following morning. A send and receive daemon will take care of this process during the night.

The second option is to increase the bandwidth. At this moment that means use of a peer to peer 30 line ISDN connection or ATM. This will mean an increase of

expenses, which can not be always justified. At this moment several test connections are being implemented between University Hospitals and referring centres using peer to peer 2-line ISDN connections.

The third option is to reduce the amount of data by using lossy or lossless compression, by selecting part of runs, or by a selection of complete runs. Lossy compression however is not yet in line with the present DICOM standard. The selection of a sequence of frames of a run is not supported by the DICOM standard and can be a dangerous process [2]. So the selection of complete lossless compressed runs is the only officially allowed option.

In the Netherlands however there appears to be a wish for selecting partial image runs, so maybe a thorough international investigation will reveal the same need in other centres. Maybe this will lead to an extension of the DICOM standard to support selection of frames within a run. The same applies to the option of exchanging lossy compressed images which is the subject of a large study presently in progress [3].

## 4.2 How safe is encryption

In the Escarin project two encryption algorithms are being used, the DES and the RSA algorithm, and only one has to be cracked to retrieve the original information. So in this paragraph the safety of both algorithms will be discussed.

The DES algorithm is used in Escarin to speed up the encryption and decryption process. The DES procedure has been endorsed by the government of the United States as an official standard in 1977 and has never been broken since. A lot of efforts have been made by scientists to find a way to break DES, but it all ended in using exhaustive search. Other attacks have been tried to break DES, which resulted in the announcement of the so-called differential cryptanalysis. This technique requires the encryption of 2^47 by the attacker chosen plain texts, therefore this method doesn't form a serious threat for DES. The most practical way to crack DES is using exhaustive search, but that requires a lot of money and time. To make things even more difficult for possible hackers is the Triple DES technique. It uses three different DES keys to encrypt the message in succession, so the first DES key encrypts the file, the second key encrypts the encrypted file and so on.

DES encryption therefore can still be regarded as secure until techniques have been found to break it without exhaustive search. The same story also applies to RSA encryption. Most people think that when computers become faster and more powerful it will be easier to break the RSA encryption technique. This is not true because with a faster and more powerful computer it is possible to generate larger keys, and therefore the job to decipher the encrypted message will be tougher.

## 5. Conclusion

When demonstrating the Escarin solution to several clinicians it became apparent that the functionalities of the system were highly appreciated. Several discussions were raised about the open architecture of the Internet in relation with patient data and the data reduction methods. Some clinicians prefer to spend money to increase the bandwidth to be able to transfer complete studies in a reasonable amount of time. Other clinicians liked the extensive selection functionalities to reduce the transmission time.

The Escarin solution is being implemented in several University Hospitals as a test site, using peer to peer ISDN-2 connections. When more experiences with the system have been acquired the first Internet connections will be established.

The smart card system offers a cheap and secure solution for each implementation site. Based on standards like DICOM, RSA and DES a cost effective product has been developed.

## References

[1] Dijk W A, Heijer P den, Visscher K J, Haagen F D M, Festen M J J, Kolkman W J M, Velde W van der, Dassen W R M and Crijns H J G M. Evaluation of a DICOM-3 Link Between a Referring and a University Hospital. In: Computers in Cardiology 1996. Indianapolis

[2] Baljon M H, Gerritsen M G J M, Rappard F van and Putten N van der. A DICOM Profiler for Modelling and Checking DICOM datasets. In: Computers in Cardiology 1996. Indianapolis

[3] Koning G, Meurs B A van, Haas H, Reiber J H C. Effect of lossy data compression on quantitative coronary measurements. In: Cath and Cardiovascular Diagnosis 34, 1995, 175-185

Address for correspondence:
Anja Kleijhorst
Dept. of Cardiology, University Hospital Leiden
POBox 9600, 2300 RC Leiden
The Netherlands
E-mail : kleijhorst@cardio.azl.nl