# SMART CARD APPLICATIONS IN SECURITY AND DATA PROTECTION

by Jean GOUTAY Président de la Société INFOSCRIPT

## INTRODUCTION

The several security elements of the smart card are based on phisical and logical barriers.

- Materially, the smart card is a monolithic component including a microprocessor and a memory of 8 K bits, this memory being indelible.

  .In addition entry test points have been destroyed before activating the smart card.

  .In practice it is impossible to read, modify or duplicate the contents of the smart card.

- Logically, the chip is able to memorize the different wrong access attempts and invalidate the electronic circuit after three repeated attempts for example or N attempts on the whole.

  Let's see in addition that the dialogues between the chip and the exterior depend on a random value, which is a known element of security and a protection against the passive intrusion and possibilities of simulation.

- What are the uses of the smart card, specially in matter of protection of information and more generally in security ?

  They concerned : Identification
  Authentication
  Enciphering and key management

  They allow the security of :
  - The access to premises or to a network
  - the payment at P.O.S. or at distance
  - the transmission in networks, electronic messeging for instance
  - access to services such as: broadcoast videotex or toll TV, interactive videotex, database.

First let's look at the different uses of the smart card.

### 1. Portable Protected Data

- The smart card contains a memory not very big (from eight to sixteen K) but protected against the exterior by a microprocessor (or a firmware) and it is possible to store in it clear confidential data. These data will be accessible only on production of a secret code.
  The applications are : protected portative file such asmedicine, student portable file, ...

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 459-463, 1985.

- However the smart card is able probably to encipher short messages, store and transmit them.
  In particular this system can be used for sending enciphered keys at distance.

## 2. Identification

Thanks to the content of the secret and inviolable area in the smart card, thanks to computation which remains with in the card, it is possible to verify a personal code with a very good security and so to identify the card's bearer.

But a better identification can be obtained by a more secure storage of patterns bounded with physical characteristics of the person, such as :

- the finger prints
- the speech
- or the dynamic signature.

## 3. Data Authentication

After data compression by an algorithm (hash code, ...). it is possible to compute and to store in the smart card an "electronic signature", function of this compression and of the transmitter identity. In another connection this signature is added to the original text, a fact wich permits the verification.

This process can apply for the certification of accountant, original documents, banking orders and transfers, files and software, at different levels of development for instance.

## 4. Software protection

In matter of software protection, several systems can be envisaged, wether at the transport level with the encipherment of the software and the deciphering key stored in the smart card
or at the level of running with computation elements in the program requiring the presence of the smart card
or with holes in the program which can be restored with the smart card only.

It is easy to see the applications in the domestic computers area or in the area of video cassettes.

We can see in this case that decoding must be put at the monitor level.

Now let's see other applications.

## 5. Reciprocal recognition and access control

A simple algorithm computed in the card permits verification, with a random value E , that the two cards are well matched, e.g. $R_a = R_b$.

Whether in the case of the access control to premises, or a network or a data base.
In the network case, every passive intrusion on the line does not allow either listening or simulation or re-use of the dialogue, the informations being completely random.
In the case of access control, the combination changes at every access because the key R is fugitive.

## 6. Card authentication by general system

Another application can be the recognition of the smart card by the system, that is to say it's authenticity, based in theory on public key use.

Using a random message M , the system computes
C = f (M), f being the public key.

C is transmitted to the card which contains the secret part of the function.

The big advantage is that the system, which can be a general public terminal, doesn't require any secret function.

So in the case of electronic payment at point of sale, the system verifies :
- the authenticity of the smart card and of the bearer
- the guarantee limit
- possibly the black list.

Let's see in this case that the card allows the management of several access codes : banker code for the valorization, bearer's code, service providers codes ...

But the possibilities of the smart card are even more interesting in the networks, in matter of security.

In addition to the previously described functions, they allow the automatic logging the management of preloaded credit fields and if they can't encipher at this moment they provide solutions to the delicate problems of key management.

## 7. Exchange ol enciphered data

With a generator of enciphered bits and a random number E , messages can be enciphered thanks to the smart card along a network, with keys R which can be changed at a desire frequency.

In particular the enciphering algorithm A can be very simple.

This system can be set up on any encipherment equipment in networks and provides a solution to delicate problems of key transportation.

One application is given in electronic mail where the cards are used for reciprocal identification of interlocutors and encipherment of informations by fugitives keys.

Let's see now very present applications.

## 8. The telepayment

The first wordwide experiment of telepayment has been in Velizy, near Paris, "TELETEL" and allows a suscriber to make from a vidéotex terminal, the minitel :

- the bank statement display
- the remote cash transfer
- the telepayment of goods providers
  as retraiters La Redoute .

The smart card (with it's reader) consequently permits :

- the sure identification of the suscriber
- the encipherment of messages on line and generation of "certificates" ensuring it's integrity ang giving the proof that the information is well registered in the card.

All is in an environment at distance non controlled.
The security of the system is based on the exchange of fugitive random keys.

Another system of telepayment wouldbe possible.

With the use of public keys and the signature of the messages by a secret key of the user, whose the public part, signed by the key of the bank, would be transmitted previously by the user. This system does'nt require any black box at the central processor.

## 9. Protected electronic messaging.

General systems can be envisaged to protect in addition informations during the storage in the mailbox of the service computer.

It is possible for example to encipher on line the data, and to decipher them immediatly with synchronous mode, finally to encipher again with another key for the storage.

It would be possible also to envisage another scheme with the use of public key for authentication of the transmitter, but also for transportation of the random key the message being enciphered it self with this key changing at every message.

## 10. Broadcast interactive vidéotex

In the case of access to toll services, whether broadcasted programs or videotex services or data base, we have two possible systems :

- one using the preliminary enciphering and decoding informations thanks to the smart card for those who have paid?
- the other one (pre-payment) permitting the access to the services after having destroyed bits area in the card, previously credited.

In conclusion, by its vast possibilities not yet explored, the smart card open new vistas in matter of security, networks and data protection.

Thank you for your attention.