SMART CARDS AND CONDITIONAL ACCESS

Louis C GUILLOU

Chef du département "Accès aux Services et Protocoles"

Centre Commun d'Etudes de Télédiffusion et de Télécommunications
BP 59 F35510 CESSON SEVIGNE
FRANCE

Synopsis : Smart cards are introduced through chip design, card interface, and card security. Applications are divided in three classes : log books, certified records, key carriers.
Conditional acces is analyzed with a clear distinction between entitlement checking and entitlement management. The key carrier CP8 card is then described. Smart card cryptology is examined, and also the probable evolution towards digital signatures.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 480-489, 1985.

I - INTRODUCTION TO SMART CARDS

According to ISO (International Organization for Standardization), an IC (Integrated Circuit) card is an ID (Identification) card including in its thickness (.76 mm) one or more integrated circuits.

An IC card is "smart" when the integrated circuit is a microprocessor, with processing power combined with permanent storage capacity. The operating system in the microprocessor controls and manages all the accesses to the electrically programmable memory.

I.1 - Chip design

The first step in the design of a dedicated chip for smart cards is to choose some central processor unit and some EPROM technology (such as UV-erasable REPROM, and soon, single voltage EEPROM). The CPU must be redrawn in the EPROM technology.

The design of the buses must allow EPROM self-programming under control of the operating system in masked ROM. Various traps and mechanisms must be introduced to increase physical security and to facilitate tests during the manufacturing process.

The CP8 chip, till now the only one in the world, is manufactured by MOTOROLA Inc. in GLASGOW (SCOTLAND) under licence by BULL CP8 established in LES CLAYES SOUS BOIS (FRANCE). This chip is described here as an illustration : a 6805 CPU, 1.6 kbyte masked ROM, 1 kbyte EPROM, 36 bytes RAM, 18 mm^2.

The operating system is masked programmed, so that the same production line provides chip for various applications, and that new applications are easy to develop.

In the future, new chips will appear in order to reduce prices and to increase performances ; but due to interface standardization, remote controlled terminals will not become obsolete.
And moreover, chip evolution can keep the security features one or two steps ahead the efforts of them trying to defeat them.

I.2 - Card interface

Smart cards are intended for transactions negotiated between the outside and the microprocessor through the interface.

Only six electrical contacts are required in the French proposal presented by AFNOR (Association Française de Normalisation) to ISO. While suitable signals are provided by the outside on five contacts : GND (Ground), VCC (power supply), VPP (programming voltage), CLK (clock), and RST (reset), information may be exchanged in half-duplex asynchronous mode on the sixth contact : I/O (input / output). In its answer to reset, the card instructs the outside in its performances, its conventions and its nature.

A transaction with the card consists of the successive operations : activation of the contacts, reset of the card, processing of one or more instructions, deactivation of the contacts. As a result of a transaction, the card modifies its content (data storage, event memorization,...) and/or delivers information (stored data, computation results,...).

An instruction (always initiated by the outside through I/O) tells the card what to do in a 5-byte header (APP-INS-A1-A2-L) and allows the transfer of one block of data (D1-D2... DL) in one direction under control of procedure bytes from the card. The header consists of the application name (APP), the instruction code (INS) completed by a reference (A1-A2), and the length (L) of the block of data. Procedure bytes allow the card to manage the programming voltage and to control the data transfer.

I.3 - Security

Smart cards have security features that only a computing device could provide. The transactions are negotiated between the outside and the internal microprocessor. The passive cards with magnetic stripes and digital optical records do not have such properties, like complex choices.

The physical security relies upon the impossibility to modify the operating system in the masked ROM, and upon the difficulty to read secrets in the protected memory : a clever chip design increases significantly the physical security of the cards.

The logical security relies upon the processing power of the chip and upon the cryptographic algorithms used in the application : the operating system must be written very carefully. An improved processing power may increase significantly the logical security of the cards.

Absolute security does not exist, for smart cards no more than for other computing devices. So in a new application, the designer must consider the consequences of successful violations. The secrets in a user card must be individualized, tied to the card identity ; a card violation results then in an attack against one user not endangering the whole system.

2 - SMART CARD APPLICATIONS

Smart cards are portable information carriers with three fundamental aims :

- Secure memorisation in the card - destruction of the corresponding writing mechanisms prevents further alteration of recorded data.

- Personalized memorisation in the card - confidential codes recorded in the EPROM memory and checked by the card itself allow operator recognition by the card.

- Cryptographic computation in the card - cryptographic algorithms described in the operating system are executed under control of secret keys recorded in the EPROM memory.

Depending on the leading aim, smart card applications can thus be divided into three classes : log books, certified records, key carriers.

2.1 - Log books

First aid efficiency should be considerably improved by reliable and convenient personal medical files. A user code is not recommended in case of emergency.

Student cards are being experimented at PARIS University.

Such cards can be used as repairment and maintenance note books for vehicles : cars, planes, trucks, ships...

2.2 - Certified records

Confidential codes control the life of such cards : manufacturer code, issuer code, user code. When an incorrect code has been entered three times in a row, even on different terminals, the card locks itself preventing any further operation.

The card tests its availability and its purchasing power before recording a new operation (date and amount). The banker will consider a readable card as a begin of proof in a settlement of dispute between a user and a retailer.

2.3 - Key carriers

Assuming chip inviolability and cryptographic algorithm security, the holder cannot get a copy of the keys recorded in his card. A highly secure identification of the bearer is achieved through use of cryptography to defeat fraud, and through use of confidential codes to defeat theft. Key carriers are particularly suitable in conditional access to services, to resources, to selected areas...

3 - CONDITIONAL ACCESS

In conditional access, a key carrier card materializes authorizations : the holder can use the card, but the card itself remains under issuer ownership.

Each authorization is an entitlement. A remote controller, through an insecure transmission line and an insecure domestic terminal, can securily negotiate a transaction with the card :

- VERIFY the validity of an entitlement,

- DEVALORIZE an entitlement either on a substractive basis by consuming a credit, or on an additive basis by storing a debit,

- VALORIZE an entitlement, either by delivering credits, or by clearing debits,

- ENTITLE, by delivering a new entitlement.

The transaction negotiated through the card interfaceincludes an instruction requesting a cryptographic computation by the card. An important distinction is made between transactions to check entitlements (VERIFY, DEVALORIZE), and transactions to manage entitlements (VALORIZE, ENTITLE). This description of conditional access is influenced by the work of EBU (European Broadcasting Union) on Direct Broadcasting Satellite.

3.1 - Entitlement checking

An entitlement checking transaction is used to verify or to devalorize an entitlement. The aim of such a transaction is to deliver control words. The cryptographic computation during such a transaction is executed with an authorization key.

An authorization key is common to a group of customers for a limited time. The usage of such a key may be restricted by additional parameters to be compared with the authorization status in the card.

Authorization keys encipher control words. The corresponding cryptograms are known as the verification signal.

Depending on the application, control words may be sent back to the remote controller for verification, or used in the terminal as cryptographic keys.

3.2 - Entitlement management

An entitlement management transaction is used to valorize or to entitle. The aim of such a transaction is to increase the value of a card. The cryptographic computation during such a transaction is executed with a distribution key.

A distribution key is unique to each card, or a very small group of cards. The distribution keys belong to the card issuer ; they allow the management of distributed authorizations owned by the card holder.

A distribution key enciphers individual customer messages and/or authorization keys. The corresponding cryptograms are known as the validation signal.

3.3 - Implementations

In access control through interactive networks to services or resources (videotex, public telephone, data networks, teletex, files and computers...), the control word can be sent back on the line to prove user's right to access, or used by the terminal to decipher subsequent data.

In conditional access to broadcast services, the control word must be used in the decoder, according to synchronisations, in order to descramble the service components (video and sound, teletext pages, various data...).

The entitlement management can be done over-the-air by addressing through a broadcast signal, as well as on-line through switched networks. The management can also involve other networks like mail or banks.

4 - A CP8 CARD FOR CONDITIONAL ACCESS

Conditional access key carrier cards are now manufactured by BULL CP8 : the specifications were elaborated for application to ANTIOPE teletext ; but these cards are now proposed for pay-TV, for taxation of videotex databases, and for identification purposes in so various fields as public telephone, computers, and selected areas.

The card may carry up to thirty two authorizations consisting of an authorization key (127 bits), an identifier (24 bits), and a status (variable in size and structure).

4.1 - Mode of operation

In the instruction requesting a cryptographic computation, the block of data given to the card consists of an identifier (24 bits), a parameter (24 bits) and a cryptogram (127 bits).

The identifier names the authorization concerned by the transaction. The status of this authorization must be compatible with the parameter. For example, when the authorization is a subscription, the date indicated in the parameter must lie in the interval (validity date and period) indicated in the status.

When the conditions are verified, the card performs the computation : a result (61 bits) is obtained from the cryptogram (127 bits), the parameter (24 bits), and the secret key (127 bits).

During an entitlement checking transaction, on an instruction requesting the result, the outside gets the control word as a 8-byte block. The authorization status is modified or not depending on the operation : a devalorization or a verification.

During an entitlement management transaction, the card must apply the distribution key (varying from one card to another). The card checks the result (the four first bytes must be equal to the four last bytes), and modifies the status of the designated authorization.

4.2 - Card elaboration

Chips still on the wafer are tested by a dedicated machine writing a serial number and a manufacturer secret code in each valid chip. Testing points are then destroyed, thus definitely disabling invalid chips. This operation is known as chip creation.

Thereafter chips are cut and inserted in ID cards. The card issuer then writes in each card a distribution key computed from the chip serial number. The issuing secret function may be materialized by another card. This distribution key must be correctly used to write any other secret in the card, and to manage authorizations in the card. Assuming the secrecy of the issuing function, only the card issuer can do these operations : he will really control the card life.

The card is now ready to receive authorizations. A wide variety of card life scenarios can be prepared during the card configuration.

After these three successive operations (chip creation, card issue, card configuration), the cards are distributed to the public.

5 - SMART CARDS AND CRYPTOLOGY

Cryptographic algorithms are essential in conditional access. But widely known algorithms does not fit the CP8 chip :

- a 36 byte RAM is sufficient for the DES, but the microcode size is about 1.6 kbyte which is the size of the masked ROM.

- with a 36 byte RAM, one can compute exponentials modulo a composite number up to ninety bits. So a 128 byte RAM is a minimum to implement a medium security RSA scheme, with 320 bit composite numbers. And a 192 byte RAM is hoped for a good security.

5.1 - Actual algorithms

- A first algorithm (one-way, 200-byte microcode) is known as TELEPASS. A result R (64bits) is computed from secret key S (96 bits), data I_n (32 bits) stored at address n, and input E (64 bits).

$$R = P\ (S,\ I_n,\ E)$$

This first algorithm is used to remotely verify rights and identity claimed by a card, and to remotely verify the writing of some information at the right address in the card.

- A second algorithm (inverting another algorithm; 300-byte microcode) is known as the double-field algorithm. A result K (61 bits) is computed from a cryptogram M (127 bits) and a secret key C (127 bits) modified by a parameter P (24 bits).

$$K = g\ (C + P\ ,\ M)$$

Inversibility is essential : in a broadcast system, the same control word is described by as many entitlement checking messages as there are audiences authorized to access the information. For example, the same movie may be accessible by impulse-pay-per-view as well as by subscription, or by a prepaid ticket.

Inversibility is essential also to ensure entitlement management : enciphered personalized directives may be addressed to an identified card.

- A third algorithm (invertible, 200-byte microcode), also named TELEPASS, has been prepared for the new bank card specifications. This algorithm allows the introduction of key carrier philosophy in the bank cards.

The evolution will strengthen these algorithms. But a question is opened : what is the most complex algorithm on a 6805 CPU with the performances : 200-byte microcode, 30-byte RAM, a half second execution time ?

5.2 - Identity certificates

Improved card personalization is obtained by recording identity certificates in the card.

Such a certificate (a 320-bit RSA scheme in IPSO bankcards used on public telephone) is computed by applying a signature function (take the cubic root modulo) to the concatenation of chip serial number (50 bits), subscriber identifier (50 bits), various codes (60 bits), date and period of validity (40 bits), completed by some easily checked redundancy (120 bits).

Any remote or local controller can verify the genuineness of identity certificates by applying the verification function (raise to the cube modulo). Forgery being computationally infeasible, black lists on serial numbers and user identifiers are then very efficient.

5.3 - Some reflexions

The actual key carriers allow only pseudo off-line systems, well fitting hierarchical situations with a central authority, such as a computer and time-sharing terminals.

In IPSO payment experiments, the main proof remains inside the card. Computation results may be stored by the retailer in order to certify records in the card, but only the authority can check the genuineness of such results. There is an important parallel with arbitrated signature schemes.

6 - TOWARDS DIGITAL SIGNATURES

Secret functions of a public key cryptosystem can play two parts in an electronic mail environment :

- regenerate the control word deciphering the subsequent message.
- sign an authentication code added to the message.

But in both cases, the security of the secret function is essential ; if this function is materialized by a key carrier card with a good level of physical security, the legitimate holder himself has the greatest difficulty to get a copy.

Depending on the main part played by the secret function, such a key carrier can be seen :

- as a paper-knife, opening the protection envelope,
- or as a signature stamper, certifying the letter.

Such smart cards are now under investigation ; and this evolution will lead to off-line systems and digital signatures.

6.1 - Scenario for electronic payment

- 1 - The user controls the parameter generation on some domestic device producing random primes under additional conditions so as to construct a composite number. In the example, the composite number has the special form $N = 2^{4X} + K$, with $2K \quad 2^{3X} \quad K$. So the 240-bit K describes the 321-bit N.

The prime factors are recorded as secret parameters in a stamper : a key carrier card dedicated to signatures (take the cubic root modulo N). And the value K is recorded as a public parameter describing the verification (raise to the cube modulo N).

- 2 - The banker tests the stamper produced by the user. He computes a stamper registration by applying his own signature (take the cubic root modulo a 512-bit number) to the concatenation of the public value K (240 bits) given by the stamper, the user identifier (50 bits), the bankcard serial number (50 bits), date and period of validity (40 bits), various codes (60 bits), and an easily checked redundancy (72 bits).

The banker issues the bank-card by recording in it the stamper registration.

- 3 - The retailer checks the stamper registration by applying the bank verification (raise to the cube modulo the 512-bit number published by the bank), thus regenerating the user's public value K. The retailer consults the black lists on card serial numbers and on user identifiers. The user stamps the financial operation (date and amount), thus producing a signature easy to check by raising to the cube modulo $2^{320} + K$.

The electronic check thus consists of two informations : the stamper registration (issued by the banker), and the operation signature (issued by the user). Such a check can be efficiently checked at each step in the clearing circuit between banks.

7 - CONCLUSION

The current needs concerning new services, dedicated to business as well as opened to the general public, are secrecy, discretion, identification, authentification, certification, signature, attestation, confirmation, acknowledgement of receipt... GARANTIR is the French word that best describes all these concepts. It requires only a step further to create a new word : "garantics" to say "implementation of security in new services".

Cryptographic algorithms, security protocols, smart cards are the basic tools of garantics.

Let us keep in mind : the more our countries are computerized, the more bank frauds, economic sabotages, and industrial spying are prejudicial !