

Smart-cards : a cost-effective solution against electronic fraude

Dr. Marc Lassus
Gemplus

PB 100, F-13881, Gemenos, France

Abstract. Smart-cards have the tremendous advantage, over their magnetic stripe ancestors, of being able to execute cryptographic algorithms locally in their internal circuitry. This means that the user's secrets (be these PIN codes or keys) never have to leave the boundaries of the tamper-resistant silicon chip, thus bringing maximum security to the overall system in which the cards participate.

Smart-cards contain special-purpose microcontrollers with built-in self-programmable memory and tamper-resistant features intended to make the cost of a malevolent attack far superior to the benefits. This paper is both a survey of the existing componets, their applications and an attempt to describe some of their possible evolutions.

1. What is a smart-card ?

In the time-scale of the silicon industry, the idea of inserting a chip into a plastic card is rather old : the first patents are now twenty year's old but practical applications emerged only a eight years ago due to limitations in storage and processing capacities of past circuit technology. New silicon geometries and processing refinements lead the industry to new generations of cards and more ambitious applications such as wireless communications (GSM), pay-TV, loyalty and physical access-control.

Over the last four years there has been an increasing demand for smart-cards from national administrations and large companies such as telephone operators, banks and insurance corporations. More recently, another market opened up with the increasing popularity of home networking and Internet.

The physical support of a conventional smart-card is a plastic rectangle on which can be printed information concerning the application or the issuer (even advertising) as well as readable information about the card-holder (as for instance, a validity date or a photograph). This support can also carry a magnetic stripe or a bar code label. An array of eight contacts is located on the micromodule in accordance with the ISO 7816 standard but only six of these contacts are actually connected to the chip, which is (usually) not visible. The contacts are assigned to *power supplies* (Vcc, Vpp), *ground*, *clock*, *reset* and a *serial data*

communication link (commonly called I/O). Their specification part in the standard is currently reconsidered upon requests from various parties (suppression of the two useless contacts, creation of a second I/O port, I2C bridging etc.).

For the time being, card CPUs are still 8 bit microcontrollers and the most common cores are Motorola's 68HC05 and Intel's 80C51 but new 32-bit devices will soon begin to appear. RAM capacities (typically ranging from 76 to 512 bytes) are very limited by the physical constraints of the card. The program executed by the card's microprocessor is written in ROM at the mask-producing stage and cannot be modified in any way. This guarantees that the code is strictly controlled by the manufacturer. For storing user-specific data, individual to each card, the first generation of non-volatile memories used EPROMs¹ which required an extra "high" voltage power supply (typically from 15 V to 25 V). Recent components only contain EEPROM which requires a single 5 V power supply (frequently that of the microprocessor) and can be written and erased thousands of times (cycles). Sometimes, it is possible to import executable programs into the card's EEPROM according to the needs of the card holder. EEPROM size is a critical issue in the design of public-key applications (where keys are relatively large). Consequently, smart-card programmers frequently adopt typical optimization techniques such as re-generating the public-keys from the secret-keys when needed, re-generating the secret-keys from shorter seeds, avoiding large-key schemes (for instance Fiat-Shamir) or implementing compression algorithms for redundant data (text, user data, etc.) and EEPROM garbage collection mechanisms. Real and complete operating systems have been developed for this purpose by several manufacturers. Finally, a communication port (serial via an asynchronous link) for exchanging data and control information between the card and the external world is available. A common bit rate is 9600 bits/s but much faster interfaces are commonly being used (from 19,200 up to 115,200 bits/s) in full accordance with ISO 7816.

¹ Electrically PROgrammable Memory (EPROM) and Electrically Erasable PROgrammable Memory (EEPROM or E²PROM); non-volatile memory (NVM) means usually provided for data storage.

A first rule of security is to gather all these elements into a single chip. If this is not done, the external wires, linking one chip to another could represent a possible penetration route for illegal access (or use) of the card. ISO standards specify the ability of a card to withstand a given set of mechanical stresses. The size of the chip is consequently limited and present constraints (especially memory and cryptographic capabilities) mainly follow from this limitation.

Smart-card chips are very reliable and most manufacturers guarantee the electrical properties of their chips for ten years or more. ISO standards specify how a card must be protected against mechanical, electrical or chemical aggressions but for most existing applications, a card is far obsolete before it becomes damaged. A well known example is the French phone card where the failure rate is less than three per 10,000 pieces.

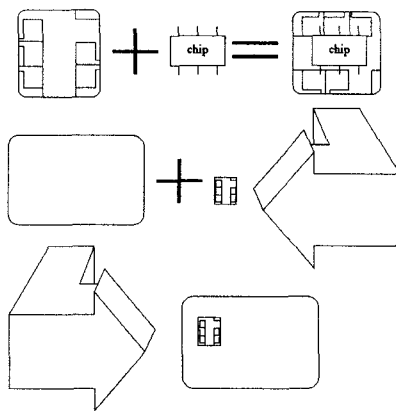


Figure 1. Smart-card manufacturing

Annex 1 lists some of today's most common chips as well as their characteristics (where \oplus = maximal clock rate given in MHz, \updownarrow = EEPROM, \downarrow = EPROM, *Witness cell* (detects if the EEPROM was erased abnormally), *Clock Frequency.*, *Temperature*, *Abnormal Voltage (V_{pp})*, *Light exposure and passivation sensor*. Information about such security detectors and tamper-resistance capabilities is usually rather hard to obtain from the manufacturers for obvious security reasons).

In general, smart-cards can help whenever secure portable objects are needed, and in particular whenever the « external world » needs to work with data without knowing its actual value. The card's tamperproofness, combined with public-key cryptography (secretless terminals), generally provide adequate solutions to many everyday security problems.

2. Smart-card communication and command format

Communication with smart-cards is ruled by the (previously-mentioned) ISO standard 7816/3. Only two protocols are currently defined in this standard (byte-oriented T = 0 and block-oriented T = 1) although up to 14 are reserved (T = 14 is very rare, and means that the communication protocol is proprietary). Thus the electrical levels and error handshakes as well as the frequency used impose a specific hardware on the « external side » which is the equivalent of a UART with more sophisticated functions. This minimal hardware, needed to operate a card, consists of :

- ♦ a mechanical interface : the *connector*
- ♦ an electronic interface : the *coupler*
- ♦ and a box containing the above two elements : the *smart-card reader* (or simply « *reader* »)

The simplest readers are quite similar to modems and manage only the ISO communication protocol without interacting « intelligently » with the operating system of the card. They are called « transparent readers » and should (but in practice may...) operate with any smart-card from any vendor which complies with the ISO standard.

The most sophisticated readers can be programmed with parts of the application logic and data (for instance RSA or DSA public keys), files and programs. They can execute cryptographic functions, replace completely a PC, have keyboards, pin-pads or displays and generally use a specific programming language and do not support all types of smart-cards even if they comply with the ISO standard (because they often integrate particular commands dedicated to a given card).

To operate a card, the reader needs to implement the following four functions :

- ❶ Power on/off the card
- ❷ Reset the card
- ❸ Read data from the card (*get commands*).
- ❹ Write data to the card (*put commands*).

Get and put commands contain a header (actually a function code consisting of 5 bytes designated by CLA, INS, P1, P2 and LEN) according to which the card processes the incoming data. An acknowledge byte and a couple of status bytes (SW1 and SW2) are sent during (and after) the execution of each command.

3. Card lifecycle

Although the card lifecycle and manufacturing are described in many different sources, we particularly recommend Fuchsberger & al's *excellent* overview² :

Smart-card manufacturing starts with the design of the card operating system and the application software, following the principles applying to any software for use in security applications. This is in itself a nontrivial task but at least the memory available in smart card chips is relatively small which limits the eventual size of the software. There have to be checks that the operating system meets its specification and also that no unintended features have been included.

The ROM mask of the operating system is then given to the chip manufacturer, who will return an implementation of the code for cross-checking before manufacturing the batch of chips. This is in itself a useful integrity check but clearly one normally requires this code to be kept confidential and therefore its distribution should be carefully controlled. Furthermore, the manufacturer has to be accountable for all chips made, some of which, due to yield failures, will need to be destroyed. Otherwise, an attacker may obtain raw chips to mount any form of counterfeit operation.

The batch of chips is distributed to the fabricator [smart-card manufacturer] whose task it is to embed the chips into the plastic cards ? The role of the fabricator varies considerably between customers and their services. As a very minimum the fabricator must test the complete IC card to ensure its operational state. In some cases the fabricator completely personalises the card to the requirements of the issuer.

4. Applications

4.1. Pay-TV

One of the first applications of micro-controller-based smart-cards was pay-TV. The card appears to be both an ideal identification token (associated to the subscriber) and an efficient loyalty support.

In most pay-TV applications (the two best-known examples are most probably Eurocrypt and Videocrypt), the program provider broadcasts periodically (typically each 100 to 500 ms) an encrypted *control-word* (temporary key) under which the image is encrypted. Only valid cards can extract

this control-word from the data stream, decrypt and send it to the decoder.

A second interesting marketing model is « pay-per-view ». In this setting, the viewer buys a pre-loaded card and spends progressively the loaded amount (In general, a time coefficient is associated to each program).

Finally, cards also appear to an efficient sponsoring tool. In general, the sponsor issues free cards, valid only during a given event (for instance a base-ball match) and distributes them. The broadcast will then be only (freely) accessible by the card-owners.

4.2. Mobile communications

GSM security is essentially based on the tamper-proofness of the smart-card (renamed SIM = Subscriber Identity Module in the standard). Each SIM is associated with a set of secret and public parameters (IMSI, Ki, PIN, PUK etc) that allow the operator to locate the mobile phone, route calls and digital messages (Short Message Services).

Smart-cards present major security and cost advantages over passive code identification. Fraud (mainly due to card lost or password disclosure) is far lower than fraud losses due to password eavesdropping in non-tamper-resistant systems.

4.3. Electronic cash

Microcontroller or authenticated-memory cards can be used for storing or representing legal-tender in several ways :

① The smart-card can be a bi-directional link between the card-holder and his bank account. In such a case, terminals may check the genuineness of the card by diverse cryptographic protocols (mainly depending on the terminal and card's respective computational powers).

② The card can also act as an electronic purse and store in EEPROM a balance that can be converted or transferred from the card to the POS (Point of Sale) terminal and the bank.

Payment protocols can be anonymous (preserve the user's privacy exactly as usual paper money) or auditable (just as a regular cheque account). The smart-card industry considers that the banking sector will be one of the main card application fields during the coming decade.

² *Public-key cryptography on smart-cards*
Proceedings of the International Conference on
Cryptography, Policy and Algorithms, LNCS
1029, pp. 250-269.

4.4. Other applications

Smart-cards are also used in loyalty applications, electronic copyright (typically software protection), gaming, physical access control, Internet security and many other areas.

Gemplus considers that, on the long-term, the best way of fitting to the clients needs will probably consist in providing to the end-user with a *blank card* which ROM mask contains a general purpose high-

level operating system, on the top of which each user will either add his own (home-made) applications or ready-to-use programs bought and downloaded from a software editor.

In this scenario, the card's natural tamper-resistance, combined with public-key cryptography capabilities, appears to be a very natural solution to passive and active software protection.

ANNEX 1
COMMON SMART-CARD CHIPS

Name	Core	Manuf.	RAM	ROM	NVM	Detectors	Surface	⊕
SC01	68HC05	Motorola	36	1.6 K	1 K ↓	N.S.	3.5 × 5.5	4
SC03	68HC05	Motorola	52	2 K	2 K ↓	N.S.	3.5×5.6	4
SC11	68HC05	Motorola	128	6 K	8 K ↓	F, V	3.5×5.6	4
SC21	68HC05	Motorola	128	6 K	3 K ↑	F, V	3.5 × 5.6	4
SC24	68HC05	Motorola	128	3 K	1 K ↑	F, V	4.14×3.44	5
SC26	68HC05	Motorola	160	6 K	1 K ↑	F, V	13.4 mm ²	5
SC27	68HC05	Motorola	240	16 K	3 K ↑	F, V	5×5.4	5
SC28	68HC05	Motorola	240	12.8 K	8 K ↑	F, V	27 mm ²	5
ST1821	68HC05	SGS	44	2 K	1 K ↓	F, T, V, L	3.4 × 5.36	5
ST1834	8048	SGS	76	4 K	3 K ↓	F, T, V, L	3.61× 5.79	5
ST16612	8048	SGS	224	6 K	2 K ↑	F, T, V, L	5.66 × 5.87	5
ST16601	68HC05	SGS	128	6 K	1 K ↑	F, T, V, L	10.1 mm ²	
ST16623	68HC05	SGS	224	6 K	3 K ↑	F, T, V, L	3.66 × 6.61	5
ST16F44	68HC05	SGS	512	16 K	8 K ↑	F, T, V, L	18.6 mm ²	5
ST16F48	68HC05	SGS	512	16 K	8 K ↑	F, T, V, L	4.8 × 4.9	5
ST16301	68HC05	SGS	160	3 K	1 K ↑	F, T, V, L	3.66 × 4.93	5
65901	prop.	Hitachi	128	3 K	3 K ↑	W	secret	5
6483108	H8300	Hitachi	256	10 K	8 K ↑	W	secret.	5
H8310	H8300	Hitachi	256	10 K	8 K ↑	W	5.3×5.2	5
H83102	H8300	Hitachi	512	16 K	8 K ↑	W	18.08 mm ²	5
62720	prop.	Oki	128	3 K	2 K ↑	secret.	secret	5
62780	prop.	Oki	192	6 K	8 K ↑	secret.	secret	5
44C10	80C51	Siemens	128	4 K	1 K ↑	«hardware»	13 mm ²	5
44C40	80C51	Siemens	256	8 K	4 K ↑	«hardware»	18.39 mm ²	5
44C80	80C51	Siemens	256	16 K	4 K ↑	«hardware»	24.49 mm ²	5