BULL CP8 SMART CARD USES IN CRYPTOLOGY

Yves GIRARDOT

BULL CP8

rue Jean Jaurès

78340 LES CLAYES SOUS BOIS

FRANCE

ABSTRACT

The CP8 smart card has memory and intelligence.
These two characteristics joined to its technology, make of it an unfraudable and unduplicable portable strong box.
Thus CP8 is a very secure and convenient device to transport, generate or transmit cryptologic keys or data.

THE CP8 CIRCUIT

The CP8 circuit designed in FRANCE by BULL, is a monolithic silicon chip, containing an eight bit microprocessor, three kinds of memories, and alimentation and dialog interfaces.

- The 36 bytes RAM memory is a scratch one, whose content is lost when the circuit is not powered.

- The 1,6 K bytes ROM memory is an unerasable one. This memory is loaded during the fabrication of the chip itself, and contains a software corresponding to the intelligence given to the circuit.
  Each kind of software called "mask" corresponds to a specific array of applications such as payment, toll television, software protection, etc...

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 464-469, 1985.

- The 1 K byte PROM memory is the application unerasable storage memory. This memory is empty at the fabrication of the chip, and is loaded later during the different steps of the life of the circuit.
  A very important and specific characteristic of the CP8 circuit concerning security is the fact that writing in the PROM memory is totally controled by the microprocessor. Thus the CP8 circuit is a "self-programmable" one.

- Communications with the CP8 circuit are insured by only six points.
  Powering needs three connexions (ground, logical tension, writing tension for the PROM).
  Operating the chip needs two signals coming from the outside (initialization and clock).
  The dialog itself is done by only one connection is an asynchroneous bidirectionnal way.

THE CP8 SMART CARD

The CP8 SMART CARD is a plastic ISO card in which a CP8 circuit is embedded. Connections with the circuit are insured through a round printed goldered patch divided into 8 zones (6 only are used). Yet for special applications it is possible to insert the CP8 circuit on various different supports such as ticket, jock, pen, key...

PROM MEMORY

The PROM memory contains 256 words of 32 bits, and is divided into several zones corresponding to different uses and accesses modes from the outside of the card. The lengths of these zones are parametrable.

- The SECRET ZONE is impossible to read from outside the chip, either by logical or physical way.

  The logical protection is insured by the microprocessor and its associated software located in the ROM memory.

  The physical protection is due to the technology chosen to built the circuit.

  This zone is loaded by several keys (fabrication, issuer, user's key) and by a secret which is a pattern of about one hundred bits (3 words of 32 bits).
- The ACCESS ZONE is a service one, in which are memorized accesses using the issuer's or the user's keys.

  This memory allows to count good or wrong submitted keys, and to lock the circuit in case of several wrong tentatives (usually three).
- The CONFIDENTIAL ZONE can be read if the good issuer's or user's key is given. It contains generally personal or sensitive data.
- The TRANSACTION ZONE is used during the current life of the card. This zone can be read or written, with or without a key, according the application.
- The FREE ZONE can be read without any key and contains non sensitive data.
- The FABRICATION ZONE is a service one. It contains data related to the nature of the card and to the organization of its PROM memory.

ROM MEMORY

The ROM MEMORY contains three kind of programs :

- Service programs dealing with all what is necessary to initialize and currently use the card.
- Security programs insuring a very high level of security by checking flags and data, in order to detect abnormal or frauduleous operations.

- A program corresponding to the implementation of an algorithmic function, to be executed in the card itself

  One of these algorithms is the TELEPASS one-way function.

  A result R (64 bits) is obtained given three inputs. Two of them are taken in the card. The secret S (96 bits) and an Identifier I (32 bits) located at an address i to be chosen.

  The third parameter E (64 bits) is given to the card.

$$R = f(Ei, I, S)$$

CP8 AND SECURITY

CP8 is a very high security card

This is due to its architecture, its technology and its unerasable unduplicable memories (resistant to magnetic fields, UV and X rays).

CP8 allows to treat with a very smart and secure manner classical security problems such as identication, authentication, message certification, integrity checks...

Dialogs are randomised using random numbers as input parameters in the TELEPASS ALGORITHM, executed simultaneously in the user's card, and in the reference card connected to the host system.

CP8 AND CRYPTOLOGY

The main problem in cryptology is key management.

All the security given by cryptologic equipments depends on the protection of keys during their preparation, their transport or transmission, their storage and their use.

- Transport and storage problems can be solved with CP8, considering that it is a true portable strong box to be opened or closed by electronic codes.
  The issuer's code allows to load a set of keys corresponding for instance to a week, a month, a year, according to the application.

  The capacity of the card represents for instance 50 keys of 150 bits, to be loaded in one or several operations.
  The loaded CP8 container card can be transported or mailed without problems. It is an infraudable, induplicable, very convenient, and very secure key vector.
  The user's code allows to read the key in the card and to load the cryptologic equipment.

  For more security during storage before usage, the user has the ability to choose a new user's code only known by him.
  For more security during loading and reading operations, it is recommanded to use "habilitation cards" given only to security responsibles.
  These CP8 habilitation cards are able to generate issuer's or user's codes from the data contained in the habilitation card itself and in the key vector cards. These codes TELEPASS generated are longer and so more secure than manual ones.

- With CP8, key loading and reading operations are automatised, hence operators need not read, or write, or punch them. The values of the keys remain secret.

- Another manner to prevent problems during keys transportation is to suppress this operation. Two accorded CP8 cards (same secret and same Telepass Algorithm) are able to generate two equal secret numbers, given a common unsecret one transmitted on the line.

These two equal numbers can attack at both sides directly the cryptologic equipments,or a pseudo ramdom numbers generator connected to it.
This procedure is limited to symetric key systems.

- Transmission of keys can be done by ciphered ways, using CP8 as ciphering and deciphering systems at the both sides.
In this case the CP8 card contains simultaneously the ciphering or deciphering key (the secret pattern in the secret zone of its PROM) and a reversible algorithm (written in its ROM).
Operating the cryptologic cards can be under the control of habilitation cards.

CONCLUSION

The CP8 smart cards security characteristics have been recognized and are now currently used in many applications such as points of sale, home banking, logical access control, portable file, physical access control, toll services...

Their use in cryptology begins now first at key management level, but will increase in the future by dealing with data requiring more processing power in order to execute quicker more sophiticated algorithms.