IC-CARDS IN HIGH-SECURITY APPLICATIONS

I. Schaumüller-Bichl
VOEST-ALPINE AG
P.O. Box 2
A-4031 Linz

IC-cards, which are credit-card-size plastic cards with integrated CPU and memory, have increasingly attracted public interest in recent years.

Mainly used as "electronic money" in the business of banking and as a storage medium at first, the IC-card is gaining more and more importance as a secure and user-optimised component for cryptographic systems.

The following article analyses IC-cards with regard to their own security and their applications in the field of "EDP security".

The paper is concluded with a glance at the requirements to be met by future card generations and on possible developments.

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 177-199, 1988.

Contents

I) IC-CARDS

IC-cards are plastic cards of the dimensions of conventional credit cards (85.6X54X0.76mm). One or several ICs as well as a system interface are implanted in the plastic card.

Different card types

Depending on the number and design of the implanted chips, the cards are classified according to various criteria:

Number of chips

- "Single-chip cards"
  containing exactly one chip

- "Multi-chip cards"
  containing two or more chips which are connected with each other within the card

Types of chips

- "Passive cards"
  The chips implanted in these cards are merely storage modules. Therefore, the cards are frequently referred to as "memory cards".

- "Active cards"
  containing a CPU in addition to the memory, which
  . secures the access to the data in the memory, and
  . can execute special functions.

Thus, cards with an implanted CPU are often designated as "intelligent cards".

Memory technology

- Erasable cards
  based on EEPROM technology

- Non-erasable cards
  generally based on EPROM technology

For applications in the fields of "electronic money" and "cryptographic systems", mainly active single-chip cards are used for safety reasons. They are often briefly called IC-cards.

System interface

The interface to the IC-card is determined by the ISO Draft International Standard DIS 7816/2 "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimension and location of contacts".

This standard defines 8 contacts (C1 to C8), which are located on the left card side, either in the centre or in the upper edge.

Pin assignment:

C1: VCC, circuit supply voltage
C2: RST, reset signal
C3: CLK, clock signal
C4: RFU, reserved for future use
C5: GND, zero voltage
C6: VPP, programming voltage
C7: I/O, Data Input/Output
C8: RFU, reserved for future use

The exact location and arrangement of the contacts is specified in ISO 7816/2.

II) SECURITY DEMANDS ON THE CARD, SECURITY ANALYSIS

Unlike many other high-security systems, which are often developed for a special problem and which are used by trained specialists in relatively small numbers, the IC-card is intended for large-scale use in a broad range of applications.

Currently, the range of applications chiefly comprises the following fields:

- Electronic money
  (ATM, POS, telephone cards, credit cards, ...)

- Security
  (Personal identification, access control, cryptographic carrier medium in cryptographic systems, ...).
  These interrelated topics are dealt with in detail in chapter III.

- Portable personal files
  (Medical files, study records, ...)

- Take-over of routine functions
  (Start-up of devices, service cards, inventory control, ...)

Thus, the card applications are numerous and manifold, and so are the demands on the cards as far as security, ease of use and flexibility are concerned.

The "ideal" IC-card must meet a number of high requirements:

- Resistance, physical properties:

  IC-cards are designed for frequent use. A typical user will carry his IC-cards with him like his credit cards or his bunch of keys. Special protective measures cannot be taken. For this reason, the cards must show a relatively high stability and high resistance to bending, torsion, heat, radiation, electromagnetic fields, chemicals, etc. These requirements are fully specified in the ISO Draft International Standard 7816/1 "Identification Cards - Integrated Circuit(s) Card with Contacts - Part 1: Physical Characteristics".

- Flexibility:

  Especially in the commercial or private sector, it cannot be reasonably expected of the user to handle each system based on cards, e.g. ATM, credit card, access to building and rooms, etc., differently.
  The acceptance of the system will largely depend on the successful development of a card concept that is flexible enough to be used in a great variety of applications, in spite of differing security requirements.

- Ease of use:

  In former times, security problems were basically confined to the military and diplomatic service, where specialists carried out the necessary security operations.
  Today, the situation is completely different. Due to the common use of computers, networks and telecommunication media, the protection of data is increasingly becoming a real concern to everyone.

Thus, the demands on the protective systems change. Since a special training in this field cannot be required of a user in the commercial or private sector, the system must be provided with a clear interface that is easy to handle. IC-cards are excellently suited for this purpose.

- Security:

  Naturally, paramount importance is attached to the security requirements to be met by the cards. A proper card concept must be suitable for various applications. Therefore, it must be also protected against the entire scope of possible attacks as well as a great variety of potential attackers.

Security analysis

The following considerations prove that the group of possible "attackers" of the system as well as all potential attacks are hardly limited:

A) Potential attackers

Basically, it has to be assumed that every individual person as well as every institution may be considered a potential "attacker". Even trustworthy institutions run the risk of employing personnel who misuse the special knowledge available for their own purposes. So, even if the employees have been selected extremely carefully, there is always the danger of an "attack from inside".

According to their knowledge about the card, the potential attackers can be subdivided into 4 main groups:

a) Manufacturers

This group comprises e.g. chip manufacturers and card producers (or their staff members respectively), which might carry out manipulations in the production sequence

b) Card issuers

Companies or organisations, which issue cards for their customers or employees (e.g. banks, credit card organisations, ...)

c) Authorised card users

d) Unauthorised third parties,

which find or steal cards or try to forge cards.

In order to reduce the risks, during the life cycle of a card, i.e. chip production, card manufacture, issuing of the cards, use, taking out of service, it should be seen to it in general that means of production and information on individual cards may be made available only to persons who need them by all means.

B) <u>Potential attacks/protection requirements</u>

IC-cards are exposed to the entire range of possible cryptoanalytic attacks.

The most important protective mechanisms with which the cards have to be provided if they are to be used in a broad range of applications, are as follows:

a) Protection against unauthorised reading

This corresponds to the "classic" data protection problem. Since usually confidential data (cryptographic keys, passwords, personal information, ...) are stored on the IC-card, it has to be ensured that these are read by authorised persons only.

In principle, there are two possibilities of protection:

i) via a logical or physical "barrier", which permits access to the data only if certain criteria are fulfilled, such as biometric characteristics like finger-prints or voice identification, or the input of "personal identification numbers" (PINs).

ii) Enciphered storage of the data to be protected: The data are enciphered on the card under a key that is known to the authorised user only.
As compared to the method described above, this one offers the advantage that a "circumvention" of the barrier or "direct reading out" is made impossible - or actually senseless - by mechanical devices (e.g. electron microscope).

b) Protection against unauthorised modification of data

Not only confidential but also non-confidential data have to be frequently protected against unauthorised modification. "States of accounts", for instance, especially with minor amounts paid in advance, like with telephone cards, etc., need not necessarily be kept secret, but must be protected against unauthorised modification in any case. In this context, it is noticeable that such a modification, i.e. an "increase" of the current state of account, in special cases, may well be in the interest of the legitimate card holder, and thus the card - unlike most of all the other high-security systems - has to be protected even against manipulations by the legitimate user.

Basically, this problem can be solved in the following ways:

i) a logical or physical "barrier" analogous to Section a) i)

ii) Calculation of a "message authentication code" (MAC)
From the data to be protected, a "test sum" is calculated by applying cryptographic methods; this test sum indicates unauthorised, subsequent manipulation of the data.
Such a method has been standardised in the USA under the designation Ansi X9.9.

iii) Encryption of data
Analogous to Section a) ii)

In addition, the VOEST-ALPINE card concept provides two further security functions:

- PIN check
  Even though the PIN is not stored in the card, it can be checked for correctness upon request.

- Block locking
  Each block, and thus each application, can be locked after a certain number of wrong PIN inputs. The locking of a block has no effect on the operativeness of the other blocks on the card.

  These considerations result in the following card concept:

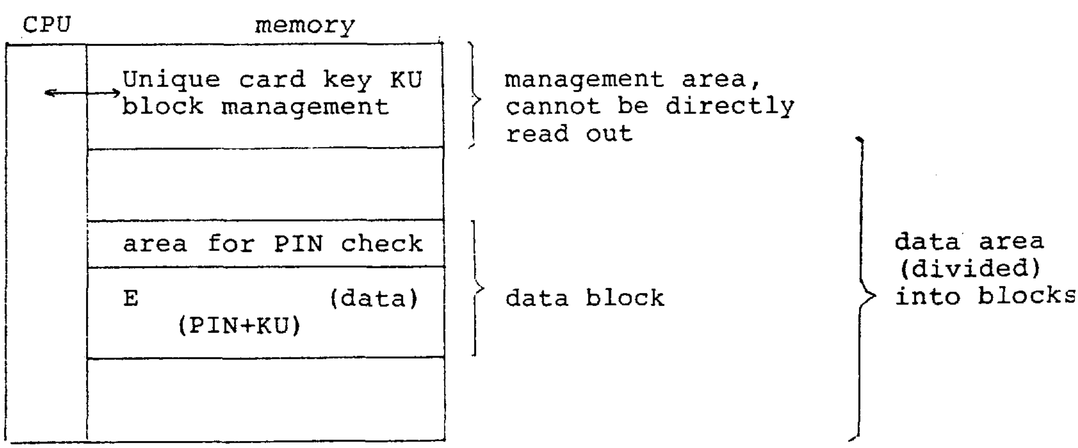


Fig.1: The VOEST-ALPINE IC-card concept

c) Protection against unauthorised copying of cards

In almost all IC-card applications, unauthorised copying of cards is a special security hazard. In high-security applications like the access control system, copying of cards corresponds to making of skeleton keys, and in "electronic money" applications to printing of counterfeit money.

In both cases, the possible attacker need not know the actual contents of the card, i.e. the meaning of the data; a bit-by-bit copying of the data onto another card would suffice.

In order to effectively prevent such an attack, every card must be provided with a unique key that cannot be modified or copied but checked.

Today, this key is usually realised in the form of a random number that is automatically generated for every card, stored in the card and protected by the microprocessor of the card. In the following, this key is called KU ("Unique Card key").

KU can be checked explicitly or implicitly.

i) Direct check
For direct checking, the KU would have to be input directly and compared with the stored value in the card, which involves considerable security hazards.

ii) Indirect check
For indirect checking, a (pseudo) random number is transmitted to the card to be checked for authenticity. By means of a

special function, the card calculates a value that depends on the random number (PRN) as well as on the Unique Card Key.

R: = f (PRN, KU)

The result R serves for checking of the correctness of the card.

In some cases, this method may entail difficulties. In order to be able to check R for correctness, and thus, the card for authenticity, either

- the secret card key KU must be known outside the card,

- a number of reference values must be stored, or

- a suitable "check card" must exist for every card, which contains the same KU.

Each of these 3 solutions involves a considerably great expenditure for the "key management", which is necessary to ensure a minimum of security, and which may cause great problems in the large-scale application of the cards.

iii) Implicit check

For implicit checking, a connection between the data stored on the card and the Unique Card Key is established. This is achieved by applying special cryptographic methods, for instance. Based on the concept described in a) ii), i.e. enciphered storage of data on the card, these data are enciphered under a key which results from a combination of PIN and Unique Card Key.

The card can be copied only if the PIN is known; even data that can be read out by means of an electron microscope cannot be appropriately copied onto another card. In case several groups (e.g. bank/customer) are interested in the protection of data, the PIN proper must consist of the corresponding partial PINs.

d) Protection against simulation of the card

An attacker may - sometimes without major technical and organisational expenditure - intercept the connection between the IC-card and the master (card reader, PC or host), and thus store the request data and the corresponding responses of the card. A subsequent re-input of the data, and thus a simulation of the card, is possible. This attack can be effectively prevented by utilising the "intelligence" of the card, i.e. its abilitiy to execute computer operations.
Similarly to the generation of "session keys" with communication encryption, a pseudo random number is transmitted to the card upon every call. The card calculates the response as a function of this pseudo random number.

III) A NEW CARD CONCEPT AND ITS APPLICATIONS

Chapter II deals with the security of IC-cards with regard to various attacks, while this chapter gives examples of how the IC-card in turn helps to increase the security of systems.

IC-cards are effective especially in two functions:

- as carrier medium for confidential data, such as cryptographic keys and passwords, and

- as "special computer" for taking over selected security functions.

The following section describes an IC-card, which has been developed for high-security applications.

The basic card concept

The concept is based on the considerations of Chapter II, concluding that the cryptographic protection of the data stored on the card provide a maximum degree of security in general.

i) Block structure
The data memory is segmented into blocks of freely selectable lengths. Each block is allocated to a

specific application and protected by a separate PIN, i.e. the PINs are block-specific, and thus application-specific, but not card-specific.

ii) Encryption of data on the card

All (user) data on the card are basically stored in enciphered form. In order to fulfill the security requirements to be met by the card (cf. Chapter 1, security analysis), the encryption of the data must comply with a number of specifications.

- Dependence on the PIN

  In order to prevent misuse of a stolen or lost card, it has to be protected by some additional information that is known to the legitimate user only, i.e. usually a "PIN" (Personal Identification Number).

  In the VOEST-ALPINE concept, the PIN is highly involved in the protective mechanism; it serves as part of the key under which the data stored on the card are enciphered.

  The PIN can be replaced by other - user-related - parameters, such as biometric parameters, without the basic concept having to be modified.

- Dependence on the card

  In order to effectively prevent copying of the enciphered data onto another card, and thus, duplicating the card, the encryption must depend on a paramater which is different for each card, secret and not predicatable ("pseudo random").

  This "Unique Card Key", in the following referred to as "KU", is exclusively used for the encryption of data on the card and cannot be read out.

Other card functions

In addition to the basic functions of the card as described above, two other functions are provided, which are based on the cipher algorithm integrated in the card:

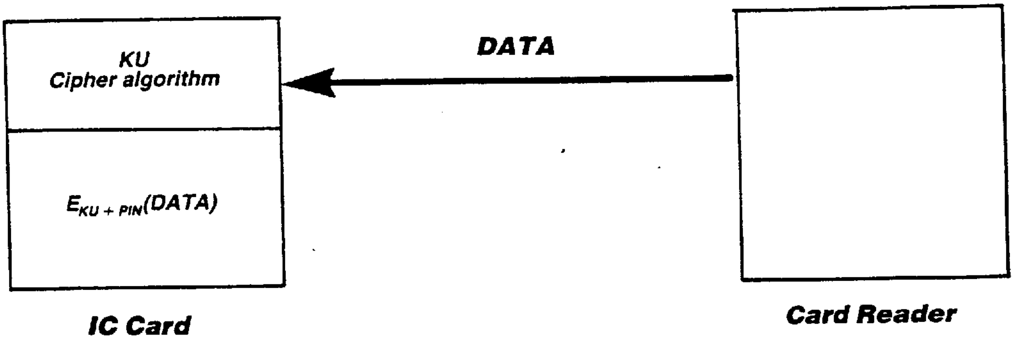
- Enciphered communication

  It is possible to encipher all data transmitted between the card and the card reader. This - expensive - function is intended for special applications.

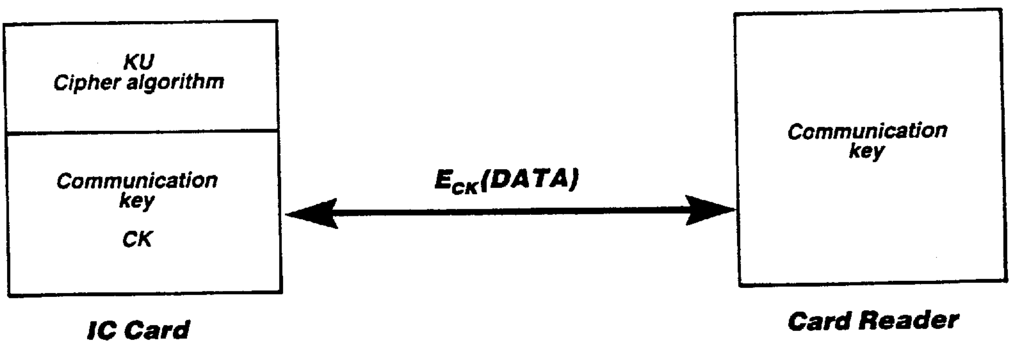
- Encryption of external data ("Black Box Cipher")

  This functions enciphers external data under key stored on the data and retransmits them to the card reader. It is especially used for the realisation of key management functions.

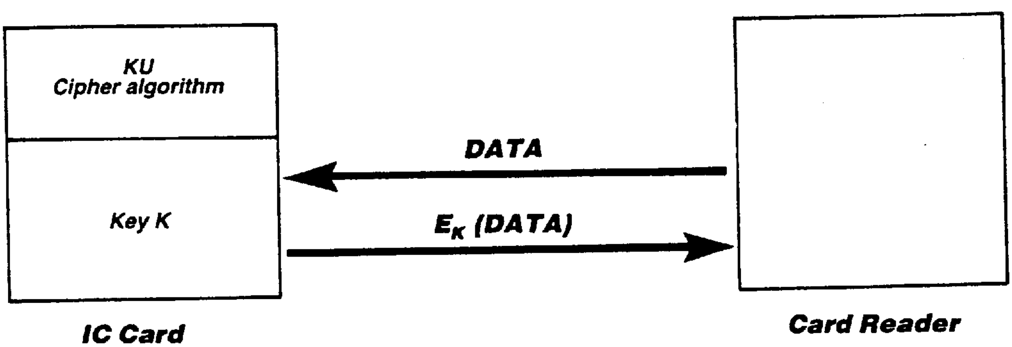
  Thus, the cipher algorithm on the card is used for 3 different functions:



a) Data are stored on card in enciphered form



b) Enciphered communication between card and card reader



c) "Black Box"- Encryption of external data

Fig.2

Range of applications

Basically, there are two possibilities of using IC-cards in an efficient way:

i) as "carrier medium" for confidential data:

Cryptographic keys, passwords, identification parameters, states of account, medical information and similar data can be securely stored on the card and retrieved in a user-friendly way. By storing several keys, it is possible to set up key hierarchies.

ii) as "special computer":

Special functions, such as encryption of external data, are taken over by the card.

Thus, it is ensured that
- these functions cannot be manipulated, and
- secret parameters cannot occur outside the card.

The card concept described above is mainly used in:

- Applications with high security requirements, e.g.

  - EDP security:

Data protection:	File encryption, database encryption, communication encryption
Access protection:	Identification, authentication, access control

. Software protection: Protection against software piracy, protection against unauthorised software applications

Electronic money: Credit cards, debit cards, telephone cards, POS, ATM, etc.

- Multi-functional cards:

If, in the future, IC-cards are to be applied to the degree planned today and accepted by the users, the use of multi-functional cards is indispensible.

The above card concept is an attempt to meet these requirements:

- The block organisation allows the use of a card in a number of different applications
- PIN depends on the application
- PIN can be selected by the user or preset by the issuer
- Locking of a block on the card has no effect on the other blocks (= applications)
- Varying number of allowed wrong inputs possible for the individual blocks.

IV. FUTURE REQUIREMENTS

In the unanimous opinion of technical engineers and market research specialists, the IC-card will spread widely in the future.

Even today, IC-cards are used especially in the fields of "electronic money" and "portable personal files" on a large scale; by 1988, several million IC-cards will be in circulation.
With the continuous spreading of the cards and new fields of applications, however, the requirements to be met by the cards increase, too.

In the next few years, further developments in the card technology are to be expected particularly in the following 3 fields:

a) Memory expansions

In general, the current (single-chip) IC-cards have a memory size of 1, 2 or 8 kilobytes. According to the progress made in IC-technology, a gradual expansion of the data memory of the card is to be expected.
Moreover, the combination of IC-cards with laser cards is taken into consideration. The card resulting would unite an increased security of the IC-card and the high storage volume of the laser card.

b) The "Super Smart Card"

The "Super Smart Card" is an IC-card at which the keyboard and the display are already integrated in the card.

This extra equipment

- ensures an increased security of the entire system, and

- allows its application as an "Offline Security Device".

The security is increased primarily in applications in which the card reader or the keyboard respectively is unprotected, and thus exposed to the danger of manipulation.
It is possible, for instance, to intercept the connection between the keyboard and the card reader unnoticed and with a relatively small expense, and to store also the PINs typed in by the users.
If the keyboard is located on the card, and thus is controlled by the card user, such an attack is impossible.

As an "Offline Security Device", the Super Smart Card can be applied in fields in which peripheral devices are used to which a card reader cannot be connected - which is the case with the major part of the terminals used today.
The common direct data transfer between the card and the computer is replaced by manual typing in of the request or response data respectively by the user.
Such a procedure also permits the realisation of a homogenous security system even if different hardware (terminals and PCs) is used.