# 1
# Introduction



This book is intended for students, engineers, and technically minded persons who want to learn more about smart card technology. It attempts to cover this broad topic as completely as possible, in order to provide the reader with a general understanding of the fundamentals and the current state of the technology.

We have put great emphasis on a practical approach. The wealth of illustrations, tables and references to real applications is intended to help the reader become familiar with the subject much faster than would be possible with a strictly technical approach. Consequently, this book is intended to be practically useful instead of academically complete. This is also the reason for making the descriptions as illustrative as possible. In places where we were faced with a choice between academic accuracy and ease of understanding, we have tried to strike a happy medium. Where this was not possible, we have given the preference to ease of understanding.

The book is structured such that it can be read in the usual way, from front to back. We have tried to avoid forward references as much as possible. The structure and content of the individual chapters are formulated to allow them to be read individually without any loss of understanding. A comprehensive index and a glossary allow this book to be used as a reference work. If you wish to know more about a specific topic, the references in the text and the annotated directory of standards will help you find the relevant documents.

Unfortunately, a large number of abbreviations have become established in smart card technology, as in so many other areas of technology and everyday life. This makes it particularly difficult for newcomers to become familiar with the subject. We have tried to minimize the use of these cryptic and frequently illogical abbreviations. Nevertheless, we have often had to choose a middle way between internationally accepted smart card terminology used by specialists and common terms more easily understood by laypersons. If we have not always succeeded, the extensive list of abbreviations should at least help overcome any barriers to understanding, which we hope will be short-lived. An extensive glossary at the end of the book explains the most important technical concepts and supplements the list of abbreviations.

An important feature of smart cards is that their properties are strongly based on international standards. This is also essential for interoperability, which is a fundamental requirement in most applications. Unfortunately, these standards are often difficult to understand, and in some problematic places they require outright interpretation. Sometimes only the members of the relevant standardization group can explain the intended meaning of certain sections. In such

*Smart Card Handbook: Fourth Edition* Wolfgang Rankl and Wolfgang Effing

cases, *The Smart Card Handbook* attempts to present the meaning generally accepted in the smart card industry. Nevertheless, the relevant standards remain the ultimate authority, and in such cases they should always be consulted.

## 1.1 THE HISTORY OF SMART CARDS

The proliferation of plastic cards began in the USA in early 1950s. The low price of the synthetic material PVC made it possible to produce robust, durable plastic cards that were much more suitable for everyday use than the paper and cardboard cards previously used, which could not adequately withstand mechanical stresses and climatic effects.

The first all-plastic payment card for general use was issued by the Diners Club in 1950. It was intended for an exclusive class of individuals, and thus also served as a status symbol, allowing the holder to pay with his or her 'good name' instead of cash. Initially, only the more select restaurants and hotels accepted these cards, so this type of card came to be known as a 'travel and entertainment' card.

The entry of Visa and MasterCard into the field led to a very rapid proliferation of 'plastic money' in the form of credit cards. This occurred first in the USA, with Europe and the rest of the world following a few years later.

Today, credit cards allow travelers to shop without cash everywhere in the world. A cardholder is never at a loss for means of payment, yet he or she avoids exposure to the risk of loss due to theft or other unpredictable hazards, particularly while traveling. Using a credit card also eliminates the tedious task of exchanging currency when traveling abroad. These unique advantages helped credit cards become rapidly established throughout the world. Billions of cards are produced and issued annually.

At first, the functions of these cards were quite simple. They served as data storage media that were secure against forgery and tampering. General data, such as the card issuer's name, was printed on the surface, while personal data, such as the cardholder's name and the card number, was embossed. Many cards also had a signature panel where the cardholder could sign his or her name for reference. In these first-generation cards, protection against forgery was provided by visual features such as security printing and the signature panel. Consequently, the system's security depended largely on the experience and conscientiousness of the employees of the card-accepting organization. However, this did not represent an overwhelming problem, due to the card's initial exclusivity. With the increasing proliferation of card use, these rather rudimentary functions and security technology were no longer adequate, particularly since threats from organized criminals were growing apace.

Increasing handling costs for merchants and banks made a machine-readable card necessary, while at the same time, losses suffered by card issuers as the result of customer insolvency and fraud grew from year to year. It became apparent that the security features for protection against fraud and manipulation, as well as the basic functions of the card, had to be expanded and improved.

The first improvement consisted of a magnetic stripe on the back of the card, which allowed digital data to be stored on the card in machine-readable form as a supplement to the visual information. This made it possible to minimize the use of paper receipts, which were previously essential, although the customer's signature on a paper receipt was still required in traditional credit card applications as a form of personal identification. However, new approaches that rendered paper receipts entirely unnecessary could also be devised. This made it possible to

finally achieve the long-standing objective of replacing paper-based transactions by electronic data processing. This required a different method to be used for user identification, which previously employed the user's signature. The method that has come into widespread general use involves a secret personal identification number (PIN) that is compared with a reference number in a terminal or a background system. Most people are familiar with this method from using bank cards in automated teller machines. Embossed cards with a magnetic stripe and a PIN code are still the most commonly used type of payment card.

However, magnetic-stripe technology has a crucial weakness, which is that the data stored on the stripe can be read, deleted and rewritten at will by anyone with access to a suitable magnetic card reader/writer. It is thus unsuitable for storing confidential data. Additional techniques must be used to ensure confidentiality of the data and prevent manipulation of the data. For example, the reference value for the PIN can be stored in the terminal or host system in a secure environment, instead of on the magnetic stripe in unencrypted form. Most systems that employ magnetic-stripe cards thus use online connections to the system's host computer for reasons of security, even though this generates significant costs for the necessary data transmission. In order to minimize costs, it is necessary to find solutions that allow card transactions to be executed offline without endangering the security of the system.

The development of the smart card, combined with the expansion of electronic data processing systems, has created completely new possibilities for devising such solutions.

In the 1970s, rapid progress in microelectronics made it possible to integrate nonvolatile data memory and processing logic on a single silicon chip measuring a few square millimeters. The idea of incorporating such an integrated circuit into an identification card was contained in a patent application filed by the German inventors Jürgen Dethloff and Helmut Grötrupp as early as 1968. This was followed in 1970 by a similar patent application by Kunitaka Arimura in Japan. However, real progress in the development of smart cards began when Roland Moreno registered his smart card patents in France in 1974. It was only then that the semiconductor industry was able to supply the necessary integrated circuits at acceptable prices. Nevertheless, many technical problems still had to be solved before the first prototypes, some of which contained several integrated circuit chips, could be transformed into reliable products that could be manufactured in large numbers with adequate quality at a reasonable cost.

The basic inventions in smart card technology originated in Germany and France, so it is not surprising that these countries played the leading roles in the development and marketing of smart cards.

The great breakthrough was achieved in 1984, when the French PTT (postal and telecommunication services authority) successfully carried out a field trial with telephone cards. In this field trial, smart cards immediately proved to meet all expectations with regard to high reliability and protection against manipulation. Significantly, this breakthrough for smart cards did not come in an area where traditional cards were already used, but in a new application. Introducing a new technology in a new application has the great advantage that compatibility with existing systems does not have to be taken into account, so the capabilities of the new technology can be fully exploited.

A pilot project was conducted in Germany in 1984–85, using telephone cards based on several technologies. Magnetic-stripe cards, optical-storage (holographic) cards and smart cards were used in comparative tests.

Smart cards proved to be the winners in this pilot study. In addition to a high degree of reliability and security against manipulation, smart card technology promised the greatest

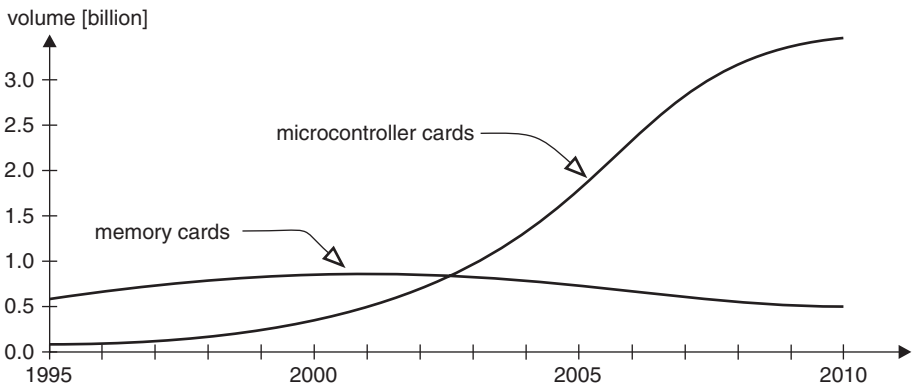


**Figure 1.1** Worldwide production figures for memory cards and processor cards. The numbers are estimated values, since the various sources differ considerably. Average values have been used here

degree of flexibility for future applications. Although the older but less expensive EPROM technology was used in the French telephone card chips, newer EEPROM chips were used from the start in German telephone cards. The latter type of chip does not need an external programming voltage. An unfortunate consequence is that the French and German telephone cards are mutually incompatible. Further developments followed the successful trials of telephone cards, first in France and then in Germany, with breathtaking speed. By 1986, several million 'smart' telephone cards were in circulation in France alone. The total rose to nearly 60 million in 1990, and to several hundred million worldwide in 1997.

Germany experienced similar progress, with a time lag of about three years. These systems were marketed throughout the world after the successful introduction of the smart card public telephone in France and Germany. Telephone cards incorporating chips are currently used in more than 50 countries. However, the use of telephone cards in their original home countries (France and Germany), as well as in highly industrialized countries in general, has declined dramatically in the last decade due to the widespread availability of inexpensive mobile telecommunication networks and the general use of mobile telephones.

The integrated circuits used in telephone cards are relatively small, simple and inexpensive memory chips with specific security logic that allows the card balance to be reduced while protecting it against manipulation. Microprocessor chips, which are significantly larger and more complex, were first used in large numbers in telecommunication applications, specifically for mobile telecommunication. The production trends of smart cards with memory chips (memory cards) and smart cards with microprocessor chips (microcontroller cards) in recent years are shown in Figure 1.1.

In 1988, the German Post Office acted as a pioneer in this area by introducing a modern processor card using EEPROM technology as an authorization card for the analog mobile telephone network (C-Netz). The reason for introducing such cards was an increasing incidence of fraud with the magnetic-stripe cards used up to that time. For technical reasons, the analog mobile telephone network was limited to a relatively small number of subscribers (around one million), so it was not a true mass market for processor cards. However, the positive experience gained from using smart cards in the analog mobile telephone system was decisive for the introduction of smart cards in the digital GSM network. This network was put into service in

1991 in various European countries and has presently expanded over the entire world, with more than three billion subscribers in nearly every country of the world.

Progress was significantly slower in the bank card area, in part due to the more stringent security requirements and higher complexity of bank cards compared with telephone cards. These differences are described in detail in the following chapters. Here we would just like to remark that the development of modern cryptography has been just as crucial for the proliferation of bank cards as developments in semiconductor technology.

With the widespread use of electronic data processing in the 1960s, the discipline of cryptography experienced a sort of quantum leap. Modern, high-performance hardware and software made it possible to implement complex, sophisticated mathematical algorithms in single-chip processors, which allowed previously unparalleled levels of security to be achieved. Moreover, this new technology was available to everyone, in contrast to the previous situation in which cryptography was a covert science in the private reserve of the military and secret services.

With these modern cryptographic algorithms, the strength of the security mechanisms in electronic data processing systems could be mathematically calculated. It was no longer necessary to rely on a highly subjective assessment of conventional techniques, whose security essentially rests on the secrecy of the methods used.

The smart card proved to be an ideal medium. It made a high level of security (based on cryptography) available to everyone, since it could safely store secret keys and execute cryptographic algorithms. In addition, smart cards are so small and easy to handle that they can be carried and used everywhere by everybody in everyday life. It was a natural idea to attempt to use these new security features for bank cards, in order to come to grips with the security risks arising from the increasing use of magnetic-stripe cards.

The French banks were the first to introduce this fascinating technology in 1984, after completion of a pilot project with 6000 cards in 1982–83. It took another 10 years before all French bank cards incorporated chips. In Germany, the first field trials took place in 1984–85, using a multifunctional payment card incorporating a chip. However, the Zentrale Kreditausschuss (ZKA), which is the coordinating committee of the leading German banks, did not manage to issue a specification for multifunctional Eurocheque cards incorporating chips until 1996. In 1997, all German savings associations and many banks issued the new smart cards. In the previous year, multifunctional smart cards with POS capability, an electronic purse, and optional value-added services were issued in all of Austria. This made Austria the first country in the world to have a nationwide electronic purse system.

An important milestone for the future worldwide use of smart cards for making payments was the adoption of the EMV specification, a product of the joint efforts of Europay, MasterCard and Visa. The first version of this specification was published in 1994. It provides a detailed description of the operation of credit cards incorporating processor chips, and it ensures the worldwide compatibility of the smart cards of the three largest credit card organizations. Hundreds of millions of EMV cards are presently in use worldwide.

With a delay of around ten years relative to normal contact smart cards, the technology of contactless smart cards has developed to the point of market maturity. With contactless cards, an electromagnetic field is used to supply power to the cards and exchange data with the terminal, without any electrical contact. The majority of currently issued EMV cards use this technology to enable fast, convenient payment for small purchases.

In the 1990s, it was anticipated that electronic purses, which store money in a card and can be used for offline payment, would prove to be another driver for the international proliferation

of smart cards for payment transactions. The first such system, called Danmønt, was put into service in Denmark in 1992. There are presently more than twenty national systems in use in Europe alone, many of which are based on the European EN 1546 standard. The use of such systems is also increasing outside of Europe. Payment via the Internet offers a new and promising application area for electronic purses. However, a satisfactory solution to the difficulties involved in using the public Internet medium to make payments securely but anonymously throughout the world, including small payments, has not yet been found. Smart cards could play a decisive role in such a solution.

The anticipated pioneering success of electronic purses has failed to materialize up to now. Most installed systems remain far below the original highly optimistic expectations, which among other things can be attributed to the fact that fees for online transactions have decreased dramatically, with the result that one of the key advantages of electronic purse systems – cost savings resulting from offline capability – has largely vanished. Today the electronic purse function is often included as a supplementary application in multifunction smart cards for payment transactions.

Another potentially important application for smart cards is as personal security devices for electronic signatures, which are slowly becoming established in several European countries after the legal basis for their use was created in 1999 when the European Parliament adopted an EU directive on digital signatures.

Another application has resulted the issuing of smart cards to nearly all the citizens of several countries. These smart cards serve as health insurance cards, which are issued to the insured persons and which contribute to cost savings in the billing of services to health insurance organizations. In most cases, the first cards to be issued were simple memory cards containing only the personal data of the insured person necessary for identification, but the patient cards now in common use contain complex security microcontrollers that also make it possible to store prescriptions and patient files, and to use electronic signatures to enable secure access to centrally stored data via the Internet.

The high functional flexibility of smart cards, which even allows programs for new applications to be added to a card already in use, has opened up completely new application areas, extending beyond the boundaries of traditional card uses.

As already mentioned, the technology of contactless smart cards has reached a level of maturity that enables economical mass production. For this reason, contactless smart cards are used as electronic tickets for local public transport in many cities throughout the world. In addition, this technology has established a firm position in electronic passports. Although electronic passports do not have the same size or shape as a credit card, which is standardized as an ID-1 card, under the cover they have the same circuitry as a contactless smart card, consisting of a security microcontroller connected to an antenna coil for contactless data exchange.

Intensive efforts are presently underway at the European level to achieve standardization of a contactless electronic card to be issued to all citizens, which will have an ID1 form factor (the same as a credit card) and is intended to be used as a personal identification card, among other things.

Although the history of smart cards and their applications goes back more than 25 years, a steady stream of promising new applications is still being developed. The increasing, almost omnipresent networking of our world creates major problems with regard to the security, confidentiality, and anonymity of personal data. Smart cards as personal security devices, with their ability to store and encode data securely, can make a major contribution to solving these problems.

## 1.2 CARD TYPES AND APPLICATIONS

As can be seen from the historical summary, the potential applications of smart cards are extremely diverse. With the steadily increasing storage and processing capacities of available integrated circuits, the range of potential applications is constantly expanding. Since it is impossible to describe all of these applications in detail within the confines of this book, a few typical examples must serve to illustrate the basic properties of smart cards. This introductory chapter is only meant to provide an initial overview of the functional versatility of these cards. Some typical application areas with their memory and processing capacities are shown in Figure 1.2, and several typical applications are described in detail in later chapters.

To make this overview easier to follow, it is helpful to divide smart cards into two categories: memory cards and processor cards.

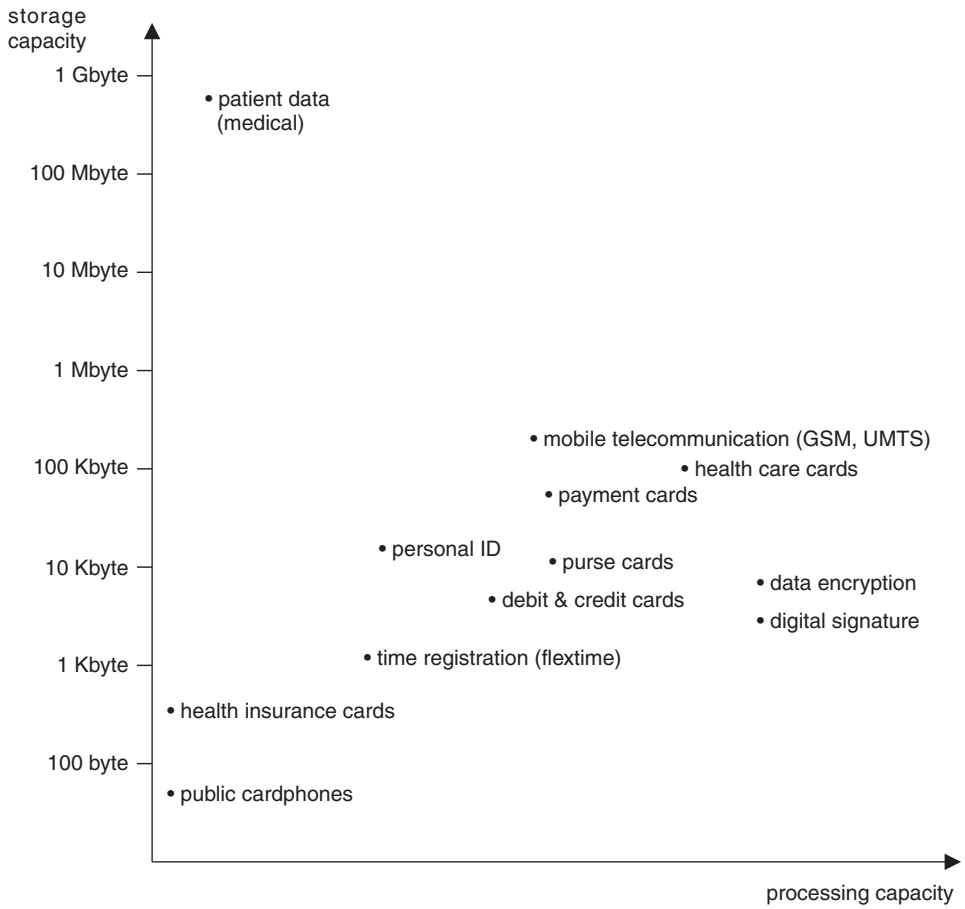


**Figure 1.2** Typical smart card application areas, and the required memory capacity and arithmetic processing capacity

### 1.2.1 Memory cards

The first smart cards used in large quantities were memory cards for telephone applications. These cards are prepaid, with the value stored electronically in the chip being decreased by the amount of the calling charge each time the card is used. Naturally, it is necessary to prevent the user from subsequently increasing the stored value, which could easily be done with a magnetic-stripe card. With such a card, all the user would have to do is record the data stored at the time of purchase and rewrite it to the magnetic stripe after using the card. The card would then have its original value and could be reused. This type of manipulation, known as buffering, is prevented in smart phone cards by security logic in the chip that makes it impossible to erase a memory cell once it has been written. Decreasing the card balance by the number of charge units used is thus irreversible.

This type of smart card can naturally be used not only for telephone calls, but also whenever goods or services are to be sold against prior payment without the use of cash. Examples of possible uses include local public transport, vending machines of all types, cafeterias, swimming pools, car parks and so on. The advantage of this type of card lies in its simple technology (the surface area of the chip is typically only a few square millimeters), and hence its low cost. The disadvantage is that the card cannot be reused once it is empty, but must be discarded as waste – unless it ends up in a card collection.

Another typical application of memory cards is the German health insurance card, which has been issued since 1994 to all persons enrolled in the national health insurance plan. The information previously written on the patient's card is now stored in the chip and printed or laser-engraved on the card. Using a chip for data storage makes the cards machine-readable using simple equipment. However, the next generation of German health insurance cards will have a security microcontroller and significantly expanded functionality.

In summary, we can say that memory cards have limited functionality. Their integrated security logic makes it possible to protect stored data against manipulation. They are suitable for use as prepaid cards or identification cards in systems where low cost is a primary consideration.

### 1.2.2 Processor cards

As already mentioned, processor cards were first used as bank cards in France. Their ability to store secret keys securely and to execute modern cryptographic algorithms made it possible to implement highly secure offline payment systems.

As the processor embedded in the card is freely programmable, the functionality of processor cards is restricted only by the available memory and the computing power of the processor. The only limits to the designer's imagination when implementing smart card systems are thus technological, and they are extended enormously with each new generation of integrated circuits.

As the prices of processor cards steadily decline due to mass production and ongoing technological progress, more and more new applications are developed. The use of smart cards with mobile telephones has been especially important for their international proliferation.

After being successfully tested in the German national C-Netz (analog mobile telephone network) for use in mobile telephones, smart cards were specified as the access medium for the European digital mobile telephone system (GSM). In part, this was because smart cards allowed a high degree of security to be achieved for accessing the mobile telephone network.

At the same time, they provided new possibilities and thus major advantages in marketing mobile telephones, since they made it possible for network operators and service providers to sell telephones and services separately. Without smart cards, mobile telephones would certainly not have spread so quickly across Europe or developed into a worldwide standard.

Other potential applications for processor cards include identification cards, access control systems for restricted areas and computers, secure data storage, electronic signatures, electronic purses, and multifunctional cards incorporating several applications in a single card. Modern smart card operating systems also allow new applications to be loaded into a card after it has been issued to the user, without endangering the security of the various applications. This new flexibility opens up completely new application areas.

For example, personal security modules are indispensable if Internet commerce and payments are to be made trustworthy. Such security modules can securely store personal keys and execute high-performance cryptographic algorithms. This task can be handled elegantly by a processor card with a cryptographic coprocessor.

In summary, we can say that the essential advantages of processor cards are large storage capacity, secure storage of confidential data, and the ability to execute cryptographic algorithms. These advantages make a wide range of new applications possible, in addition to the traditional bank card application. The potential of smart cards is by no means yet exhausted, and furthermore, it is constantly being expanded by progress in semiconductor technology.

### 1.2.3 Contactless cards

The rapid progress of integrated circuit technology has led to a dramatic decrease in the power consumption of smart card microcontrollers. As a result, contactless cards, in which energy and data are transferred without any electrical contact between the card and the terminal, have become mature, inexpensive mass-produced products in the form of memory cards as well as processor cards. Although contactless processor cards are limited to operation at a distance of up to ten centimeters from the terminal due to their relatively high power consumption, contactless memory cards can be used up to a meter away from the terminal. This means that contactless memory cards do not necessarily have to be held in the user's hand in use, but can remain in the user's purse or wallet. Contactless cards are thus particularly suitable for applications in which people or items should be identified quickly. Sample applications include access control, local public transport, ski passes, airline tickets, and luggage identification.

However, there are also applications where operation over a long distance could cause problems and should be prevented. A typical example is an electronic purse. A declaration of intent on the part of the cardholder is normally required to complete a financial transaction. This confirms the amount of the payment and the cardholder's agreement to pay. With a contact card, this declaration takes the form of inserting the card in the terminal and confirming the indicated amount using the keypad. If contactless payments over relatively long distances were possible, a swindler could remove money from the electronic purse without the knowledge of the cardholder. Dual-interface cards offer a possible solution to this problem. These cards combine contact and contactless interfaces in a single card. Such a card can communicate with the terminal via either its contact interface or its contactless interface, according to what is desired.

There is considerable interest in using contactless cards for local public transport. If the functionality of smart cards used in payment systems, which are generally contact cards, is

expanded to enable them to act as electronic tickets with a contactless interface, transport system operators can utilize the infrastructure and cards of the credit card industry.

## 1.3 STANDARDIZATION

The prerequisite for the worldwide use of smart cards in everyday life, such as their present worldwide use in the form of SIM cards, health insurance cards, bank cards and passports, was the generation of national and international standards. Due to the special significance of such standards, in this book we repeatedly refer to currently applicable standards and those that are in preparation.

A smart card is normally part of a complex system. This means that the interfaces between the card and the rest of the system must be precisely specified and coordinated. Of course, this could be done for each system on a case-by-case basis, without regard to other systems. However, this would mean that a different type of smart card would be needed for each system. Users would thus have to carry a separate card for each application. In order to avoid this, an attempt has been made to generate application-independent standards that allow multifunctional cards to be developed. Since the smart card is usually the only component of the system that the user holds in his or her hand, it is enormously important for user awareness and acceptance of the entire system. However, from a technical and organizational perspective the smart card is usually only the tip of the iceberg, since complex systems (which are usually networked) are often hidden behind the card terminal, and it is these systems that make the customer benefits possible in the first place.

Let us take telephone cards as an example. In technical terms, they are fairly simple objects. By themselves, they are almost worthless, except perhaps as collector's items. Their true benefit, which is to allow public telephones to be used without coins, can be realized only after umpteen thousand card phones have been installed throughout a region and connected to a network. The large investments required for this can only be justified if the long-term viability of the system is ensured by appropriate standards and specifications. Standards are also an indispensable prerequisite for multifunctional smart cards that can be used for several different applications, such as phoning, an electronic purse, an electronic ticket, and so on.

**What are standards?**

This question is not as trivial as it may appear at first glance, especially because the terms 'standard' and 'specification' are often used interchangeably. A standard requires the consensus of all interested parties, while a specification has looser requirements with regard to consensus and open consultation. To make things clear, let us consider the ISO/IEC definition of a standard:

> A document that is produced by consensus and adopted by a recognized organization, and which, for general and recurring applications, defines rules, guidelines or features for activities or their results, with the objective of achieving an optimum degree of regulation in a given context.

Here it should be noted that standards are based on the established results of science, technology and experience, and their objective is to promote the optimization of benefits for society. International standards should thus help make life easier and increase the reliability and usefulness of products and services.

In order to avoid confusion, ISO/IEC have also defined the term 'consensus' as general agreement, characterized by the absence of continuing objections to essential elements on the part of any significant portion of the interested parties, and achieved by a procedure that attempts to consider the views of all relevant parties and to address all counter-arguments. Here it should be noted that consensus does not necessarily mean unanimity.

Although unanimity is not required for consensus, the democratic process naturally takes a lot of time in many cases, especially because it is necessary to consider not only the views of the technical specialists, but also the views of all involved and affected parties, since the objective of a standard is the promotion of optimum benefits for the whole of society. Hence, the preparation of an ISO or CEN standard usually takes several years. A frequent consequence of the slowness of this process is that a limited group of interested parties, such as commercial firms, generates its own specification ('industry standard') in order to accelerate the launch of a new system. This is particularly true in the field of information technology, which is characterized by especially fast development and correspondingly short innovation cycles. Although industry standards and specifications have the advantage that they can be developed significantly faster than 'true' standards, they carry the risk of ignoring the interests of the parties that are not involved in their development. For this reason, ISO uses the 'fast track' procedure to allow important, publicly accessible specifications to be quickly published as ISO standards after the fact.

**What does ISO/IEC mean?**

The relevant ISO/IEC standards are especially significant for smart cards because they are based on a broad international consensus and define the fundamental properties of smart cards. What lies behind the abbreviations 'ISO' and 'IEC'? 'ISO' stands for the International Organization for Standardization, while 'IEC' stands for the International Electrotechnical Commission.

The International Organization for Standardization (ISO) is a worldwide association of around 100 national standards organizations, with one per country. ISO was founded in 1947 and is a nonnational organization. Its task is to promote the development of standards throughout the world, with the objective of simplifying the international exchange of goods and services and developing cooperation in the fields of science, technology and economy. The results of the activities of ISO are agreements that are published as ISO standards.

Incidentally, 'ISO' is not an abbreviation (the abbreviation of the official name would of course be 'IOS'). Instead, the name 'ISO' is derived from the Greek word *isos*, which means 'equal' or 'the same'. The prefix 'iso-' is commonly used in the three official languages of ISO (English, French and Russian), as well as in many other languages.

As already noted, the members of ISO are the national standards bodies of the individual countries, and only one such body per country is allowed to be a member. Germany is represented in ISO by the DIN organization. The member organizations have four basic tasks, as follows:

- Informing potentially interested parties in their own countries about relevant activities and opportunities for international standardization,
- Fashioning agreed national opinions and representing these opinions in international negotiations,
- Providing secretarial services for the ISO committees in which the country has a particular interest,

- Paying the country's financial contribution to support the activities of the central ISO organization.

The IEC (International Electrotechnical Commission) is an international standardization organization whose scope of responsibility is electrical technology and electronics. The first card standards, which did not include parts on the subject of electronics, were issued by ISO. After the introduction of smart cards, a difference of focus arose between the ISO and the IEC. In order to avoid duplication of effort, standards are developed in a joint technical committee (JTC 1, Joint Technical Committee for Information Technology) and published as ISO/IEC standards.

**How is an ISO standard generated?**

The need for a standard is reported to a national standards organization by a special interest group, such as an association or a industrial sector committee. The national organization then proposes this to ISO as a new working topic. If the proposal is accepted by the responsible working group, which consists of technical experts from countries that are interested in the topic, the first thing that is done is to define the application area of the future standard.

After agreement has been reached on the technologies and applications to be defined in the standard, the details of the standard are discussed and negotiated between the various countries. This is the second phase in the development of a standard. The objective of this phase is to arrive at a consensus of all participating countries, if possible. The outcome of this phase is a 'draft international standard' (DIS).

The final phase consists of a formal vote on the draft standard. Acceptance of a standard requires the approval of two thirds of the ISO members that actively participated in drafting the standard, as well as three quarters of all members participating in the vote. Once the standard has been accepted, the agreed document is published as an ISO standard.

To prevent standards from becoming outdated as the result of ongoing development, ISO rules state that standards should be reviewed, and if necessary revised, after an interval of at most five years.

**Cooperation with the IEC and CEN**

As already mentioned, ISO is not the only international standardization organization. In order to avoid duplication of effort, ISO cooperates closely with the IEC in certain areas. The areas of responsibility are defined as follows: the IEC is responsible for electrical technology and electronics, while ISO is responsible for all other areas. Combined working groups are formed to deal with topics of common interest, and these groups produce combined ISO/IEC standards. Most standards for smart cards belong to this category.

ISO and the Comité Européen de Normalisation (CEN) (European Standardization Committee) have also agreed on rules for the development of standards that are recognized as both European and international standards. This leads to time and cost savings.

The major industrial countries are represented in all relevant committees, and they generally also maintain 'mirror' committees in the form of national working groups and voting committees. The ISO website [ISO] provides an overview of the structure of ISO and its standardization projects. Smart card standards are developed by JTC 1/SC17 ('Cards and Personal Identification'). This working group also provides an overview of recently published standards and standards in progress.

At CEN, the topic of smart cards is handled by the TC 224 committee ('Personal identification, electronic signature and cards, and their related systems and operations').

The activities of CEN complement those of ISO. As much as possible, ISO standards are taken as the basis for CEN standards. If necessary, they are augmented with specifically European sections. In many cases, the number of options is reduced to simplify their implementation for purely European applications. The CEN working groups also produce standards for specific European applications that would not be able to achieve a consensus with ISO in a given form or at a given time.

An additional European standardization body, the European Telecommunications Standards Institute (ETSI), has made a significant contribution to the widespread international use of smart cards with its standard for SIM cards. ETSI generates standards for information and telecommunication technologies, which include mobile telecommunication and Internet technology.

ETSI is recognized by the European Commission as a European standardization organization. The members of ETSI are not the national standardization committees, but instead nearly 700 member organizations worldwide, which essentially represent the industrial sector, telecommunication companies, user groups, and research organizations. The smart card standards are prepared by the Technical Committee for Smart Card Platform (TC SCP). The TS 51.011 family of standards (formerly GS 51.011) specifies the interface between the smart card (called the subscriber identity module, SIM, in the GSM system) and the mobile telephone. This family of standards is based on the ISO/IEC standards. With the international expansion of GSM systems outside Europe, the ETSI standards have achieved global significance for the smart card industry.

After more than thirty years of standardization effort, the most important basic ISO standards for smart cards are now complete. They form the basis for further, application-oriented standards, which are currently being prepared by ISO and CEN.

These standards are based on prior ISO standards in the 7810, 7811, 7812 and 7813 families, which define the properties of identification cards in the ID-1 format. These standards include embossed cards and cards with magnetic stripes, which we all know in the form of credit cards.

Compatibility with these existing standards was a criterion from the very beginning in the development of standards for smart cards (which are called 'integrated circuit(s) cards', ICC, in the ISO standards), in order to provide a smooth transition from embossed cards and magnetic-stripe cards to smart cards. Such a transition is possible because all functional components, such as embossing, magnetic stripes, contacts and interface components for contactless interfaces, can be integrated into a single card. Of course, a consequence of this is that the integrated circuits, which are sensitive electronic components, are exposed to high stresses during the embossing process and recurrent impact stresses when the embossed characters are printed onto paper. This makes heavy demands on the packaging of the integrated circuits and the manner in which they are embedded in the card.

A summary of the currently available standards, with brief descriptions of their contents, can be found in the Appendix.[1]

In the last few years, an increasing number of specifications have been prepared and published by industrial organizations and other nonpublic groups, with no attempt being made to incorporate them in the standardization activities of ISO. The reason most often given for this approach is that the way ISO operates is too slow to keep pace with the short innovation cycles of the information technology and telecommunication industries. Some examples of consortiums that generate specifications relevant to smart cards are Java Card Forum, Open

[1] See also Section 25.4, 'Directory of Standards and Specifications', on page 999

Mobile Alliance (OMA), Global Platform, and NFC Forum. In many cases, only a few interest groups are involved in drafting these industry standards, so there is a risk that the interests of smaller companies, and especially the interests of the general public, may be ignored in the process. Fortunately, the most important consortiums work closely together with standardization organizations and try to include the most important specifications in the standardization process later on. It is a major challenge to the future of ISO and IEC to devise processes that make it possible to safeguard general interests without hampering the pace of innovation.