Cryptographic Smart Cards

[Published in *IEEE Micro* **16**(3):14–24, 1996. Japanese version in *Nikkei Electronics* **12**:95–110, 1996.]

David Naccache and David M'Raïhi

Gemplus PSI - Cryptography Department
1 Place de la Méditerranée, F-95200, Sarcelles, France
email: {100142.3240, 100145.2261}@compuserve.com

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, which brings maximum security to the overall system in which the cards participate.
Smart-cards also provide special-purpose microcontrollers with built-in, self-programmable memory. Together these features make the cost of a malevolent attack far greater than the benefits.

In 1996, 600 million IC cards will be manufactured throughout the world. This articles surveys the existing crypto-dedicated microprocessors and describes some of their possible evolutions.

—As cryptography progresses, semiconductor manufacturers are introducing new silicon geometries and cryptographic refinements at a very fast pace.

What Is a Smart Card?

The idea of inserting a chip into a plastic card is as old as public-key cryptography. The first patents are now 20 years old but practical public-key applications emerged only a few years ago, however, because of previous limitations in the storage and processing capacities of circuit technology. New silicon geometries and cryptographic processing refinements lead the industry to new generations of cards and more ambitious applications such as RSA [1], the US Digital Signature Standard [2], or the Russian Gost 34.10.

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

The physical support of a conventional smart-card is a plastic rectangle printed with information—even advertising—concerning the application or the