SECURE ACCESS TO MEDICAL INFORMATION BY SMART CARDS

R. BEUSCART (MD, PHD) (*), C. GRAVE (MD) (**), P. GEORGE(*)

(*) RD2P (Recherche et Développement Dossier Portable)
Hôpital CALMETTE - 59037 Lille Cédex

** DIM - Rez-de-jardin - Hôpital CALMETTE - Bd du Pr. LECLERCQ
CHRU de Lille - 59037 Lille Cédex

Summary :

The recent development of Medical Information Systems is due to the connection of medical data bases through networks.But this development emphasizes the problems of security and confidentiality of medical data.

This security requires the implementation of three complementary functions : identification-authentication, signature, encryption. The smart card is a possible tool for this security because of its micro-computer and RAM Memory. The most frequently used algorithm is TELEPASS. Recently, standard algorithms (RSA and DES) were implemented in enlarged memory cards. The Professional Access Card (CPS in France) and specific "Key Cards" are vectors for the generalization of security statements in the medical domain.

Key words : Smart card , Security , Tele - Medicine , Communication systems

Introduction :

The management of medical information is more and more realized through computer systems. Hospitals are developing Hospital Information Systems for the archieving of medical records and for the communication between medical units, labs, X-Ray departments, administrative boards. The development of telematics and public networks (LAN or WAN) makes possible the transmission of medical information and the synchronous as well as asynchronous exchanges between physicians.

But these new technologies arise general problems concerning the confidentiality and the security of the transfer of medical data.

I. LEGAL AND ETHICAL CONSTRAINTS.

The rules concerning the security of the transmission of medical data between medical units and physicians are widely different from one country to another. In France, the Commission Nationale Informatique et Libertés (CNIL) pointed out at the following points :

1) It is recommended to use and to send a record number and not the patient's name. If necessary identity items must be encrypted.

2) For sensitive applications in the medical domain (Psychiatry, AIDS, Blood-diseases) it is recommended to use identifications and authentication by smart card (micro-processeur card).

3) If the results of blood analysis are send through the network , automatic correction of errors must be possible.

These recommendations are necessary both to protect the medical information of the patient and to guarantee the indepedance of the physician towards health care institutes and insurance companies.

The electronic signature is also possible by means of smart card but legal constraints are limiting this use. In fact, only the manual signature is recognized as legally valid.

In summary, there are 3 constraints for a wide use of telematic networks in the health care domain :

- Identification, authentication,
- Security of the transfer of data,
- To avoid the fraudulent use of medical information .

II. PROFESSIONAL ACCESS CARD.

II.1 Micro-processor cards.

A smart card (or micro-processor card) is made of :

- A micro-processor;
- Three memories.

. RAM memory for temporary storages of information during the calculations and the operations of the micro-processor.

. PROM memory for fixed programs written when the card is manufactured.

. A programmable memory [EPROM or EEPROM], empty when the card is manufactured, containing the new information necessary for the users of the card. The capacity of this memory is variable from 1024 bytes to 64 kbytes. This part of the memory is divided in a number of zones the access of which may be :

- Free,
- Confidential (they are protected by a secret code),
- Secret (only the micro-processor of the card can have access to this information).

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

The chip is fixed under a metallic patch and the link is effective by means of six contact points for asynchronous exchanges.

II.3 The professsional Access Card.

In the first experiences of Patient Data Cards in Europe, the access to sensitive information was protected by the use of a "key" card, distributed to the professionals who would take the patient in charge : physician, nurse, chemist, physiotherapist... But the rights for reading/writing were different according to the profession of the owner. A physician could read and write all the areas of the patient data card whereas the nurse could only read emergency and historic information.

The French Ministry of Health has decided to generalize the use of the smart card as a professional access card for :

- The identification and authentication of the owner,
- Securtity of data,
- Coherence of the cards systems.

III. SECURITY FUNCTIONS

The security functions are assured by the micro-processor smart card using specific algorithm for indentifications of the owner but also to secure data transfers between medical units.

III.1. The TELEPASS example.

One of the most common algorithm is TELEPASS which has the following functionalities :

- The algorithm corresponds to a program or a function F, stored in the micro-processor with secrete data S written in the card and confidential data In written by the responsible of the specific application. We can take 2 examples of the use of the "TELEPASS" smart card :

1) Authentication

If n persons are authorized to access to the application "X", each person has a card with :

- Program F and a personal code
- A secret number S
- The identity In of the bearer.

When the card is introduced in a reader, then the system reads the identity In of the bearer and sends to the card a random number R. Then the micro-processor of the card computes :

$$A = F(S, In, R)$$

and sends this result to the system which has the list of the n authorized clients. Then the system computes A'=F(S, In, R) and verifies the equality : A=A'. The key 'R' is secure as the random number R is generated every time ; if K and R are 64 bits long, then the risk of rutilizing the same key is 10^{-9}.

2) Encryption.

The system sends C and the random number R. At reception, the calculation is the following one :

$$K = F(S, In, R).$$

The decryption function of C is :

$$P = dK(C)$$

So a smart card is, with a simple algorithm, a very secure method for identification, authentication, encryption or decryption of confidential data as medical information.

III.2. RSA and DES.

Recently, smart cards with higher RAM memory size, permitted the implementation of higher level algorithms.

. The RSA (Rivest, Shamir, Adleman) algorithm uses the following function : When X wants to send the m message to the user A, them it computes : (m^p mod n) and sends this result to A. Only the user A may rebuild m using the secret exposant s to calculate :

$$m = (m^p \text{ mod } n)^s \text{ mod } n$$

This RSA algorithm exists on specific smart card as MIMOSA (Gemplus)

. The DES algorithm was obtained by arrangement of several encryption functions. DES is the "Data Encryption Standard" published as a Federal Information Processing Standard n°46 in 1977. In the DES algorithm, encryption and decryption use an algorithm on data blocks of 64 bits, under the control of a 56 bits key. A block is submitted to an initial permutation, then to a complex calculation (depending on the key) an then to an inverse permutation.

IV. CONCLUSION

Smart cards, because they are equiped with three types of memory and a true micro-computer, are effective and secure ways to ensure the confidentiality of medical data. The principal possible functions are :

- Identification
- Authentication of the bearer by means of a secret code
- Electronic signature
- Encryption and decryption of electronic mails.

The recent availability of classical algorithms as DES or RSA on the smart card reinforces the potential of smart cards as a key acces to medical information.

REFERENCES :

R. BEUSCART and P.C. PARADINAS
Smart cards for Health Care
In "Telematics in Medicine" J. Duisterhout ed.
p. 357-367. - North-Holland, 1991.

J.M. LAMERE, Y. LEROUX, J. TOURLY
La sécurité des réseaux - p. 294-300
Dunod ed. Paris (1987)

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.