The smartcard as a mobile security device

by D. Scheuermann

Modern society would like to replace paper by electronic data carriers and mechanical processes by electronic processes. Smartcards offer one means to this end in the form of a personal mobile security device. Personal data can be stored in a mobile personal environment instead of in a central database, and processor smartcards additionally provide a sort of pocket PC that can perform security functions at a higher level of security than an ordinary PC. Interoperability of different smartcards with different smartcard readers and data terminals is very important; therefore, standards exist for the structure of data objects on the card and for coding the commands sent to the card. Biometric user-authentication is becoming increasingly important for smartcards as an alternative to the previously used PIN or password authentication. Additional convenience for the user can be provided by contactless cards.

1 Introduction

Storing and filling out paper forms is troublesome work. It is not surprising therefore that there is much interest nowadays in replacing paper by devices that can store and process data electronically. One such device is the smartcard, whose portability and size make it particularly suitable for small personal data records. Considerable work related to filling out paper forms can be saved simply by presenting a smartcard; in addition, storing data on a smartcard provides more privacy than storing them in a central database.

PCs are often not secure enough for specific applications. Intelligent processor smartcards, however, provide the possibility to build up security infrastructures and to execute security functions in a personal environment on a mobile device. They represent a sort of mobile pocket PC with high security features that make a good contribution to the desired security for mobility.

This paper gives an overview of general smartcard technologies and some of their applications.

2 Storage cards and processor cards

A smartcard may be a data storage device only or may contain a processor to execute some functions. Some types of processor smartcard also enable the user to implement individual programs.

Storage cards

Storage cards are the simplest form of smartcard. They are only used to store data, which can be read out at any time. They contain no processor to execute functions and no security features to protect the data from being read out.

Storage cards are smaller and easier to handle than paper documents and the data on them can be directly read and processed electronically by a PC.

The only security feature is that once manufactured it is not possible to write on the card, i.e. to change the data on it. This is a disadvantage in comparison with processor cards: once the validity of the data on the card has expired and the data needs to be changed, the card becomes useless and must be thrown away and replaced by a new card, just as paper documents need to be renewed.

Processor cards

Processor cards are intelligent smartcards that not only provide electronic storage of data but can also function as a small mobile PC, powered and handled by an appropriate data terminal, to process the data. They incorporate certain security features to guard against unauthorised access to the data and to certain functions. These features enable a smartcard to be personalised, i.e. bound to a certain person. As does an ordinary PC, a processor smartcard has the following fundamental components:

- a random access memory (RAM)
- a read-only memory part (ROM) containing the operating system
- a non volatile memory (EEPROM—electrically erasable programmable ROM)
- a central processing unit (CPU).

Currently available smartcards have the following amounts of memory and computing power:

- RAM: 2 kbytes

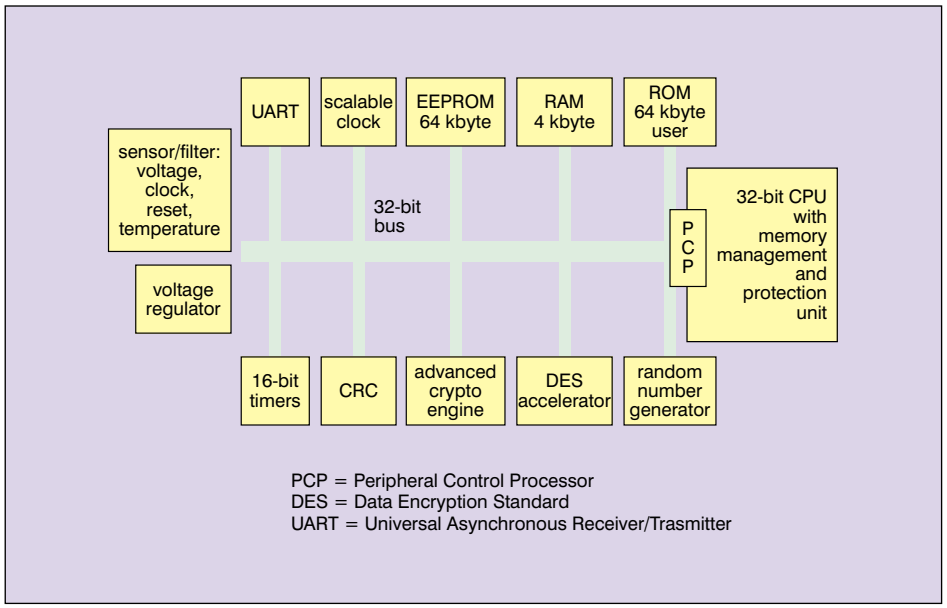

Fig. 1 Block diagram of a smartcard chip with 32 bit CPU

- ROM: 64 kbytes
- EEPROM: 32 kbytes
- CPU: 16 bit.

Smartcards with a 32-bit CPU and 64 kbytes of EEPROM are under development. Fig. 1 shows the block diagram of such a smartcard.

The following general security functions are provided:

- application of cryptographic functions (encipherment, decipherment, electronic signatures)
- user authentication (personal identity number (PIN) or password)
- device authentication with the aid of cryptographic protocols.

The storage capacity and computing power of these mobile devices is still limited, but they provide higher security than ordinary PCs.

Cards with downloadable program code

One particular type of processor smartcard has an important feature for users who want more flexibility to design their own security applications: they can use downloadable program code. If considered as a mobile PC, these cards follow the strategy employed in PCs having a RISC (reduced instruction set computer) architecture: only a few basic functions have to be provided by the hardware or the operating system, the various other possible functions being provided by software installed in the non-volatile memory by the user.

An important variety of these cards is the Java card, which allows Java byte code to be implemented in EEPROM. Standardised smartcard commands (as defined in ISO/IEC 7816, see the next section) are no longer handled directly in ROM but by a Java applet in EEPROM. By installing individual applets on the card, standardised commands may be executed in different ways on the same card, depending on the desired application context.

3 Standardised data objects and commands

ISO/IEC 7816 standards

Important features of smartcards that need to be standardised are the data objects present on the card and the structure of the commands sent to the card. The standardisation of these features, besides the specification of the general physical characteristics of smartcards, is one important task of the ISO/IEC 7816 series of standards. General transmission protocols for exchanging data between the card and the data terminal are specified in part 3 (ISO 7816-3)[1]. Part 4 (ISO 7816-4)[2] covers file structures on the card, the structure of commands and the specification of some basic commands. Part 8 (ISO 7816-8)[3] specifies special commands for cryptographic purposes. And, for the increasingly important use of biometric user verification with smartcards, a new part 11 (ISO 7816-11)[4] is under development that provides a more detailed specification of command sequences and data objects for this special purpose; further details are presented in Section 5. The following subsections focus on two important general features, namely the system of files on the card and the structure of the smartcard commands.

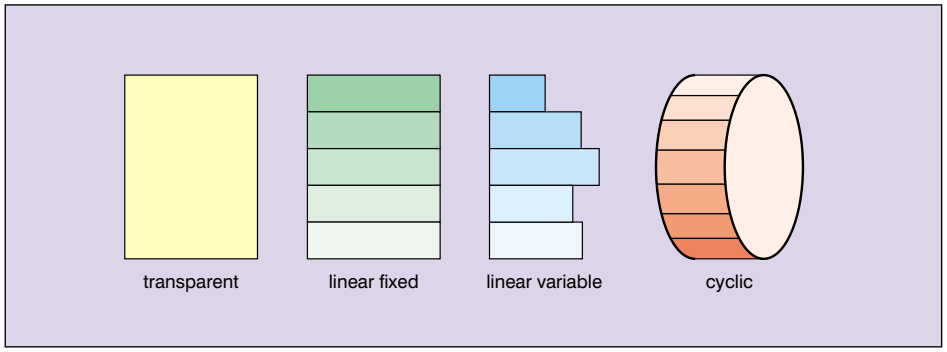

Fig. 2 Data structures in smartcards

File system

A smartcard has a file system in a similar way to a PC. The following categories of files exist: a single master file (MF), dedicated files (DF) and elementary files (EF).

The mandatory master file, which is implicitly selected

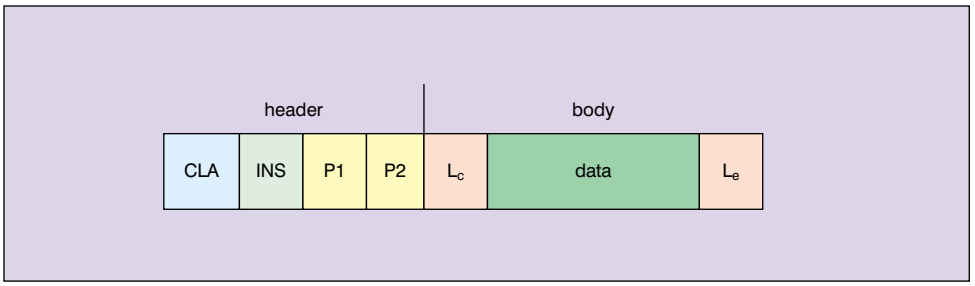

Fig. 3 Structure of smartcard commands

when the card is activated, is the root file on top of all other files; it is comparable to the root file on a PC system. Dedicated files represent directories, and elementary files correspond to individual files containing data.

In contrast to PCs, a smartcard operating system provides different structures for files which are useful for particular applications. Fig. 2 illustrates these structures. *Transparent files* are amorphous files similar to files on ordinary PCs: they have no inner structure, and each byte is individually addressable for reading or writing. For some applications, e.g. storing tables, it is useful to have structured files. For this purpose, *linear fixed* and *linear variable* files exist on smartcards. These files are separated into records; each byte is addressed by a record ID and an offset number giving the exact location inside the record. In the case of linear fixed files, all records must have the same length (which is a specified file parameter), whereas for linear variable files different record sizes are allowed, giving more flexibility. One additional file structure for smartcards, also divided into records, is provided by the *cyclic* structure, which represents a sort of drum storage: if the data to be written exceeds the space remaining up to the end of the file, the first record is overwritten. Cyclic files are useful, for example, for storing a particular number of transactions previously made with the card.

The structure, size and security features are specified during the creation of the file and are unchangeable afterwards. The access rights to the files are specified with the security features. Access for reading from, writing to, or possibly deleting the file may be protected by knowledge-based or biometric user-authentication as well as by cryptographic device authentication; access may even be denied completely. With these unchangeable features, a much higher level of security is provided than on a PC since accidental modification of data or reading out of critical data can be avoided. For example, cryptographic keys, PINs and passwords are stored in files with no read or write access; they can only be accessed by special security commands (see also the next section) using or modifying the data without reading them out of the card.

Smartcard commands

According to ISO 7816-4[2], a command sent to the smartcard consists of a so-called application protocol data unit (APDU). Such an APDU consists of two major parts: a mandatory, 4 byte command header, which must be present for all commands, and a command body, which can be missing for some commands. The individual fields of the APDU are shown in Fig. 3.

A class byte (CLA) at the beginning of the header contains general information about the command, including regulations to interpret the subsequent fields. The instruction byte (INS) specifies the fundamental function of the command. Besides the interindustry commands defined in ISO 7816-4[2] and ISO 7816-8[3], a card manufacturer or programmer may also define their own commands, so-called private use commands; information on which sort of command the instruction code belongs to is provided in the class byte. Two further bytes in the header, P1 and P2, specify further parameters for command execution. For commands that include input data, the command body contains a data field preceded by an L_c byte defining the length of the data. For commands that deliver back output data, an L_e byte indicates the expected length of these data. Compared with functions executed on a PC, the instruction byte represents the function name, whereas P1, P2 and the optional command body represent the input parameter list of the function.

So that the user is always given feedback, for each command the smartcard delivers a response string, whose structure is also standardised. This response contains a mandatory part and an optional body (see Fig. 4). The mandatory status bytes SW1 and SW2 indicate correct or incorrect execution of the command with precise error specification; they are comparable to the predefined return values of functions indicating certain errors. Additional response data, if indicated by the L_e byte of the command, are contained in the optional response body.

Secure messaging

For certain security applications, data transmitted to or obtained from the card are strictly confidential and, additionally, the integrity or authentic origin of the data must be ensured. In ISO 7816-4[2], a solution to this problem is also provided; the general concept is called secure messaging. With the aid of this concept, data may be cryptographically protected: the command data may be enciphered to ensure confidentiality and a cryptographic checksum can be calculated and appended to ensure

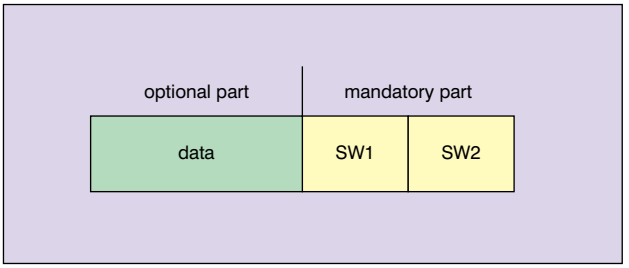

Fig. 4 Structure of responses to smartcard commands

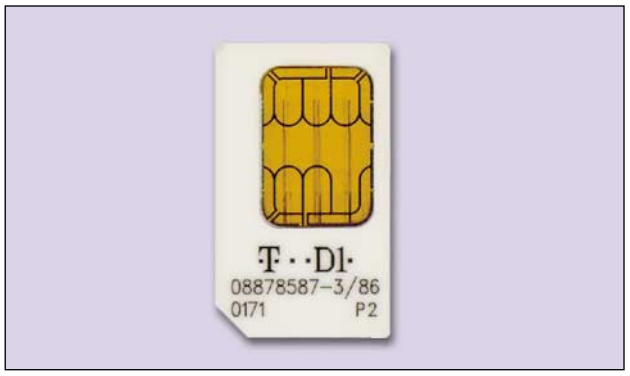

Fig. 5 Example of a German SIM

integrity. The use of secure messaging and its exact mode are indicated within the CLA byte of the command.

4 Sample applications

Existing applications for storage cards

People are already accustomed to some applications where a smartcard is used just to store data. Two common examples are telephone cards and health insurance cards. Telephone cards avoid the inconvenience of having to carry small coins, and insurance cards avoid the need to fill in paper forms. However, there is no specific protection regarding the use to which the data on the card is put, i.e. the data can be read out and used by anyone finding the card. Also, it is known that these cards are not reloadable or rewritable—if a telephone card is empty, it has to be thrown away and a new one bought. Moreover, after the end of the validation period of an insurance card or after any change of the patient data, e.g. name or address, the patient has to apply to his/her insurance company for a new card.

Nevertheless, the data objects on the patient data card and the current process for reading it are already compatible with the new concept of intelligent insurance cards with enlarged functions (see below).

Identification cards for mobile phones

The most popular application for processor cards currently is with mobile phones. The central security processor of a mobile phone is provided by a GSM subscriber identification module (SIM). Unique identification of such a SIM on a worldwide basis is provided by an 8 byte 'international mobile subscriber identity' (IMSI). Fig. 5 shows an example of a German SIM.

In this context, the smartcard can also be used to work together with some protocol specified within the series of specifications for wireless communication network applications, that is the Wireless Application Protocol (WAP). This is done by inserting, at manufacture, the WAP identification module (WIM) application (as defined in Reference 5) onto the same smartcard as the SIM application.

Signature cards

An important security application for smartcards is the creation of electronic signatures (some further specific applications are mentioned in the following subsections). With the signature function implemented, smartcards provide a personal mobile device for performing signatures. If the smartcard meets rigorous security requirements it may be classed as a so-called 'secure signature creation device' (SSCD) as defined in Reference 6. Signature cards must be personalised and contain a certificate of the owner.

Office identity cards

Smart cards may be used in place of paper documents. They may also be used for automatic access control, so avoiding the need to employ people to watch entrances. An electronic office identity card is a typical application.

Access control could be provided by simple data storage cards. However, processor cards are more useful as office identity cards as they may provide different individual access rights or authorisations to perform certain security functions.

The German consortium TeleTrusT has established a specification for a German office identity card[7]. Certain cryptographic security functions, including electronic signatures, are provided as basic services for the office identity card.

Health applications

In the future, smartcards will play an important role for health applications. Basically, two cards will be involved: a patient data (health insurance) card and a health professional card (to be used by a pharmacist or a physician).

A major aspect of using smartcards for health applications is enlargement of the functions of the patient data card: the basic data storage card (see above) is to be replaced by an intelligent processor card with security features to regulate access to the card. Access may be granted, for example, to the patient following knowledge-based or biometric user-authentication or to a physician or pharmacist after cryptographic device authentication with the aid of the health professional's card. Besides providing authentication prior to being granted read or write access to the patient's data card, the health professional card will also be equipped with an electronic signature function, e.g. for signing electronic prescriptions.

5 Smartcards and biometrics

Traditionally, user verification is performed with the aid of PINs or passwords. However, biometric methods, by which a user is recognised from their personal features, are becoming increasingly important. Biometric features have the advantage that they can not be lost, forgotten or unintentionally given to someone else.

Biometric verification and identification methods are also becoming more important in connection with smartcards; they provide a means not only to relate but also to bind mobile security devices to an individual.

With respect to the processing of the biometric data, the smartcard may fulfil one of two general functions: it may simply be a device for storing the data or it may process the data, i.e. perform the biometric verification. In which way the smartcard is used depends strongly on the application scenario: the biometric verification or

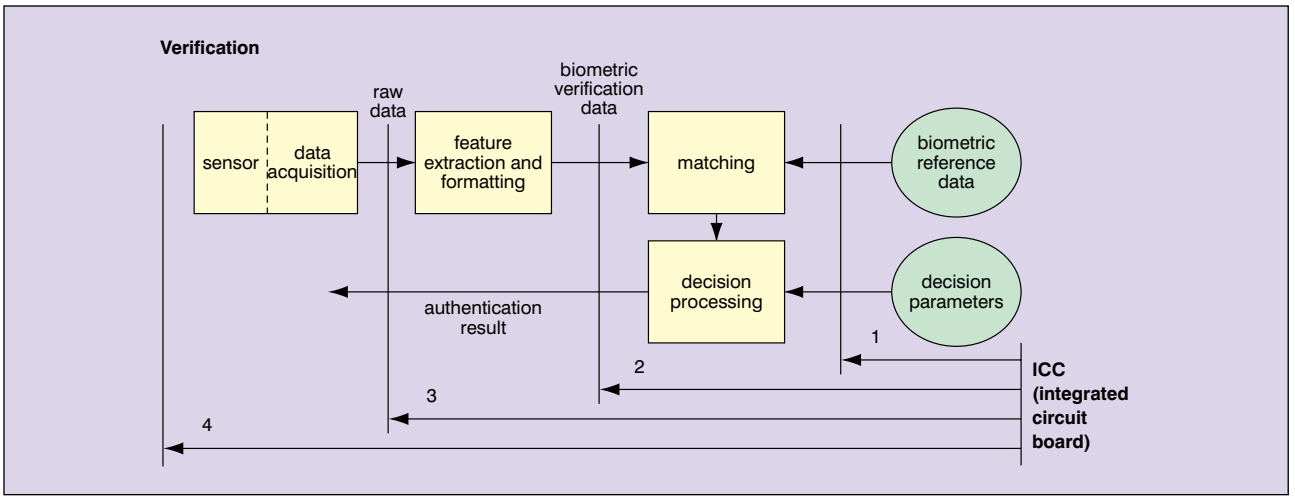

Fig. 6 Possible roles of smartcards in biometric verification systems

identification process has to be performed by the device holding the protected security application or the protected data since this represents the verifying authority.

Smartcards as a data storage device

If the security application to be protected by biometric verification or identification is located outside the smartcard, the card is used as a data storage device only. Typical examples are access control systems or cash dispensers; it is the access control system or the banking system, respectively, that has to check the identity of the user, not the smartcard.

In these scenarios, the smartcard provides a mobile personal storage device avoiding the necessity to store biometric data in a central database. This provides advantages with respect to data privacy. Users will trust biometrics more if they are not afraid that the personal data on them stored in a central database could be misused.

Smartcards as a verification device

If a security application or valuable or critical data are contained in a smartcard, it is important that the smartcard itself should be able to recognise its legal user. For this purpose, the biometric verification process must be incorporated into the smartcard (on-card matching). A typical example is the signature card already described above.

With this functionality, the smartcard becomes a mobile security device that is more strongly bound to its owner than one which uses just PIN or password verification.

Basic smartcard commands for biometric user verification, based on commands previously used for PINs or passwords, were defined in ISO 7816-4[2]. However, due to the importance of this new technology, a new standard that specifically addresses the necessary command sequences and data objects is now under development (ISO 7816-11[4]).

On-card matching provides a broad market for smartcards with downloadable program code. Standardisation activities in biometrics are currently restricted to data objects and general command sequences; there are no standards for biometric algorithms. Therefore, card manufacturers will not provide biometric algorithms directly within the operating system. Instead, individual algorithms will be implemented in smartcards by software manufacturers or application providers.

It should be noted that some biometric data, for example fingerprints, are not secrets, and are publicly available. Even though biometric data will be treated in the same way as PINs or passwords (i.e. stored in a file with no read or write access), the security of a biometric verification system must not depend on keeping the biometric reference data safely inside the card. To avoid replay or data acquisition attacks, e.g. by obtaining a fingerprint from a glass and sending the digitised data to the smartcard, secure messaging can be used, as described earlier.

Implementation of further steps

Besides comparison (matching) of the biometric data, the full biometric verification process includes two further preliminary steps. First of all the data must be captured by a biometric sensor. Then specific data must be extracted from the raw data. It is expected that with continuous further development of smartcard technology both of these processes will be implemented on the card in the future. This will make the mobile security device more secure and independent by avoiding the need to transport biometric data between the card and a data terminal.

The four possible roles of the smartcard, as shown in Fig. 6, are:

- data storage only (1)
- biometric verification (feature matching and decision processing) on the card, the sensor and feature extraction outside it (2)
- feature extraction and feature matching with decision processing on the card, the sensor outside it (3)
- complete system on the card (4).

6 Contactless cards

The ISO/IEC 7816 standard series, which also encompasses biometric verification on smartcards, covers contact cards only. For some applications, where certain actions are to be performed very quickly while passing by, user convenience can be increased by using contactless cards.

Standards for contactless cards

The maximum distance between a card and a data terminal varies depending on the application. International standards already exist for specifying the following three basic types of contactless cards:

- close-coupled cards for distances up to 1 cm (defined in ISO/IEC 10536)
- proximity cards for distances up to 10 cm (defined in ISO/IEC 14443)
- vicinity cards for distances up to 1 m (defined in ISO/IEC 15693).

The market for close-coupled cards is small as some effort is required to position the card correctly and hence they do not offer much improvement in convenience. Proximity and vicinity cards on the other hand are not suitable for high-security applications where critical data is transmitted. A typical application for close-coupled cards is in access control systems; contactless cards with greater card-to-sensor distances may be used for some payment processes, e.g. fare payment when boarding a bus or payment for use of toll roads. Field trials of public-transport fare payment systems have already been conducted in Germany.

Dual-interface cards

For some critical applications, it is still desirable to use contact cards. Therefore, it is planned to design dual-interface multi-application smartcards that provide interfaces for both contact and contactless communication. As a first step, the card will contain two different chips. The next step will be a single dual-interface chip able to handle both modes of communication. The office identity card described earlier represents one possible example: the embedded signature function designated by the specification[7] would be handled over a contact interface whereas the access control function would be better suited for a contactless interface.

7 Summary

The smartcard is a personal mobile security device that is well suited to improving the security of mobile applications. Besides avoiding the need to handle paper documents, intelligent processor cards also provide a security infrastructure at a higher level than a PC does. The option of downloading programs to the card provides even greater flexibility in designing multi-application smartcards with individual security applications. The most common smartcard application at present is the GSM card in mobile phones.

As outlined in Section 3, standards already exist that provide for interoperability between different smartcard operating systems and data terminals as well as standardised security levels. The security of smartcards is further enhanced by the use of biometric user verification, which can strongly bind a mobile security device to an individual.

The computing power and memory capacity of smartcards is still limited, but being increased continuously. Future developments will concentrate on placing complete systems, e.g. a biometric verification system with all its processing steps, on the card to avoid the exchange of critical data with the data terminal.

The convenience of using smartcards will increase further with the development of contactless cards. The future belongs to dual-interface cards that can handle different applications, some better suited to contact cards, others better suited to contactless cards.

Smartcards are being developed into a universal mobile security device for an ever increasing number of security applications.

Dirk Scheuermann studied mathematics at the Technical University of Darmstadt and received his diploma in 1994. From 1992 to 1994, he was employed at the GMD Institute for Telecooperation Technology (TKT) as a working student; during this time he developed smartcard applications and worked on a diploma thesis on integer factoring algorithms. After completing the diploma, he worked at the TKT Institute as a postgraduate student; his research covered hash functions based on modular arithmetic, smartcard interface functions and biometric products and algorithms. Since receiving a doctorate in 1998, he has been a researcher at FhG-SIT (previously GMD-TKT, resp. GMD-SIT). His principal areas of work are the investigation and development of biometric algorithms and he has contributed to standardisation efforts on the use of smartcards with biometrics.

Address: Fraunhofer Institute for Secure Telecooperation (SIT), Rheinstrasse 75, D-64295 Darmstadt, Germany
E-mail: Dirk.Scheuermann@sit.fraunhofer.de

References

1 ISO/IEC 7816-3: 1997: 'Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 3: Electronic signals and transmission protocols'
2 ISO/IEC 7816-4: 1995: 'Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 4: Interindustry commands for interchange'. Revised Version: ISO/IEC CD 7816-4: 2002
3 ISO/IEC 7816-8: 1999: 'Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 8: Security related interindustry commands'. Revised Version: ISO/IEC CD 7816-8: 2002: 'Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 8: Interindustry commands for a crypto-graphic toolbox
4 ISO/IEC CD2 7816-11: 2001: 'Information technology—Identification cards—Integrated circuit(s) cards with contacts—Part 11: Personal verification through biometric methods'
5 Wireless Identity Module Specification, WAP-260-WIM-20010712-a, July 2001
6 EU Directive 1999/93/EC of the European Parliament and the Council of 13th December 1999 on a Community framework for electronic signatures
7 German Office Identity Card, Version 1.0, 6.7.2000 (TeleTrusT Deutschland e.V., Erfurt, Germany)

Received 28th June 2002