THE CHIPCARD - AN IDENTIFICATION CARD WITH CRYPTOGRAPHIC PROTECTION

Dr. Thomas Krivachy
Siemens AG
D-8000 München 70

1 Identification Cards

1.1 Card technologies with machine-readable data

Plastic cards for identification purposes (ID-cards) have been in use for over 50 years, while cards with machine-readable data have been available for about 20 years. Figure 1 shows card technologies commonly employed today. Most widespread are cards with magnetic stripe. Holographic cards are used e.g. as prepaid cards for public telephones, laser cards for mass storage applications.

	Card technologies			
	magnetic stripe	holo-graphic	laser	chip
Memory today (bits)	500/180/500	20..200	$0,1..1.10^6$	0,2.. 16K
Capacities tomorrow (bits)	500/180/500	20..200	$0,1..80.10^6$	0,2.. 64K
Alterable memory	yes	no	no	yes
Protected memory	no	no	(yes)	yes
Logic functions in the card	no	no	no	yes
ISO standards existing	yes	no	no	(yes)

Figure 1 Card technologies

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 200-207, 1986.

Chipcards have existed for about 5 years. They are one type of identification cards with machine readable data and they are characterized by one or more chips embedded in the 0.76 mm thick card material.

1.2 Chipcards

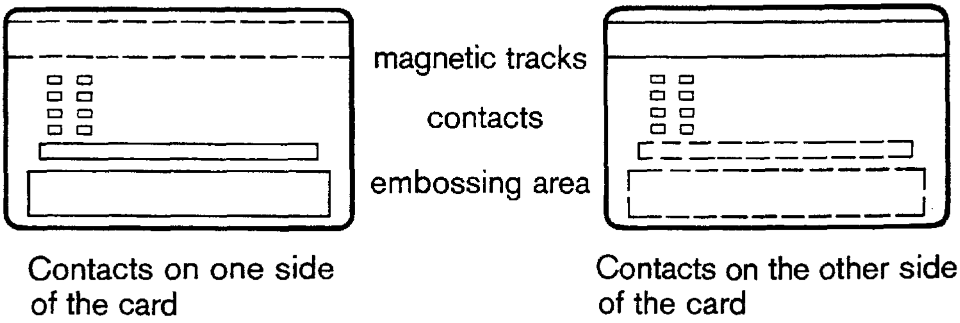
Either non-volatile memory chips or chips with logic functions (e.g. microprocessors) can be embedded in the card. If non-volatile memory chips are embedded then the card can be used like as a magnetic stripe card. If chips with logic functions are embedded, a new kind of card is obtained, that is, one with processing capabilities or intelligence. This characteristic was chiefly responsible for the name coined in the USA, where chip cards are also called "smart cards".

Since chips with logic functions and non-volatile memory can be embedded, it is possible to subdivide the overall memory capacity into sub-areas of differing access. The data stored in the chipcard can therefore be protected with a variety of access methods. In the main, we distinguish between the following sub-areas of the memory:

- Free memory area: All the information which does not need protection from reading, erasing or altering is stored here. This sub-area has similar features as magnetic stripes.
- Protected memory area: To gain access to this sub-area the user has to enter a password. This password may be a four-digit PIN (Personal Identification Number), a multi-digit system password or, at some future date, even a finger-print or speech recognition. Access to this area is not possible before the right password is entered. After entering the right password the data can be read out. The data read out can be altered or erased too, depending on the application.
- Secret memory area: The data stored in this area can be neither read out nor erased nor altered. Secret data can only be written in at certain phases in the manufacturing process. Data to be checked or to be processed during the application is read in and only the result is read out. Regarding applications which are very sensitive, this secret area surely provides the most important and significant advantage over other card technologies. A PIN, a system password, a program, a secret algorithm or the key to this algorithm can be stored here. Further, incorrect entries of a password can be counted internally by chipcard logic functions and, as soon as a certain number in succession is exceeded, the chip is disabled so that any further attempt to access will fail.

ID-cards and the magnetic stripe have additionally been standardized internationally. The ISO (International Organization for Standardization) also has a Working Group for chipcards with contacts, and a corresponding resolution on a Draft International Standard is scheduled this very year.

Figure 2 shows the location of contacts according ISO DP 7816/2 and the areas of an ID-card which are already standardized, the magnetic tracks and the embossing area. It is of greatest importance for the standardized ID-card that the contacts and the magnetic tracks are not adversely affected under any circumstances by an error on the part of the user.



Contacts on one side of the card

Contacts on the other side of the card

Figure 2 Location of the contacts according ISO DP 7816/2

According to ISO DIS 7816/1, Physical Characteristics, chipcards must work correctly after some specific mechanical tests, e.g. after bending. This in turn restricts the size of the chip which is to embedded. According to the experiences known today chips with a size of about 20 mm^2 located between the two rows of contacts fullfil these bending tests.

1.3 Encryption ICs

There are already several semiconductor manufacturers who supply encryption ICs for installation in terminals or computers. However, chips with common encryption algorithms known today such as DEA and RSA are out of question for standardized chipcards because they still require too large an area and therefore probably do not satisfy the mechanical test conditions after embedding in the card.

For these reasons and others, it is more appropriate to use special encryption algorithms matched to the chipcard and being programmed in the memory of the chip. Essentially, this requires the algorithm to be of maximum possible reliability, while still allowing the chip to be embedded in a standardized chipcard. Depending on the application, both symmetrical and asymmetrical encryption algorithms may be needed for chipcards.

The difficulties associated with key management and key distribution have to be considered as well as other security aspects of that application when the actual encryption algorithm is being fixed. The chipcard of the future will be used not only in hierarchically organized systems but also in "all-in-all systems". Besides, the chipcard is going to be employed not only by a scarcely changing, limited group of users on specific terminals, but also by a considerably fluctuating and practically unlimited group of subscribers (of the order of 100 million) throughout the world on different terminals fitted to the same application.

2 ID-to-end cryptographic protection

Cryptographic protection is implying here both the encryption and decryption of the transmitted data as well as the authentication of the transmitted data in a communication network. Only the encryption procedure will be explained below as an example.

2.1 Survey

The possibility of storing the algorithm and the key in the secret memory area of a chipcard offers the user a degree of mobility and the issuer a degree of security previously unknown in systems with cryptographic protected data: mobile ID-to-end encryption is available now in addition to fixed end-to-end encryption.

End-to-end encryption using ID-cards is in use since years. Data is transmitted between the card and the terminal, but the encryption is done outside of the card, i.e. usually in the terminal (Fig. 3).

Using the chipcard with its logic functions specified for cryptographic protection the following new modes are basically possible:

- ID-to-end encryption in dialog mode: Data is transmitted to and encrypted in the chipcard and then transmitted in dialog mode between the chipcard and the other end of the communication, e.g. a host (Fig. 4).

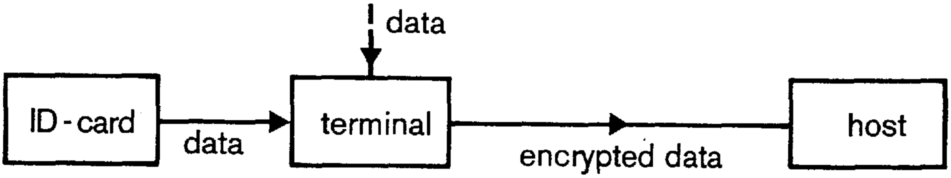


Figure 3 End-to-end encryption

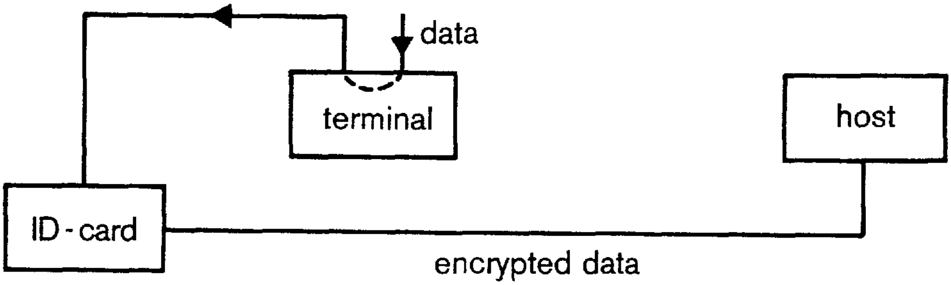


Figure 4 ID-to-end encryption in dialog mode

- ID-to-end encryption with buffer storage: Data transmitted to and encrypted in the chipcard is buffered in a terminal.After a certain time delay the data is transmitted from the terminal to the host (Fig.5).

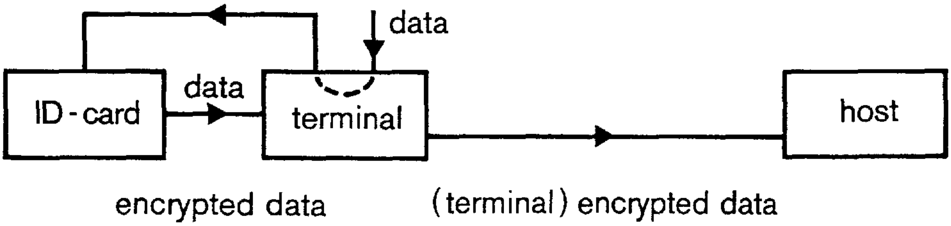


Figure 5 ID-to end encrpytion with buffer storage

Regarding the technical side of transmission,ID-to-end encryption in dialog mode is similar to end-to-end encryption /1/, but here again the advantages of the chipcard make new system and security concepts possible.

2.2 ID-to-end encryption with buffer storage

The entire system consists at least of an identification card (ID-card) with cryptographic protection, i.e. a chipcard, a terminal for buffering the messages received from the chipcard, and the other end of the communication, e.g. a host. This mode is suitable for all applications where, on various grounds, on-line dialog with a host is not always wanted every time when the chipcard is used. In a terminal which generally offers free access to several different persons, it is necessary to provide cryptographic protection so that the original data in the terminal buffer can be protected from unauthorized manipulation. We have tried to confine the description of this mode to fundamentals, omitting further subviding such as whether and on what transmission link the messages are encrypted or authenticated, whether use is made of one or two algorithms, and whether the algorithms are symmetrical or asymmetrical, secret or commonly known.

In the example in Fig. 6 it is assumed that there are two different algorithms: The algorithm f is stored in the chipcard and is used for data encryption between the chipcard and terminal. The algorithm g is used for encrypting the data between the terminal and the host. Further it is assumed that the host knows the algorithm f and the key KC stored in the chipcard as well as the algorithm g and the key KT stored in the terminal

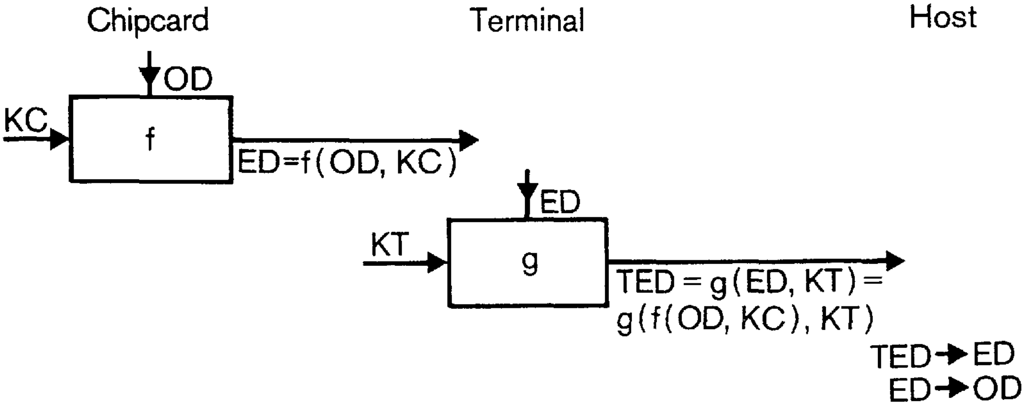


Figure 6 ID-to end encryption with buffer storage

Conventional dialog between terminal and host is conducted by encrypting the data stored in the terminal and read either from chipcards with cryptographic protection or from any type of card without cryptographic protection. This is done using the algorithm and the key stored in the terminal.

Using chipcards with cryptographic protection the data generated in the terminal (no matter whether sums of money or messages) is transmitted in the simplest case as original data OD in plain text from the terminal to the chipcard. Data transmitted to the chipcard can now be processed in the card itself as the encryption algorithm f and the key chip KC are stored in the "smart card". The original data OD is encrypted in the chip card and the output is send as encrypted data ED to the terminal. The encrypted data can now be stored securely in the terminal as the terminal doesn't know the decryption procedure for ED to obtain OD. Usually the terminal stores the encrypted data ED received from one or more chipcards over a certain time as mentioned before and then transmits it as terminal encrypted data TED to the host, using the terminal algorithm g and the key terminal KT.

The terminal encrypted data TED is decrypted in the host with the procedure required for the algorithm g and the key KT to obtain the encrypted data ED. At the next step the data ED is converted to the original data OD,i.e. in plain text, in an analog procedure.

3 Use of chipcards with cryptographic protection

Postal services and banks are particularly interested in the chipcard /2-4/. For some applications, the security mechanisms incorporated in the chip are already sufficient, and no cryptographic protection is needed, e.g. for telephoning with a prepaid card /5/. For others, e.g. for access to interactive videotex or for message service and retrieval, it has been found from experience with hackers that cryptographic protection is absolutely essential for access and maybe even for the transmitted data. Further postal applications include in a variety of services, e.g. teletex, facsimile and mobile telephones.

Interactive videotex homebanking and POS (Point Of Sales) are additional public applications for which an ID-card with cryptographic protection is needed. The credit card organizations, alerted by losses due to the abuse of magnetic-stripe cards, are also very much interested in embedding chips in their normal magnetic-stripe credit cards /6/.

In addition to these public applications (some of which have already been tested or are being tested in several countries) there are also certain private uses for identification cards with or without cryptographic protection, e.g. access to equipment (as a substitute for keylock switches), data base access, and for private text, data, image and voice communication systems.

4 Outlook

Today's chipcard already offers numerous advantages to user and issuer alike. As technology advances, we shall see chips with more efficient encryption algorithms and larger memory capacities with the small chip areas required for standardized chipcards.

A new generation of chipcards will be the chipcard cryptomodule which will contain keyboard, display and power supply. The PIN will be entered straight into this cryptomodule and will not be transmitted in plain text from the terminal keyboard to the chipcard. However the acceptance of a cryptomodule as a substitute of a chipcard has to be tested:Cryptomodules might be rigid whereas chipcards can be bent.

In order to obtain real information on the risks associated with the various system and security concepts, and on the degree of acceptance by users and issuers, it will be necessary to carry out field tests with the means available today, so that theoretical considerations for future, better systems can be developed on the basis of practical experience.

References:

/1/ Norbert Ryska, Siegfried Herda: Kryptographische Verfahren in der Datenverarbeitung, Springer Verlag 1980
/2/ Eberhard Schröther, Zeitschrift für das Post- und Fernmeldewesen, (1983), H.2, S. 28-31
/3/ Gerd Tenzer, Zeitschrift für das Post- und Fernmeldewesen (1985), H.2, S. 16-19
/4/ Industriemagazin, (1985), Februar, S. 116-119
/5/ Max Ludwig, telcom report 7, (1984), H.2, S. 151-154
/6/ Business Week, (1984), Oct. 15, pp. 112-114