

SMART CARDS - PAVING THE WAY TO THE DIGITAL AGE

The digital age today raises a number of commonly mentioned questions and challenges. For example, how can you be sure of someone's identity or guarantee a document's originality and integrity? In today's world, telling the difference between the original and a simple copy or imitation, or even guaranteeing someone's identity, is becoming a fundamental requirement that leads to new needs. Such needs arise from the very definition of digital.

The digital revolution is on the move

In many cases, it is no longer enough to simply say or show who you are. Now you need to prove and therefore calculate it. Consequently, it is increasingly essential to redefine the concept of identity and the ensuing identification.

The second obvious need created by the digital revolution relates more to the legislative or legal framework. How can evidence be produced while in certain cases guaranteeing the anonymity of the person in question, and in all cases protecting the individual's private information used?

Answers from the market

For more than 20 years, the smart card industry has been providing answers to such questions, especially over the last five years, which have seen two major trends take shape:

The first is the one that hailed the microprocessor card (1) as the only smart card worthy of the name to the detriment of the memory card, which for a long time, though, stood as the reference in the field. Smart cards may now feature computing power to prove the cardholder's identity in a dynamic (2) and therefore reliable way. It is the smart card's combined cryptography, or even biometrics, and the physical and security characteristics that currently allow for a very high level of proof that is a perfect match for professionals' requirements.

The second trend is related to the explosion in mobile phone SIM cards (3) and the emergence of electronic passports. These two new areas of development are leading to a change in the chip's medium. Chips are now used on media other than plastic cards. In view of the increasing number of applications, credit cards, the traditional form for the chip market, is therefore required to cohabit with other formats:

- **Plug-in:** this format is used with mobile phones and enables users to be authenticated, so that they can access the network. Current developments focused on this format are aimed at incorporating large capacities of "personal" memory for storing music and ultimately videos, whether or not associated with DRM systems (Digital Right Management).

(1) 1 469 million microprocessor cards were marketed last year, compared to 845 million memory cards. According to Eurosmart, the figures this year should be 1 727 million and 780 million respectively. Five years ago, the situation was the complete opposite: there were 1 031 million memory cards and only 398 million microprocessor cards.

(2) As opposed to static or so-called weak authentication, which may be replayed, as it always uses the same secrets or only computes using the same secrets.

(3) Last year, the market for SIM cards (plug-in format), with an increase of 57%, represented 1 050 million smart cards, in other words 71.4% of microcontroller cards. Next year, the number of smart cards not in credit card format may total around 1 300 million cards, according to Eurosmart, representing 75.3% of microprocessor cards.

- **USB flash drives:** this format is already used for authentication on the PC and accessing a server or web services. In actual fact, they often include a SIM card in plug-in format and may soon integrate large capacities of "personal" memory. The technological advantage over a smart card is obviously the method of connection: no reader is required - it can be plugged straight into any USB port.

- **Contactless chip:** this solution takes a bare chip and combines it with a paper or plastic medium and an aerial. It is suited to all possible forms (key cases, collars, rings, passports, visas, USB flash drives, credit cards, and so on). Visa and MasterCard are planning to use it for small payment applications (PayPass). Microsoft is going to use it for all its employees worldwide as an access "key" for its buildings and any workstation. Finally, a good many governments are looking to implement it in passports. The chip will contain authentication elements, such as biometric data associated with the holder.

A response to protecting private life

Because it is a personal and portable object and also since it is tantamount to a safe, the smart card offers means for controlling the data contained that are much more far-ranging than those featured by a centralised, even secure database. CNIL, the French data protection watchdog, has already picked up on this advantage. Although cryptography algorithms are available for authenticating holders without knowing their identity, the protection of private data today is primarily a legislative issue. These laws have to rely on a technical arsenal developed by industry to protect passports, such as against unexpected intrusions or direct attacks on the chip.