

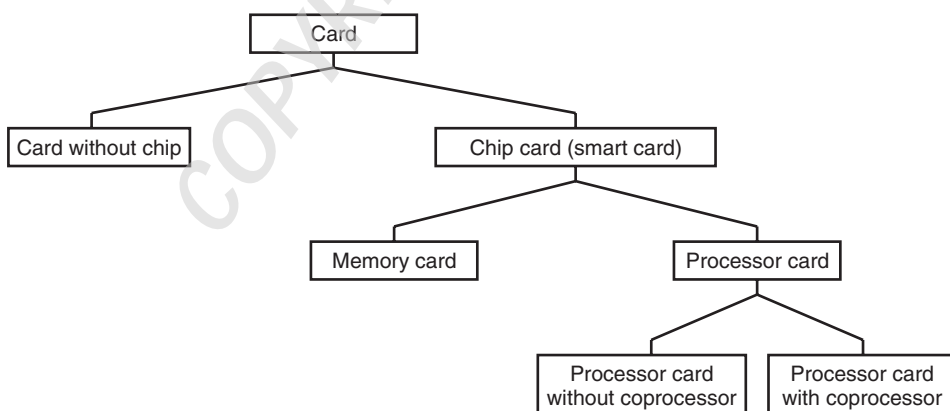
## Chapter 1

# Overview of Smart Cards

In contrast to information technology practices in the PC realm, the development and functionality of smart cards are strongly driven by international standards. The reason for this is that interoperability and interchangeability are very important factors for smart cards. From the very beginning, this has fostered specification of their characteristics in standards. Another significant factor is that none of the suppliers of smart card hardware or software has ever held a monopoly position.

### 1.1 Card Classification

If you were to classify smart cards in the same manner as living beings in biology, you would obtain a tree chart similar to what is shown in Figure 1.1. The top level includes all types of cards, which can have various formats.



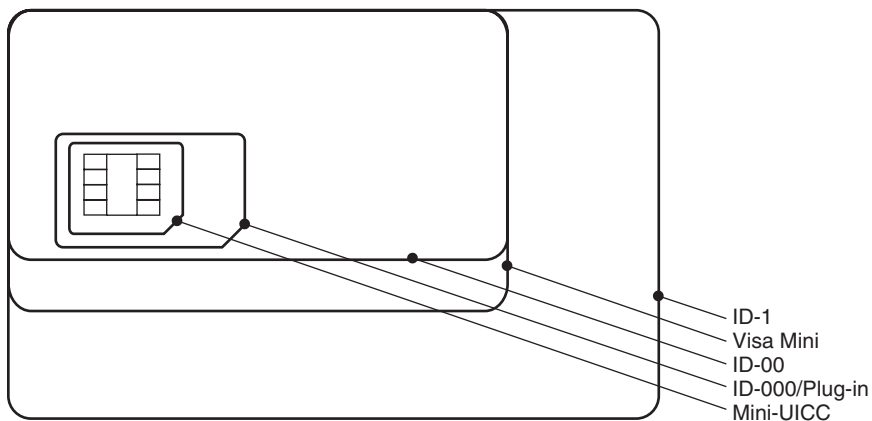
**Figure 1.1** Classification of cards with and without chips

Cards can be divided into cards without chips and cards with chips. Logically enough, the latter type are called *chip cards*, which are also commonly known as *smart cards*. The chip, which is the essential distinguishing element, can be either a memory chip, in which case the card is called a *memory card*, or a *microcontroller chip*, in which case the card is called a *processor card*. Processor cards can be further subdivided into processor cards with or without coprocessors for executing asymmetric cryptographic algorithms such as RSA (Rivest, Shamir and Adleman) or ECC (elliptic curve cryptosystems).

This classification provides an adequate overview of the most widely used types of cards. However, it can also be extended to include devices that use smart card technology. The best-known examples of such devices are ‘super smart cards’ and tokens. A super smart card has a direct user interface to the smart card microcontroller, in the form of additional card elements such as a display and buttons. A token has a different form that is better suited to its intended use than the usual card format. Typical examples include tokens in the form of USB plugs that can be connected directly to a PC. However, the underlying technology is still the same as that of smart cards, with only the appearance being different.

## 1.2 Card Formats

The most common types of cards in current use have one feature in common, which is a thickness of 0.76 mm. As illustrated in Figure 1.2, all other dimensions can differ. These formats are not arbitrary. Instead, they are specified by international standards or by specifications stipulated by major card issuers. This is also important, since at least in case of contact cards they must be able to fit into corresponding terminals or readers.



**Figure 1.2** Relative sizes of commonly used card formats

Typical smart card formats are summarised in Table 1.1. The most commonly used card format, which is also undoubtedly the best known format, is ID-1. The reason it is so widely used is that practically all credit cards and other forms of payment cards are made

**Table 1.1** Summary of typical card formats. All stated dimensions are exclusive of tolerances. All formats have the same thickness: 0.76 mm

Card Format	Width (mm)	Height (mm)	Use
ID-1	85.6	54	Well-known standard format
ID-00	66	33	Standardized for telecommunications, but not used
Visa Mini	65.6	40	Payment systems
Plug-in, ID-000	25	15	Telecommunications
Mini-UICC	15	12	Telecommunications

in this format. The plug-in format for smart cards used in mobile telecommunications applications is also very common. Another name for this format is ID-000. This has become the standard format for cards used in mobile telephones.

The recently defined mini-UICC format is also available for the mobile telecommunications sector. It was developed in response to the ongoing miniaturization trend that prevails in this sector. The Visa Mini format is a smaller version of the ID-1 format. It is intended to meet customer demand for cards with the smallest possible dimensions.

Cards with shapes other than the usual rectangular card body are also being made now. For example, there are cards with one corner rounded at a large radius and cards shaped in the outline of an animal. The constraints with respect to the shape of contact cards are that they must fit into the slot of an ID-1 terminal, be readily removed from the terminal after use, and make reliable electrical contact with the terminal. Incidentally, most cards with special shapes are made by stamping them from cards in ID-1 format to achieve the desired shape.

## 1.3 Card Elements

The card body is usually more than just a carrier for the chip module. It also includes information for the user and card accepters and of course security elements for protection against forgery. Furthermore, the card body is an excellent advertising medium. The card issuers must coordinate all these functions, some of which are mutually contradictory, with their own specific wishes. The ultimate result is the issued card.

### 1.3.1 Printing and labelling

A rather wide variety of processes are available for printing and labelling cards. Text elements that are common to all cards of a series are normally applied using offset printing or silkscreen printing, but sheet printing and individual card printing processes are also used.

Lasering is widely used for printing individual cards. This consists of using a laser beam to darken the surface of the plastic card body. This process produces irreversible card labelling, but it requires a certain amount of investment in technology. A more

economical alternative is thermal transfer printing, which can also be used for colour printing. One of the drawbacks of this method is that the colour layers are located close to the surface of the card, so they can be removed almost completely. Digital printing processes for high-quality printing of individual cards are a relatively new development.

### **1.3.2 Embossing**

The main advantage of embossing, which is commonly used with credit cards, is that the labelling can be transferred to paper using a simple stamping machine. The embossed section of the card can be restored to its original state by heating the card to a relatively high temperature. For this reason, the check digits at the end of the embossing usually extend into the hologram area. As the hologram will be visibly damaged if the card is heated, this makes it relatively easy to detect manipulation of the embossing.

### **1.3.3 Hologram**

Technically sophisticated equipment is necessary to produce the white-light reflection holograms used on cards. As forgers usually do not have access to such equipment, holograms are commonly used on smart cards as security features. Some other reasons for using holograms are that they are inexpensive in large quantities, they can be checked directly by users, and the hologram cannot be removed from the smart card without destroying it. Unfortunately, there is no link between the hologram and the microcontroller, which reduces its advantages from the perspective of the chip.

### **1.3.4 Signature panel**

The signature panel is located on the rear of the card. It must be erasure-proof so that the signature on the panel cannot be removed without it being noticed. A coloured pattern is often printed on the signature strip, so any attempt to manipulate the signature will cause visible damage to the pattern.

### **1.3.5 Tactile elements**

Tactile elements can be applied to the card to enable visually impaired and blind people to recognize the orientation of the card. The best known example is a semicircular recess in one of the long edges of the card. The hole punched in some payment cards is also suitable for use as an orientation aid, although its original purpose was to allow the card to be hung from a strap or cord.

### **1.3.6 Magnetic stripe**

With many types of cards, the only reason to retain the magnetic stripe (with its data storage capacity of a few hundred bytes) is compatibility with a widely distributed terminal infrastructure. However, it will still take a long time before magnetic-stripe cards are fully replaced by smart cards, since they are significantly cheaper.

### 1.3.7 Chip module

The chip module is a protective housing for the microcontroller chip, which is fitted to the rear of the module. The module can have six or eight visible contacts on its external surface, although modern smart cards need only five contacts. The other contacts are reserved for future applications. The microcontroller is glued to the rear of the contact substrate and electrically connected to the contact surfaces on the front side by thin bonding wires. Figure 1.3 shows the signal assignment of the contacts of a chip module.

C1		C5	Vcc		GND	Vcc		GND
C2		C6	RST		SPU	RST		SPU
C3		C7	CLK		I/O	CLK		I/O
C4		C8	AUX1		AUX2			

**Figure 1.3** Contact assignments of a smart card module. Abbreviations: Vcc = Supply voltage, RST = Reset, CLK = Clock, AUX1 = Auxiliary 1, GND = Ground, SPU = Standard or Proprietary Use, I/O = Input/Output, AUX2 = Auxiliary 2

### 1.3.8 Antenna

Smart cards that communicate without using contacts must have an integrated antenna in the card body. The antenna is a sort of coil consisting of several turns along the outer edge of the entire card. Various methods can be used to produce the antenna. Methods that are used in practice include a coil of thin copper wire embedded in the card body, etched copper tracks, and printed coils.

## 1.4 Smart Card Microcontrollers

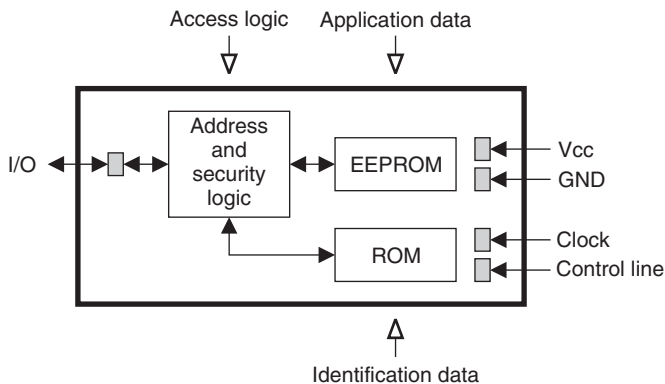
The characteristics of a smart card are largely determined by its microcontroller. Single-chip microcontrollers are normally used. A single-chip microcontroller consists of a small silicon chip equipped with all the functions necessary for its intended use. Smart card microcontrollers are not standard microcontrollers such as those used in coffee machines and toasters, but are instead chips specially adapted for use in smart cards. The adaptations encompass electrical and physical parameters such as the maximum current consumption, the range of allowed clock frequencies, and the allowable temperature range.

Besides all these functional parameters, there is another essential item: security functions. Smart card microcontrollers are specially hardened against attacks. This includes detecting undervoltage and overvoltage conditions and detecting clock frequencies outside the specified range. These microcontrollers also incorporate light and temperature sensors to enable them to recognize attacks via these routes and respond accordingly.

However, these are only relatively simple protective mechanisms. There are also relatively complex methods, which are quite widely used, such as scrambling all the memories and the busses between the processor and the memories. It is even possible to

periodically swap the scrambling key during an individual session. The microcontroller hardware can even defend against hard attacks such as measuring its current consumption in order to perform a statistical analysis to discover which data was processed by the processor.

Besides technologically advanced smart card microcontrollers, there are also memory chips which are essentially intended to be used as simple data storage devices with fixed logic circuitry designed by the semiconductor manufacturer. Figure 1.4 shows the basic functional groups present on the chip. The ROM (read-only memory) contains data about the chip type. The EEPROM (electrically erasable programmable read-only memory) provides the storage area for a unique chip identification number and data stored in read/write memory. A terminal can store several hundred bytes to a few thousand bytes of data here.

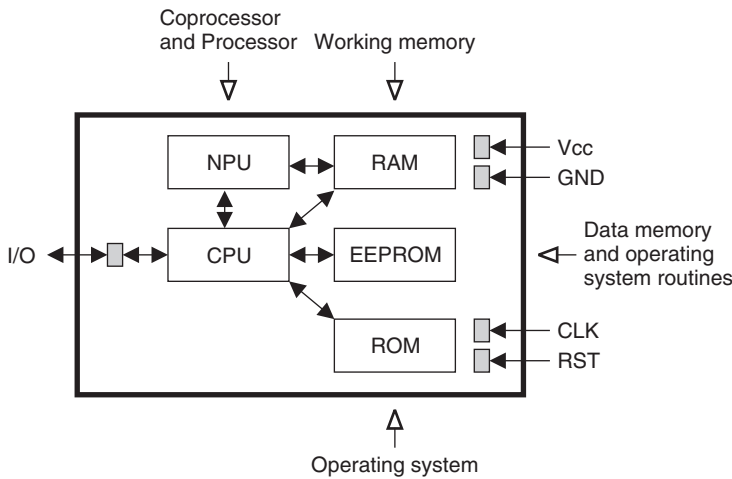


**Figure 1.4** Block diagram of a memory chip for a smart card with a contact interface

The security logic, which varies according to the chip type, monitors access to the data. For instance, successful verification of a PIN (personal identification number) in the memory chip may be necessary before write access is possible.

Telephone cards, which are chip cards that can be used with public pay phones, have a similar operating principle. The security logic of a telephone card incorporates an authentication algorithm so that the telephone can determine whether it is dealing with a genuine chip card. If the card is genuine, a counter in the EEPROM is decremented according to the duration of the call. This counter can only count down, and it stops when it reaches zero. When this happens, the card has been used up.

Microcontrollers for smart cards have significantly more functionality than simple memory chips, as can be seen from Figure 1.5 on the facing page. The CPU (central processing unit) is a freely programmable control unit that executes the machine instructions of the operating system, which is located in the ROM. The CPU is assisted by a numerical coprocessor (NPU – numeric processing unit) for numerical calculations, particularly those dealing with cryptography. These special processors combine extremely high performance with low power consumption. Operating system extensions and the actual



**Figure 1.5** Block diagram of a microcontroller for a smart card with a contact interface

applications and associated data are stored in the EEPROM. Just as in a PC, the RAM (random-access memory) serves as working memory to hold data during operation.

These functional groups must all be integrated in a single chip that is limited to a maximum size of  $25 \text{ mm}^2$  for reasons of strength and robustness. As a consequence, the amount of available memory is many orders of magnitude less than what is commonly found in a modern PC. The ROM capacity of smart card microcontrollers typically ranges from 16 to 400 KB, the EEPROM capacity ranges from 1 to 500 KB, and the RAM size ranges from 256 bytes to 16 KB. These wide ranges are due to the wide variety of application areas. The simplest processor cards do not even have an operating system, but instead contain only the application software. At the other extreme, smart cards currently at the top of the technology ladder fully exploit all the available memory.

These memory sizes are quite normal in the embedded applications area, but they are mini-memories compared with the memories of modern PCs. Nevertheless, the semiconductor technology of smart card microcontrollers is comparable to the technology used to manufacture modern high-performance processors, since integrating the various memory technologies and the necessary hardening against attacks is rather difficult. The microcontrollers are fabricated using semiconductor processes with 90-nm technology, which is only one development step away from the current state-of-the-art 65-nm technology.

Additional interfaces are integrated into smart card microcontrollers to expand their range of potential uses. For instance, the commonly used half-duplex bit-serial port can be augmented by a USB interface or a wireless communication interface. Semiconductor manufacturers usually base such developments on existing smart card microcontrollers, which are upgraded to support the additional interfaces. The result is thus a single-chip microcontroller that can communicate with the outside world via additional interfaces.

### 1.4.1 Processor

If you analyse the sales volumes of currently used smart card microcontrollers, you will find that most of them still have an 8-bit CPU. This is usually a simple 8051 CPU, which has proved itself over the last two decades, along with a few extensions. The processing power of such a CPU is sufficient for all operating systems that do not include an interpreter. However, if the operating system must provide a Java interpreter, there is a distinct preference for microcontrollers with 16-bit processors. Some of these processors are also based on a modified 8051 architecture.<sup>1</sup>

There are also a few smart card microcontrollers that are based on well-known 32-bit processor families such as ARM 7 or MIPS. The limiting factor for using such high-performance processors is the chip area. There is a more or less direct relationship between chip area and price, and a 32-bit processor occupies a significantly larger area than an 8-bit processor. It is often more economical to invest in optimizing the speed of the software than to use a processor that needs more chip area. This is ultimately a consequence of the fact that smart cards have to be low-cost, mass-production items.

### 1.4.2 Memory

In addition to a processor, every microcontroller needs several types of memory with differing characteristics. The main type of nonvolatile memory used in smart card microcontrollers is ROM. If the data located in memory must be modified in operation, electrically erasable memory (EEPROM) is used.

Besides microcontrollers with ROM and EEPROM, a steadily increasing number of chips with flash memory are being used. Flash memory is a sort of EEPROM with reduced cell dimensions, but unlike EEPROM it cannot be erased or written byte-wise. Flash memory can take over the functions of ROM and EEPROM.

EEPROM and flash memory are similar in that they cannot be erased and written an unlimited number of times and these accesses cannot occur at the full speed of the processor. Currently, the erase and write times are typically 3.5 ms each, and the guaranteed number of such accesses is 500 000. This has a major impact on the design of the operating system and application software.

Static RAM is used as volatile memory for storing data during operation.

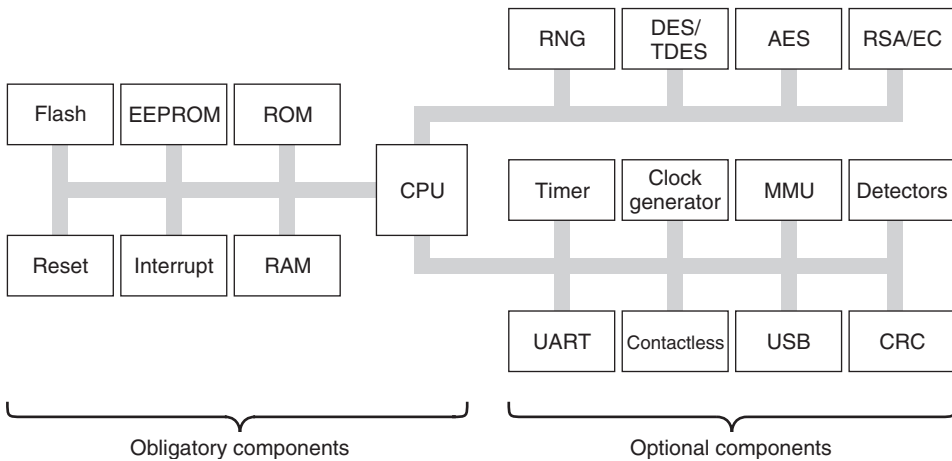
### 1.4.3 Supplementary hardware

Besides a processor and its associated memory, smart card microcontrollers incorporate various types of supplementary hardware. Figure 1.6 shows a large range of possibilities.

The clock signal required by the smart card is usually provided by the terminal. However, as the relevant standards restrict the frequency of this clock signal to a range of 1–5 MHz, more and more microcontrollers include internal clock multiplier or clock generator circuitry.

---

<sup>1</sup> If you are willing to generate the time-critical parts of the operating system in assembly language instead of C and invest a fairly significant amount of time in optimizing its real-time behaviour, it is certainly possible to develop an interpreter that will run at an acceptable speed on an 8-bit CPU



**Figure 1.6** Block diagram of a smart card microcontroller with a selection of currently common components linked to the CPU via a shared address, data and control bus. The ROM and EEPROM memories may be omitted in some types of microcontrollers if flash memory is used

A UART (universal asynchronous receiver transmitter) is included for bit-serial communication with the terminal, and in the case of smart cards with USB or contactless interfaces, the corresponding communication components are also present in the hardware.

Most of the supplementary hardware is related to cryptography, since considerable processing power is sometimes necessary for this purpose. Random numbers are almost always generated using a hardware random number generator, although the results are further processed in software before being used. Symmetrical cryptographic algorithms such as DES (Data Encryption Standard), Triple DES (TDES) and AES (Advanced Encryption Standard) are also usually present in hardware, and they generally require only a few clock cycles for full encryption or decryption.

Hardware for computing asymmetric cryptographic algorithms is not generally included in all microcontrollers, as it would increase the price. If it is present, it supports the usual algorithms such as RSA (Rivest, Shamir and Adleman cryptographic algorithm), DSA (digital signature algorithm) and ECC (elliptic curve cryptosystems). The hardware implementation of such algorithms is always kept relatively modular to enable it to support various key lengths and versions, extending as far as key generation.

#### 1.4.4 Electrical characteristics

In mobile telecommunication applications, low power consumption of all components of a mobile telephone is a visible feature even for end users, since it directly affects the speech and standby times of the telephone. The mobile telecommunication sector has thus developed into a driver for smart cards with the lowest possible operating voltages and current consumptions. This is in full contrast to all terminals connected directly to

**Table 1.2** Voltage classes as specified by ISO/IEC 7816-3. The stated maximum clock rate is a typical value, which can optionally be changed to a wider range (4–20 MHz). The terminal must be informed of this via the ATR

Voltage Class	Voltage	Clock Frequency	Current Consumption
Class A	5 V ( $\pm 10\%$ )	1–5 MHz	60 mA maximum at maximum clock frequency
Class B	3 V ( $\pm 10\%$ )	1–5 MHz	50 mA maximum at maximum clock frequency
Class C	1.8 V ( $\pm 10\%$ )	1–5 MHz	30 mA maximum at maximum clock frequency

the mains network, for which the current consumption of the smart card is practically an insignificant issue.

Voltage class A, with a 5-V supply voltage and (originally) a maximum allowable current consumption of 200 mA, has completely disappeared in mobile telephone applications. The current state of the art is still voltage class B, with a clearly visible trend in the direction of the 1.8-V C class, as summarized in Table 1.2. On the other hand, 5-V smart cards are still commonly used in payment systems.

Incidentally, modern smart cards can usually work with all three voltage classes. However, the processing power may decrease with decreasing supply voltage. This is due to the internal frequency multiplication of the chip, which depends on the amount of power available.