Smartcards: Portable Security

J.-P. Thomasson
SGS-THOMSON Microelectronics, Smart Card Division, Rousset, France
L. Baldi
SGS-THOMSON Microelectronics, Central R&D, Agrate Brianza, Italy

Abstract
Smartcards are one of the fastest growing market segments in the field of Microelectronics, since they offer an easy way to implement secure transactions. In this paper we will consider the main characteristics of smartcards, with special regard to the ones used for secure transactions, and discuss the main market and technology trends.

1. Introduction
In 1996 the smartcard market increased by around 100%, including a growth of around 700% in banking applications. There are several reasons for this explosive growth: on one side the technology has come of age, making available cards with enough computing and data storage capabilities, on the other side the smartcard industry has now a complete technical and commercial infrastructure, including software suppliers, subcontractors, high level commercial co-operation and now even international security standards. Applications include GSM mobile phones, pay TV, ID cards, banking electronic purse, health cards, access control and tickets for public transports. Even if the present growth rate is impressive, current estimates are even more optimistic, suggesting for the next five-six years an average growth rate of 47%. Evolution in technology, in security features and in overall system architecture will support the further growth of this market segment.

2. A short history
Smartcards are similar to conventional credit cards, but contain an embedded silicon chip that provides additional features, like the storage of data, and the possibility of performing security checks. The basic patent on smartcards was registered in 1974 by Roland Moreno, but at the moment there were severe technical and commercial problems for the practical implementation of the idea, for the lack of a suitable silicon and packaging technology, and of commercial infrastructures.

It took almost four years to reach the technology level to produce the first chip card devices. Prototypes were produced by SGS-THOMSON in Italy in 1978 for telephone applications, making use of the recently discovered EPROM technology. The chip card was quite simple, with minimum logic and only 128 bits of memory, and gave only the possibility of erasing used phone units. Pioneering work took place also in France, leading to patents and first commercial products in 1981.

The first application of chip cards (not yet very smart!) was in France and Germany, in the field of phone cards. With the progress of Microelectronics, the quantity of logic and memory that could be stored in a card increased rapidly, and in 1985 the first bank cards were...
produced. From this moment on, the idea started getting widespread acceptance, and in the early 90’s, chip manufacturers were able to produce smartcard chips with built-in "anti-hacking" mechanism, based on 8-bit micro-controllers. Since that moment, having the major technical problems been solved, the diffusion of the smartcards has been limited mostly by the time needed to build infrastructures and establish the required commercial and legal agreements, and by the large initial costs required to replace the existing system based on magnetic stripe cards. This last point has lead to the paradox that third world countries, starting from a "clean slate" situation, have been quicker in introducing chip cards than most European countries.

At present the smartcard market is still mainly an European one, as it is shown in Fig.1, one of the reasons being the push of some European PTT offices, mainly in France and Germany, towards the introduction of advanced technologies. Not surprisingly, also the main smartcard manufacturers are European, as shown in Fig.2, even if the picture is likely to change, once the smartcard market start developing also in U.S.A. and Asia, probably through joint ventures with local manufacturers.

### 3. Smartcard Technology Today

The total size of a smartcard chip is fixed to less than 25mm$^2$, essentially for mechanical consideration: smart card chip have to be embedded in thin plastic cards, that are likely to end up in the back pocket of trousers, inside the wallet. Very thin packages have to be used, and also the thickness of the wafer must be reduced to around 180µm by back-lapping, before assembly, which can create mechanical yield problems. Anyhow a smaller chip size, around 15mm$^2$, is preferred, because it allows for cheaper card manufacturing.
The organisation of a state-of-the-art smart card, belonging to the ST19 family by SGS-THOMSON, is shown in Fig.3: it includes a micro-controller, usually an 8-bit core, with its own clock generation, some amount of ROM, for the operating system, SRAM for temporary data storage and EEPROM memory for non-volatile data and application specific software. However, if a reasonable degree of security is required, additional logic must be added:

- a dedicated co-processor, for performing all operations related to cryptography;
- control logic for memory management, preventing unauthorised access and modification of memory blocks;
- voltage detection circuitry, to prevent the chip from being operated in marginal conditions;
- passivation sensors, that prevent chip operation when the final passivation is removed;
- pseudo-random number generator.

In smartcards, I/O pads are not a concern, since in the standard configuration, there are only six contacts available on the card.

At present, the most advanced smartcards, by SGS-THOMSON, Siemens or Motorola, make use of 0.7-0.6μm technology, and embed up to 64K EEPROM memory. This technology could be considered rather obsolete, now that 0.35μm logic is widely available, but a few points should be taken in consideration: most of card readers still make use of 5V power supply, which impose some constraint on technology, embedding EEPROM requires some dedicated process tuning, since high internal voltages are required for programming, and, last but not least, security is achieved also through the use of a well mastered and characterised technology.

4. Market Drivers

The range of applications for smartcard is very large, and covers all aspects of payment, personal identifications and data storage. A list of the main applications and of the foreseen market in year 2000 is given in Tab.1. It is obvious that requirements, both in terms of security and memory size, are very different for phone cards, on the low end of the spectrum, and banking or ID cards, and the cost and development effort change accordingly.
In the next five years or so the market will be driven by the field of secure transactions, which includes electronic purse, electronic shopping (e.g. via Internet) and smart bank cards. This market has four main needs:

- **Multifunction** capability: that is the capability of upload and run more than one application. This need is a natural consequence of the increasing proliferation of applications: since the users are not willing to carry a large number of cards, there will be an increasing demand towards the combination of different functions on the same card. The technical requirements are for a large memory, to support different types of application software, and:

- **Secure application segregation**, that is the ability to guarantee that each application is secure from others, to prevent the users to charge improper costs to one of the applications, and to guarantee that a breach in the security of one of the applications is not affecting the others. However the technical problems appear to be of second order, compared with the legal and commercial ones.

- **Reloadability**, including on-line reloading is another key requirement, especially for electronic cash, but will become increasingly important also to replace throw-away cards, for example in phone cards and transport applications.

- **Cryptographic** capabilities are then required for secure applications, especially all those implying transactions performed on open nets, like phone lines or Internet. A significant progress has been achieved with the introduction of the asymmetric key algorithm, also called public key algorithm, essentially based on the decoupling of the encryption and decryption functions. With this method is possible to release to a wide public the encryption key, enabling for example all customers to send encrypted messages to the same bank, without giving them the possibility to read each other messages, or, on the contrary, it is possible for one person to release the decryption key to several service providers, allowing them to identify the sender of the message, without allowing any of them to reproduce it. In this way secure communications and electronic signature are possible.

5. **Technology Trends**

In general smartcards must package a certain amount of logic and non volatile memory in a limited space, therefore any increase in card performances requires a more effective technology.
The market drivers can be translated into four main technology requirements:

- increased memory capacity
- greater processing power
- higher security
- lower power and contactless operation

**More memory** is required to store codes, user data and application programs. In addition to the growing complexity of programs, the use of multiapplication cards increase the memory requirements by one order of magnitude. At the moment, the ROM that holds fixed system and user code can be up to 64Kbyte, while the Non Volatile Memory that holds user data and application programs can be up to 32Kbyte. A small amount of SRAM is also needed as high speed buffer, and to store temporary data. At the moment the Non Volatile Memory is essentially EEPROM, because of its greater flexibility (byteerasability) and low power dissipation, even if rather more expensive in terms of area. If memory requirements are going to increase as expected, Flash memory could be considered for program storage, due to its smaller area/byte, even if some amount of EEPROM would be anyhow needed, for data storage. A mixed technology like “Flash-plus”, recently announced by SES-THOMSON, that mixes both functions on the same silicon could be the best compromise. The main constraints are anyhow cost of technology and power dissipation.

**More processing power** is requested to handle in a short time all the operations requested by the application, and the security verification. Traditionally smartcards have been using 8-bit micro's, also because of area constraints, and the introduction of security systems based on asymmetric algorithms, requiring complex calculations, has been solved with the addition of a dedicated co-processor. However a request for more processing power comes from different sources: more complex applications, the use of high level languages, that need to be compiled, more security, especially for multifunction cards. The improvement in technology, which allows to increase the micro-controller clock frequency, and the preparation of dedicated software libraries, have helped a lot on this way, but for the future the use of more powerful processing machines, based on 16-bit or 32-bit cores is mandatory. It will be then possible to avoid the dedicated co-processor, and cryptography will be no longer "hard-wired" in the circuit, increasing system flexibility.

**More security** is needed to prevent the ever increasing risk of frauds. We must not forget that the same technological evolution, that allows to produce better smartcards, is also giving to hackers more powerful tools to crack them. Security of smartcards is a combination of technology and system and chip design. Technology must be robust and safe, in the first place by avoiding that any marginality can be exploited by hackers, and in the second place by adopting proper process solutions, for example to avoid that the content of a ROM memory could be read by microscope inspection, or that EEPROM content could be changed with a carefully targeted E-beam. Design must take into account also memory organisation, especially important for multiapplication cards, powerful cryptographic tools, and the co-development of chip architecture and operating system. As an example, in Fig.4 is given an estimation of the effort needed to crack different types of cards, when standard, or dedicated firmware is used. Flexibility, and the possibility of up-grading codes or introducing more complex cryptography systems are also powerful tools. However, since the security of a system depends on its weakest link, increase of security can come only from a global
Fig 4: effort needed to hack different generation smartcards with std. or dedicated firmware.

Stripe to chip cards, in spite of the huge costs of conversion.

**Contactless operation** is based on a radio frequency coupling, rather than on a mechanical one, between the card and the reader. It covers essentially two fields:

- **proximity operation**, in which the time of the transaction is longer than the card insertion time, like for phone and banking cards. In this case the advantage is essentially in the elimination of the mechanical wear of card and reader contacts. The card is anyhow inserted in a reader, good radio frequency coupling is possible, and power and speed are not critical issues.
- **remote operation**, for example for highway tolls, parking, public transportation, where a fast throughput is requested, and the card should be able to interact with the reader, without the need of insertion.

Fig 5: scheme of the operation of a RF-coupled contactless smartcard.

In general contactless operation requires the availability of a coupling inductance, which could be inserted in the card, and not on the chip, and of an analogue circuitry to extract power and signal from the incoming radio frequency, separate them, rectify and stabilise the power to supply the circuit, and modulate the return signal, as shown in Fig 5. In remote operation there is the additional request of low power dissipation, and fast Non
Volatile Memory storage, because the power source could be far and moving. Contactless cards are available today, some of them based on more exotic technologies, like ferro-electric, but do not match yet the security level of contact cards. Secure operation requires processing power, and therefore the main technology demand will be for a logic circuit operating at very low voltage, ideally around 1 V. Power dissipation in the memory will probably be of second order importance, the most important thing being the programming time.

6. Conclusions

Like most semiconductor applications, the smartcard market needs ever increasing performance and flexibility at ever decreasing cost. From the point of view of the main technological constraints: high packing density, large processing power and low dissipation, the smartcard, and especially the contactless one, can be considered as the extreme representative of the nomadic electronics, and therefore could become one of the drivers for semiconductor technology evolution towards small feature size and low voltage optimised processes. However the smartcard industry has also a unique focus on security, and since security is a property of the complete system, all participants in the supply chain, from the chip manufacturer to the final service provider, must co-operate closely to achieve the target. One of the most important criteria for success in the future will therefore be the ability to form and develop effective partnerships at all levels.