16
Appendix

16.1 GLOSSARY

The following pages contain a list of terms typically used in the smart card world. Precise, comprehensive definitions of terms can also be found in the ISO/IEC 7816 family of standards. The equivalent standard in the area of electronic purses with regard to terminology is EN 1546, which comprehensively and concisely defines and explains all of the associated technical terms.

The keywords in this glossary are listed as abbreviations or in full according to customary usage. An arrow symbol (→) in front of a term refers to another entry in the glossary in which the term (set in *italics*) is explained.

Larger collections of general terms used in informatics can be found in the DIN 44 300 standard and numerous lexicons devoted to EDP terminology, such as [Pfaffenberger 97, Dictionary of Computing 91].

μP card

An alternate designation for → *microprocessor card*.

0-PIN

A common, known PIN used for all newly issued → *smart cards*, which does not allow access to the actual user functions. It is thus a type of → *trivial PIN*. The first time the card is used, the 0-PIN must be changed to a user-selected PIN using the usual mechanisms (usually CHANGE CHV), with the value of the 0-PIN not being an allowed value for the new PIN. The purpose of a 0-PIN is to allow the user to unambiguously determine whether the card is still in its original issued state when he or she receives it or has been illicitly used while underway. The term '0-PIN' comes from the fact that the value "0000" is often used for this type of PIN.

Smart Card Handbook, Third Edition. W. Rankl and W. Effing
 ISBN: 0-470-85668-8

1-μm/0.8-μm/... technology

In the fabrication of semiconductor chips, the performance of the technology used is traditionally expressed in terms of the dimension of the smallest possible transistor structure on the semiconductor material. This is usually the width of the gate oxide strip of a transistor. Currently, the smallest possible structure widths are approximately 0.25 μm and 0.13 μm. Naturally, it is always possible to make structures on the chip that are larger than the minimum dimension.

1K/2K/4K/.../*n*K-chip

The designation '*n*K-chip' (where *n* is a positive integer) is frequently used as a simplified type designation for a → *microcontroller* with a certain size of → *EEPROM* in kilobytes. A 32K-chip is thus a smart card microcontroller with 32 kB of EEPROM. Specifying the size of the EEPROM is sufficient for rough comparisons of commonly used smart card microcontrollers.

1G (first generation)

Refers to the first generation of mobile telecommunication networks, which have a cellular architecture and use analog technology. Typical examples of 1G systems are AMPS and the German C-Netz.

2G (second generation)

Refers to the second generation of mobile telecommunication networks, which have a cellular architecture and use digital technology. Typical examples of 2G systems are → *GSM* and → *CDMA*.

3DES

→*triple DES*

3G (third generation)

Refers to the third generation of mobile telecommunication networks, which have a cellular architecture and use digital technology. A typical example of a 3G system is → *UMTS*, which in turn is a member of the → *IMT-2000* family.

3GPP (Third Generation Partnership Project) [3GPP]

The task of the Third Generation Partnership Project, which was founded by the five standards institutes ANSI T1 (USA), ARIB (Japan), ETSI (Europe), TTA (Korea) and TTC (Japan), is

to generate internationally usable technical specifications for third-generation (→ 3*G*) mobile telecommunications systems based on an enhanced GSM core system (→ *GSM*). The participating standards bodies will then translate these specifications into corresponding standards. 3GPP was founded in Copenhagen by the leading international standards organizations in the field of telecommunications. The Third Generation Partnership Project 2 (3GPPP2) has similar responsibilities, although the latter project focuses on further development of non-GSM systems (such as CDMA systems) in the direction of the third generation.

3GPP2

→ 3*GPP*

4G (fourth generation)

Refers to the fourth generation of mobile telecommunication networks, which is currently only in the conceptual stage.

8-bit/16-bit/32-bit CPU

An important characteristic with regard to the processing power of a → *microprocessor* is the width of the register for data to be processed in the processing unit. It is expressed in terms of the number of bits.

A2C (administration to customer)

Public administration and end users.

A3 (algorithm 3)

Designation for a cryptographic algorithm used in → *GSM* for the authentication of the SIM by the background system using a challenge–response procedure. A3 is chosen by the network operator and is thus not the same for the entire GSM system.

A5 (algorithm 5)

Designation for a cryptographic algorithm used in → *GSM* for encrypting data on the air interface between the mobile station and the base station or background system. A5 is the same for the entire GSM system.

A8 (algorithm 8)

Designation for a cryptographic algorithm used in → *GSM* for generating session keys (Kc) used for encrypting speech data on the air interface. A8 is chosen by the network operator and is thus not the same for the entire GSM system.

Access conditions (AC)

In connection with the file system of a smart card, a finite number of conditions that must be satisfied prior to accessing the associated file using one of the various types of access supported by the operating system (e.g., read, write, delete). Access conditions are usually specified independently for each type of access.

Acquirer

An entity that establishes and manages data links and data exchanges between the operator of a payment system and individual service providers. An acquirer may consolidate individual transactions that it receives, so that the system operator receives only collective certificates.

Activation sequence

Specifies the order of events for activation of the electrical signals for a → *smart card microcontroller* when powering up a → *smart card*. It does not say anything about the sequence of events for mechanical contacting. The objective of the activation sequence is to protect the smart card microcontroller, which is sensitive to charges and voltages on its contacts. (→ *deactivation sequence*)

Administrative data

Data that are used only for managing → *user data* and no other particular significance with respect to an → *application*.

AES (Advanced Encryption Standard)

A symmetric → *cryptographic algorithm*, originally developed by Joan Daemen and Vincent Rijmen and published as the Rijndael algorithm. Following a public competition and evaluation process, the → *NIST* selected this algorithm as the successor to the DES in 2000 and published it as a US standard (FIPS 197) in 2001.[1]

AFNOR (*Association Française de Normalisation*)

A French standards organization based in Paris.

AID (application identifier)

An AID identifies an → *application* in a → *smart card*, as specified in ISO/IEC 7816-5. Part of the AID may be registered nationally or internationally, in which case it is reserved for the

[1] See also Section 4.7.1, 'Symmetric cryptographic algorithms'

registered application and is unique in the entire world. An AID consists of two data elements: a registered identifier (RID) and a proprietary identifier (PIX).[2]

AMPS (Advanced Mobile Phone System)

A cellular mobile telephone standard, predominantly used in the USA, Latin America, Australia and parts of Asia. It employs analog technology and operates in the 800-MHz band. AMPS mobile telephones do not have → *smart cards* and are often successfully attacked, in part for this reason. The upgraded version of AMPS is D-AMPS, a digital system that also operates in the 800-MHz band.

Analog

Refers to systems in which signals may assume an unlimited number of values.

Analysis

In the sense of software development, the process of determining the customer requirements for an informatics system and completely and unambiguously describing these requirements. In simplified terms, the result of analysis is a description of 'what' is to be produced. The subsequent step in a sequential software development project is → *design*.

Anonymization

Modifying person-specific data in such a manner that it is no longer possible to associate the modified data with the original person. (→ *pseudo-anonymization*)

ANSI (American National Standards Institute) [ANSI]

An American standards organization based in New York.

Anticollision method

A method that permits access to multiple contactless cards without interference.

APDU (application protocol data unit)

A software data container used to package data for an → *application* for exchange between a → *smart card* and a → *terminal*. The APDU is converted into a transmission protocol data unit (TPDU) by the transmission protocol and then sent by the smart card or terminal

[2] See also Section 5.6.1, 'File types'

via the serial interface. APDUs can be classified into → *command APDUs* and → *response APDUs*.[3]

API (application programming interface)

A software interface, specified in detail, that provides access to specific functions of a program.

Application

All of the data, files, → *commands*, processes, states, mechanisms, algorithms and programs in a → *smart card* that allow it to be used in a particular system. An application and its associated data are usually located in a dedicated DF directly below the MF. Such an application is often called an 'oncard application'. The opposite to this is an 'offcard application', which encompasses all of the programs and data not present in the smart card that are necessary for using the oncard application in the smart card.

Application operator

An entity that operates an → *application* using → *smart cards*. The application operator is usually the same as the application provider.

Applet

A program written in the Java programming language and executed by the virtual machine of a computer. For reasons of security, the functionality of an applet is restricted to a previously defined program environment. In the realm of → *smart cards*, applets are sometimes called 'cardlets'. An applet usually corresponds to a smart card → *application*.

Applet developer

A person or organization that develops an → *applet*.

ASK(amplitude-shift keying)

A modulation method in which the amplitude of the carrier wave is switched between two states.

ASN.1 (Abstract Syntax Notation 1)

A description language (syntax and grammar) for data that allows data and data types to be unambiguously defined and represented independent of the type of computer system used. The

[3] See also Section 6.5, 'Message Structure: APDUs'

corresponding data can then be coded in concrete terms using the → *BER (Basic Encoding Rules*) and the → *DER(Distinguished Encoding Rules)*. ASN.1 is defined by ISO/IEC 8824 and ISO/IEC 8825.[4]

Assembler

A program that translates assembly-language programs into machine language, which can be executed by a processor. After the assembly process, it is usually necessary to link the resulting code using a linker program. 'Assembler' is also often used as a short form for 'assembly-language program code'.

Asymmetric cryptographic algorithm

→*cryptographic algorithm*

Asynchronous data transmission

Data transmission in which the data are transmitted independent of any prescribed timing reference. (→ *synchronous data transmission*)

Atomic operation

One or more operations in a program that are executed either entirely or not at all. In → *smart cards*, atomic operations are frequently used in connection with EEPROM write routines, in order to ensure that the data content is consistent at all times.[5]

ATR (answer to reset)

A sequence of bytes sent by a → *smart card* in response to a (hardware) reset. The ATR includes various parameters relating to the transmission protocol for the smart card.[6]

Attribute

In the sense of → *object-oriented programming*, a data container holding an → *object* (in the procedural sense, the variables). Attribute values can be read or modified using → *methods.*

[4] See also Section 4.1, 'Structuring Data'
[5] See also Section 5.10, 'Atomic Operations'
[6] See also Section 6.2, 'Answer to Reset (ATR)'

Authentication

The process of verifying the genuineness of an entity (such as a smart card) using a cryptographic procedure. Put simply, authentication amounts to using a prescribed procedure to determine whether someone is actually the person he or she claims to be.

Authenticity

A property possessed by an entity or message that is genuine and unaltered.

Authorization

Testing whether a particular action is allowed to be performed; equivalent to granting someone the authority to do something. For example, when a credit card transaction is authorized by the credit card issuer, the card data are checked to see if the data are correct, the amount of the purchase is less than the permitted limit and so on. The payment is then allowed if all checks are satisfactory. An authorization can be achieved by means of authentication of the party in question (such as a smart card). Put simply, authorization amounts to giving someone permission to perform a particular action.

Auto-eject reader

A terminal that can automatically eject an inserted card in response to an electrical or mechanical signal.

B2A (business to administration)

Designates the handling of → *e-commerce* business between enterprises and public administrations.

B2B (business to business)

Designates the handling of → *e-commerce* business between enterprises.

B2C (business to customer)

Designates the handling of → *e-commerce* business between enterprises and end users.

Background system

Any type of computer system above the level of the terminal that processes and manages data.

Bad case

The case in which a logical decision leads to an unfavorable or undesired result.

Bad-day scenario

Another expression for → *bad case*.

Baud

Designates the number of state changes per second during a data transmission. Depending on the transmission method used, one or more data bits can be transmitted for each change of state. For this reason, the baud rate is equivalent to the transmission rate in bits per second only in the special case that only one bit is transmitted for each change in state.

Bearer

Designates the bearer service used to transport data to a terminal device. For example, SMS is a possible bearer for WAP

Bellcore attack

→*differential fault analysis*

BER (Basic Encoding Rules)

The BER, which are defined in → *ASN.1*, allow data to be coded in the form of data objects. A BER-coded data object has a tag, a length and a value (the actual data component), and optionally an end marker, and is thus also referred to as TLV-coded data. The BER format also permits chained data objects. The Distinguished Encoding Rules (DER), which are a subset of the BER, indicate among other things how the length parameter of the data object is to be coded (1, 2 or 3 bytes).[7]

Big-endian

→*endianness*

Binary-compatible program code

A program that can be executed directly by a → *microprocessor* without using auxiliary programs or the like (→ *program code*).

[7] See also Section 4.1, 'Structuring Data'

Blacklist

A list in a database identifying all cards or devices that are no longer allowed to be used in a particular → *application.* (→ *hotlist, graylist, whitelist*)

Blackbox test

A test based on the assumption that the party performing the test has no knowledge of the internal processes, functions and mechanisms of the software being tested.

Bluetooth [Bluetooth]

A wireless network technology intended to be used for short-range communications (<100 m) in the 2.4 GHz band, with a maximum gross data transmission rate of around 1 Mbit/s. Ericsson, as the initiator of this technology, chose the name in memory of the Danish king Harald II, who lived approximately 1000 years ago and was nicknamed 'Bluetooth'. His major achievement was merging many separate regions into a unified kingdom.

Bond-out chip

A microcontroller mounted in a multi-pin ceramic package providing free access to all of the memory busses internal to the chip, thus allowing the commonly used mask-programmed →*ROM* to be replaced by memory external to the chip. A bond-out chip is used to allow software to be tested in the target hardware without using a → *ROM mask*.

Boot loader

A small, simple program whose only purpose is to load other, larger programs into memory, for example via a serial interface, and run them from memory (→ *loader*). A boot loader is typically used to load the actual program code into a new chip or a new piece of electronic equipment. In many cases, the boot loading process can be performed only once.

BPSK (binary phase shift keying)

180-degree phase shift keying, yielding two phase states.

Browser

A program for viewing hypertext documents, navigating among such documents and running → *program code* embedded in hypertext documents. Browsers with simple structures that require little memory and processing capacity are often called microbrowsers. Some microbrowsers run as → *applications* within a → *smart card operating system* (such as the SIM Alliance browser, also known as the S@T browser), while others are integrated into the

software of the mobile telephone (e.g., WAP browsers). The functionality of browsers can be extended using downloadable software components called browser plug-ins.

Brute-force attack

An attack on a cryptographic system based on computing all possible values of a key.

BSI (*Bundesamt for Sicherheit in der Informationstechnik*) [BSI]

The German *Bundesamt for Sicherheit in der Informationstechnik* (BSI) was founded in 1991 as the successor to the *Zentralstelle für das Chiffrierwissen*. The functions of the BSI include investigating the security risks of IT applications, testing and evaluating the security of IT systems, formally approving IT systems for government agencies and assisting criminal investigation agencies and agencies charged with the protection of the German constitution. It also advises manufacturers, operators and users with regard to IT security, and in this regard it often specifies the general conditions for using cryptography in Germany.

Buffering

A typical type of attack on magnetic-stripe cards involving first reading and storing (buffering) the data on the magnetic stripe. After the data have been modified using a terminal (e.g., changing the state of the retry counter), the original data are written back to the magnetic stripe.

Bug fix

In software development, supplementary →*program code* used to remedy a known error (bug). In contrast to a →*work-around*, a bug fix eliminates the actual error.

Burst

→*signal burst*

Bytecode

This term has several different meanings and can only be correctly interpreted in the context in which it is used. One widely used meaning is related to the Java system, in which bytecode is the name given to the intermediate code produced (compiled) from the source code by a Java compiler. This bytecode is standardized by the Sun Corporation and is interpreted by the Java virtual machine. The term 'bytecode' is also used in the context of microbrowsers (→*browser*), where it is understood to mean the translated code produced from a hypertext document by the bytecode converter. The result of this translation is the bytecode, which is then interpreted by the microbrowser.

CAD (card acceptance device)

In the realm of electronic payment systems, the designation CAD is frequently used to refer to a smart card terminal, in place of the ISO abbreviation → *IFD* (interface device).

CAMEL (Customized Applications for Mobile Enhanced Logic)

Supplementary possible feature of →*GSM* for supporting the functionality of intelligent networks (IN). With CAMEL, for example, it is possible to modify a dialing number during call setup on the network. This allows applications such as international →*roaming* using prepaid cards and internationally available standard service numbers to be implemented in a simple manner.

CAP file (card application file)

A data format used to exchange data between the Java Offcard Virtual Machine and the Java Oncard Virtual Machine.

Card

General term used to refer to a thin rectangular piece of material with rounded corners whose physical dimensions comply with an international standard. A card can have various card components, including a semiconductor chip (→*chip card*, →*smart card*).

Card accepter

An entity with which cards can be used for a particular type of transaction (such as payment). A typical example is a merchant who accepts credit cards for making payments.

Card body

A plastic card forming an intermediate product in the production of smart cards. It is further processed in subsequent production steps and receives additional functional components, such as the embedded chip.

Card component

A supplementary functional unit of a →*card*, such as a →*signature panel*, →*embossing*, a →*magnetic stripe*, a chip (→*memory card*, →*microprocessor card*) or a keypad (→*system on card*).

Card issuer

An entity responsible for issuing cards. In the case of mono-application cards, the card issuer is usually also the application provider, but this is not necessarily the case.

Card manufacturer

An entity that produces card bodies in which it embeds modules.

Card Modeling Language (CML)

An abstract, operating-system independent description language for defining smart card →*applications*.

Card owner

A natural or legal person having legal control over a card who can do whatever he wishes with the card. In the case of a credit or debit card, the bank issuing the card is often the card owner, and the customer who uses the card is only the →*cardholder*.

Card reader

A device having a relatively simple electrical and mechanical construction used to accept → *smart cards* and make electrical contact with them. Unlike a terminal, a card reader does not have a display or a keypad. Despite the name, a card reader can usually also be used to write data to a card.

Card user

A person using a card, who is usually but not necessarily the → *cardholder*.

Cardholder

A person actually having a card in his possession and having the legal right to use the card. The cardholder need not necessarily be the same as the →*card owner*.

Cardholder verification method (CVM)

A method for the →*identification* of persons. This usually consists of PIN testing, but biometric user identification may be used in more sophisticated systems.

Cardlet

→*applet*

Cavity

The recess in the card body for the module to be implanted, usually produced by milling.

CCITT (*Comité Consultatif International Télégraphique et Téléphonique*)

Originally, an international committee for telephone and telegraph services, based in Geneva. With the assumption of additional responsibilities, it is now known as the → *ITU*.

CCS (cryptographic checksum)

A cryptographically generated checksum for data, which is used to allow manipulation of the data during storage to be recognized. A CCS used to protect data during transmission is called a message authentication code (→ *MAC*).

CDMA (code division multiple access)

A multiple-access method for the concurrent transmission of data from multiple transmitters to a single receiver within a frequency band. For this purpose, the narrow-band radio signal is mapped onto a wideband radio signal, or 'spread', using a transmitter-specific mapping rule. If this mapping rule is known, the receiver can recover the original narrowband signal from the received wideband signal. CDMA is used in UMTS for a the air interface between the mobile telephone and the base station.[8] With wideband code division multiple access (WCDMA), two separate frequency bands are used for → *uplink* and → *downlink*, for which reason this method is often referred to as frequency division / code division multiple access (FD/CDMA). With time division / frequency division multiple access (TC/CDMA), the uplink and downlink are separated using different time slots.

CDMA 2000 (Code Division Multiple Access 2000)

Third-generation (→ 3*G*) mobile telecommunication system using the 2000-MHz frequency band and having features similar to those of → *UMTS*. The smart card intended to be used in CMDA, which is called the → *R-UIM*, is optional.

Cell

In mobile telecommunications systems, the smallest subdivision of the geographic structure of the network.

[8] See also Section 13.1.1, 'Multiple-access methods'

Cellular technology

Refers to an analog or digital mobile telecommunication system organized in the form of cells. The transmitter and receiver stations of the network, which are commonly called base stations, are usually located at the approximate centers of the cells.[9]

CEN (*Comité Européen de Normalisation*)

A European standards organization based in Brussels. It is composed of all national European standards organizations and is the official institution of the European Union for generating European standards.

CEPS (Common European Electronic Purse Specifications) [CEPSCO]

A specification for → *electronic purses*, with emphasis on international interoperability (→ *interoperable*), including all components necessary for operating an electronic purse system. The first version of CEPS was published in 1999 by CEPSCO. It is based on many of the principles of EN 1546, the European standard for electronic purses.

CEPT (Conférence Européenne des Postes et Télécommunications)

A European standards organization for national telecommunications companies.

Certificate

A public key that has been signed by a trustworthy body and provided with associated administrative data, in order to allow it to be recognized as authentic by third parties (→*PKI*). The most widely used and best-known specification for the structure and coding of certificates is the X.509 standard.

Certification authority (CA)

A certification body in a public-key infrastructure (→ *PKI*) that certifies public keys for →*digital signatures*, which means that it guarantees their authenticity by signing the user's public key using its own private key. If necessary, the certification authority makes the signed public keys available in a directory (→*directory service*) in the form of →*certificates*. A CA can itself generate the necessary key pairs (private and public). For organizational reasons, certification authorities often have a hierarchical structure, with the highest-level certification authority being called the 'top-level CA' or 'root CA'.

[9] See also Section 13.1.2, 'Cellular technology'

Certificate revocation list (CRL)

A list, held by a → *directory service*, that identifies all certificates within a → *PKI* that are blocked and no longer accepted.

Challenge–response procedure

A commonly used authentication procedure in the smart card realm that is based on a secret key for a cryptographic algorithm, with the key being a shared secret of the communicating parties. One of the communicating parties sends the other party a random number (the challenge). The latter encrypts it using a cryptographic algorithm and sends the result (the response) back to the challenger. The challenger then applies the reverse function of the cryptographic algorithm to the encrypted version of the random number it has received and compares the result to the originally sent random number. If they match, the challenger knows that the other party also knows the secret key, and from this it concludes that the other party is authentic.[10]

Chinese remainder theorem

A technique used to accelerate the RSA algorithm. Since it requires knowing both of the prime numbers (p and q), it is only used for decryption or signing.

Chip card

A general term for a card, usually plastic, containing one or more semiconductor chips. A chip card can be either a → *memory card* or a → *microprocessor card*. In English-speaking countries, the term → *smart card* is generally used instead.

Chip module

A carrier and support for a die, with a set of contact elements arranged on its surface. The short form 'module' is frequently used to refer to the chip module.

Chip-on-tape (COT)

A packaging arrangement in which chip modules are placed in adjacent pairs on a thin, flexible tape that is typically 35 mm wide.

Chip size

The surface area of a chip, usually measured in square millimeters. The chip price is to a large degree directly proportional to the chip size. The maximum chip size for smart card microcontrollers is approximately 25 mm^2, due to the types of modules currently used.

[10] See also Section 4.11.2, 'Symmetric mutual authentication'

CHV

→*PIN*

CICC (contactless integrated chip card)

The official ISO name for a card for which data and power are transferred using electromagnetic fields without contact with the card. The chip may be a memory chip or a microcontroller chip.

Circuit-switched

Circuit-switched data transmission employs a direct connection (i.e., a physical line) between the two parties. In general, the charges for a circuit-switched connection are based on the duration of the connection, rather than the amount of data exchanged (→*packet-switched*). Some typical examples of circuit-switched data transmission are analog and ISDN telephone connections using the fixed telephone network.

Class

In the context of →*object-oriented programming*, a sort of abstract set of instructions for constructing an object, or in other words, for constructing the →*attributes* and →*methods* of an object and its relationships to other objects.

Class file

A class file stores a compiled Java program (one that has been translated into bytecode), along with supplementary information. After being loaded, the class file is executed by the Java virtual machine.

Cleanroom VM

→*Java Card virtual machine*

Clearing

In an electronic payment system, the process of settling accounts between a party that accepts electronic payments (usually a merchant) and the associated bank.

Clearing system

A computer-based background system that performs centralized account settlements in an electronic payment application.

CLIP

Europay brand name for several technologically different electronic purse systems using smart cards.

Clock-rate conversion factor

The clock-rate conversion factor (CRCF) defines the length of one bit (the bit interval) for data transmission, in terms of the number of clock cycles per bit interval. The short form 'divider' is commonly used as an equivalent term.

Clone

→*cloning*

Cloning

Attacking a smart card system by making a complete copy of the ROM and EEPROM of a microcontroller.

Closed application

A smart card → *application* that is only available to the application operator and cannot be used for general purposes.

Closed purse

An instance of a closed → *application* for an electronic purse. A closed purse can be used only within the limits defined by the application operator, and not for general payment transactions.

CMM (Capability Maturity Model)

An internationally used model for ascertaining the degree of maturity of software development. The degree of maturity is determined using a standardized list of questions and has five levels. The first maturity, Level 1 designates a more or less chaotic development process, while the highest possible maturity level, Level 5, designates a orderly and continually self-improving development process.[11]

[11] See also Section 15.7, 'Life Cycle Models'

CODEC (compressor/decompressor or coder/decoder)

A hardware chip or algorithm intended to be used for the compression and decompression or encryption and decryption of data.

Cold reset

→*reset*

Collision

A collision occurs when two or more contactless cards located within the active range of a terminal concurrently transmit data to the terminal with the result that the received data cannot be decoded or unambiguously recognized.

Combicard

A registered trademark of ADE, which designates a → *dual-interface card.*

Command

In the realm of → *smart card operating systems*, an instruction to the smart card to perform a specific action. The result of a command is a response returned by the smart card, which at minimum contains status information and optionally may contain data related to the executed command. Commands are transferred to the smart card using → *command APDUs*, while responses are transferred using → *response APDUs*.

Command APDU

A → *command* sent from a terminal to a smart card, consisting of a command header and an optional command body. The command header in turn consists of a class byte, an instruction byte and two parameter bytes P1 and P2 (→ *APDU*).[12]

Common Criteria (CC) [CC]

A criteria catalog for the development and → *evaluation* of information technology systems, which is intended to replace national and international criteria catalogs such as → *TCSEC* and → *ITSEC*. The Common Criteria were first published in 1996 by the → *NIST* as Version 1.0, and since then they have been internationally standardized as ISO 15408. The currently valid revision is Version 2.0 of 1998.

[12] The command APDU is described in detail in Section 6.5.1, 'Structure of the command APDU'

Compiler

A program that translates a program written in a language such as Basic or C into a machine language that can be directly executed by a processor. After a program has been compiled, it is normally necessary to link the code using a linker program.

Completion

The process of completing the operating system by loading the EEPROM portion. This allows the operating system to be modified and updated after the chips have been manufactured without requiring a new ROM mask to be generated. Identical data are written to each smart card during completion, so in principle it is a sort of initialization.

Contacts

The six or eight contact elements located on the front side of a → *smart card* form the electrical interface between the terminal and the microcontroller in the smart card. All electrical signal pass via these contacts.

Contactless card

Abbreviated designation for a type of → *smart card* for which energy and data are transferred using electromagnetic fields without any contact with the card (→ *CICC*).

Core foil

An alternate name for → *internal foil*.

Core voltage

The voltage used by a microprocessor or microcontroller directly within the chip. If the core voltage is lower than the external voltage applied to the chip, the external voltage must be suitably reduced by a voltage converter integrated into the chip. Low core voltages are necessary to compensate for reduced breakdown voltages resulting from increasingly smaller structure widths and to reduce the charge and discharge currents resulting from internal capacitances. A microcontroller built using 0.13-µm-technology, for instance, typically has a core voltage of 1.8 V.

COS (card operating system)

Common designation for a → *smart card operating system*. It often forms part of the product name of the operating system (e.g., STARCOS).

CP8

Brand name of a → *multiapplication smart card* operating system from Bull [Bull], available in several versions.

CPU (central processing unit)

→ *microprocessor*

CRC (cyclic redundancy check)

A simple, widely used type of error detection code (→ *EDC*) for protecting data. A CRC must be specified using an initial value and a divider polynomial before it can be used.

Credit card

A card, with or without a chip, that indicates that the cardholder has been extended credit within certain limits, and with which payment takes place some time after the goods or services have been received. This type of payment is often called 'buy now, pay later'. The widely used embossed credit cards are typical examples of this type of card.

Cryptoalgorithm

→ *cryptographic algorithm*

Cryptocard

→ *microprocessor card*

Cryptographic algorithm

A computational rule with at least one secret parameter, the → *key*, that can be used to encrypt or decrypt data. There are symmetric cryptographic algorithms (such as the DES algorithm) that use the same key for encryption and decryption, and asymmetric cryptographic algorithms (such as the RSA algorithm) that use a public key for encryption and a secret (private) key for decryption.

Cryptoprocessor

In the realm of smart cards, a supplementary numerical processing unit in a microcontroller that is optimized for the rapid computation of secret-key algorithms (such as DES) and/or public-key algorithms (such as RSA, DSA and ECC).

CT-API (Chipcard Terminal – Application Programming Interface)

An application-independent interface specification for connecting → *MKT* terminals to PCs; widely used in Germany. It is published by Teletrust Deutschland.

Customer card

In an electronic payment system, a → *smart card* used by customers to make payments at merchant terminals.

D-AMPS

→ *AMPS*

DEA (Data Encryption Algorithm)

Another name for → *DES*.

Deactivation sequence

Specifies the order of events for deactivation of the electrical signals for a → *smart card microcontroller* when powering down a → *smart card*. It does not say anything about the sequence of events for mechanical decontacting. The objective of the deactivation sequence is to protect the smart card microcontroller, which is sensitive to charges and voltages on its contacts. (→ *activation sequence*)

Debit card

A card, with or without a chip, that indicates that the cardholder has been granted certain powers of disposition, with which payment takes place when the goods or services are received. For this purpose, a debit card is linked to a bank account to allow the amount of the payment to be immediately transferred. This form of payment is often referred to as 'pay now'. A typical example of a debit card is the Eurocheque card.

Debugging

Searching for and eliminating errors, with the objective of detecting and correcting as many errors in a software program as possible. Debugging is normally performed by software developers during → *implementation* and is not the same as testing (→ *test*).

DECT (Digital Enhanced Cordless Telecommunications; previously 'Digital European Cordless Telecommunications')

A specification for cordless telephones operating the 1.9-GHz band using → *cellular technology* with digital data transmission; published by → *ETSI*. Although the DECT standard has provisions for using a smart card in the mobile part of the telephone, it is specified as being optional, with the result it is not used.

Defragmentation

The process of shifting data stored at different physical locations in memory until the data occupy a contiguous region of memory. The essential portions of a defragmentation process must operate in an atomic manner in order to prevent memory inconsistency in the event of premature termination of the process.

Delamination

The undesired separation of foils that have been attached to each other (laminated) using heat and pressure. Delamination of a card can for example be caused by using a non-thermoplastic ink to print overly large areas between the core foil and overlay foil. Such inks are commonly used in offset printing.

Depersonalization

Reversing the electrical → *personalization* of a smart card. If the → *smart card operating system* allows depersonalization, it may be performed using a special command following authentication. One use for depersonalization is to restore incorrectly personalized cards to their original condition, so that they can be reused.

DER (Distinguished Encoding Rules)

→ *BER*

DES (Data Encryption Standard)

The best known and mostly widely used symmetric → *cryptographic algorithm*, which was developed by IBM in combination with the NBS and published in 1977 as a US standard (FIPS 46) with the name 'Data Encryption Algorithm' (DEA).[13] The official successor to the DES is the → *AES*.

[13] See also Section 4.7.1, 'Symmetric cryptographic algorithms'

Design

In the context of software development, constructing a software architecture based on the requirements defined during → *analysis*. In simplified terms, the result of the design process is a description of 'how' the requirements are implemented in the software. In a sequential software development process, the subsequent stage is → *implementation*.

Deterministic

Designates a process or procedure that always produces the same result for a given set of initial conditions. It is the opposite of → *probabilistic*.

DF (dedicated file)

A directory in a smart card file system. The root directory (MF) is a special type of DF.

DF name

The DF name, like the file identifier (FID), is a DF attribute with a length of 1–16 bytes. It is used for selecting the DF, and it may contain a registered application identifier (AID), which has a length of 5–16 bytes and makes the DF internationally unique.[14]

Die, dice

A die (plural 'dice') is a small, flat piece of crystalline silicon on which a single semiconductor integrated circuit (such as a microcontroller) has been fabricated.

Differential fault analysis (DFA)

The principle of differential fault analysis was published in 1996 by Dan Boneh, Richard A. DeMillo and Richard J. Lipton, all of whom were employees of Bellcore [Boneh 96]. The method is based on intentionally introducing scattered errors into a cryptographic computation in order to determine the secret key. In the original method, only public-key algorithms were named, but within a few months this method of attack was rapidly extended [Anderson 96a], with the result that all cryptographic algorithms can in principle be attacked in this manner if they do not employ protective measures.

Differential cryptanalysis

A computational method for determining the value of a secret key using plaintext–ciphertext pairs having certain differences but the same key. The manner in which these differences

[14] See also Section 16.6, 'Registration Authorities for RIDs'

propagate with further DES cycles is analyzed to determine the key. This method was published by Eli Biham and Adi Shamir in 1990.

Digital

Designates a system in which signals can assume only a limited number of values.

Digital fingerprint

A commonly used designation for the hash value of a message (e.g., generated using the SHA-1 algorithm).

Digital signature

Digital signatures are used to establish the authenticity of electronic messages and documents. They are usually based on asymmetric cryptographic algorithms, such as the RSA algorithm. The legal validity of digital signatures is governed by legislation in many countries (such as the → *Signaturgesetz* in Germany). Digital signatures are sometimes referred to as 'electronic signatures'.

Digital watermark

A marking in an image or audio file, ideally invisible or inaudible, that cannot be removed and is used to protect proprietary rights. An analysis program can be used as necessary to check image or audio files for the presence of digital watermarks. Steganographic methods (→ *steganography*) are often used to generate digital watermarks.

Directory service

A service in a database that provides requestors with lists containing specific information. A typical example of such lists is a → *certificate revocation list*, which identifies all certificates that are no longer valid or accepted in a → *PKI*.

Divider

A short form for 'clock-rate conversion factor' (CRCF), which is commonly used in the smart card world. The CRCF specifies the duration of one bit interval during data transmission, in terms of the number of periods of the signal on the clock line.

Downlink

A connection from a higher-level system (such as a base station) to a lower-level system (such as a mobile telephone); the opposite of → *uplink*.

Download

Transferring data from a higher-level system (background or host system) to a lower-level system (e.g., a terminal); the opposite of → *upload*.

DPA (differential power analysis)

A method of attacking smart cards that represents an improvement on simple power analysis (→ *SPA*). It involves first making repeated measurements of the current consumption of a microcontroller for certain operations using known data with high time resolution and eliminating random noise by averaging. Following this, the current consumption is measured using unknown data, and conclusions regarding the unknown data are then drawn by analyzing the differences between the results for the known and unknown data. DPA was first made known in a publication by Paul Kocher, Joshua Jaffe and Benjamin Jun in June 1998 [Kocher 98].[15]

DRAM (dynamic random access memory)

A type of RAM having a dynamic structure that requires a continuous supply voltage and periodic refreshing to retain its content. DRAM cells are effectively capacitors. DRAM occupies less space on the chip than SRAM and is thus less expensive, but SRAM has shorter access times.

Dual-band mobile telephone

A mobile telephone that can operate in two different frequency bands (e.g., 900 MHz and 1800 MHz).

Dual-interface card

Designation for a → *smart card* having both contactless and contact-type interfaces for data transmission to and from the card.

Dual-mode mobile telephone

A mobile telephone that can operate in two different mobile telecommunication systems (e.g. GSM and AMPS).

Dual-slot mobile telephone

Designation for a mobile telephone having a second, externally accessible card contact unit, usually for an ID-1 → *smart card*, in addition to the contact unit for the user card (i.e., the

[15] See also Section 8.2.4.1, 'Attacks at the physical level'

SIM). A dual-slot mobile telephone could for example be used with an existing smart card electronic purse to make payments via the mobile telecommunication network.

Dual-slot solution

A smart card application based on using the second card contact unit in a dual-slot mobile telephone.

Duplicating

Transferring genuine data to a second card with the objective of producing one or more identical (cloned) cards. Generally synonymous with → *cloning*.

Dynamic STK (dynamic SIM Application Toolkit)

An outmoded expression for microbrowser solutions (→ *browser*) that are compliant with the → *SIM Alliance* specification.

ECBS (European Committee for Banking Standards) [ECBS]

A European organization founded in 1992 to develop technical solutions and standards for the infrastructure of → *interoperable* trans-European financial transaction systems.

ECC (elliptic curve cryptosystem)

Designation for a cryptographic system (generally speaking, a cryptographic algorithm) based on elliptic curves.

ECC (error correction code)

A data checksum. An ECC can be used to allow errors in the data to be detected with a certain probability and in some cases fully corrected.

E-commerce (electronic commerce)

Refers to all forms of service, trade and associated financial transactions using public networks (primarily the Internet). The term → *m-commerce* is used when mobile terminals are used for e-commerce.

EDC (error detection code)

A data checksum. An EDC can be used to allow errors in the data to be detected with a certain probability. Typical examples of EDCs are the XOR and CRC checksums used in various data transmission protocols.

EDGE (Enhanced Data Rates for GSM and TDMA Evolution)

EDGE is intended to be the final evolutionary step for GSM networks. The EDGE specification allows a GSM mobile telephone to connect to a base station with a data rate of up to 384 kbit/s by using a different modulation scheme, without altering the existing network infrastructure.

EEPROM (electrically erasable programmable read-only memory)

A type of non-volatile memory, which is used in → *smart cards*. An EEPROM is divided into 'pages' of memory, with the page size being called its → *granularity*. The content of a memory page can only be altered or erased as an entity, and there is a physically determined upper limit to the number of write or erase cycles.[16] Data storage in an EEPROM cell is based on the Fowler–Nordheim effect, rather than hot electron injection as with → *Flash EEPROM*. The typical write time for EEPROM is 3 ms per memory page.

EF (elementary file)

The actual data storage element in a smart card file tree. An EF has either the attribute 'working' (for use by the terminal) or 'internal' (for use by the smart card operating system), and an internal structure (transparent, linear fixed, linear variable, cyclic, etc.).[17]

Electronic check

An → *electronic purse* variant using fixed, non-divisible monetary amounts. This type of payment is often referred to as 'pay before'.[18]

Electronic purse (e-purse)

A card with a chip that must be loaded with an amount of money before it can be used for making payments. This type of payment is often called 'pay before'. Some typical examples are the German Geldkarte, the Austrian Quick purse, Visa Cash, Proton and Mondex. Electronic purses may also support → *purse-to-purse transactions*.[19]

[16] See also Section 3.4.2, 'Memory types'
[17] See also Section 5.6.4, 'EF file structures'
[18] See also Section 12.1.2, 'Electronic money'
[19] See also Section 12.1.2, 'Electronic money'

Embossing

Part of the physical personalization of a card, consisting of raised characters stamped into the plastic card body.

Emulator

A device that imitates the operation of some other device or equipment (the target system). An emulator implemented in software is called a → *simulator*. Emulators are frequently used in developing software for not yet existing target systems. A smart card emulator is thus hardware circuitry that completely imitates the electrical and logical properties of a real smart card. Since the majority of the functionality is implemented in hardware, emulators are usually faster (closer to real-time) than simulators.

EMV (Europay, MasterCard, Visa) [EMV]

A joint specification for payment cards with chips and associated terminals belonging to Europay, MasterCard, Visa and American Express. These specifications have achieved the status of international industry standards for credit and debit cards and electronic purses. In the payment system sector, they thus represent the counterpart to the GSM 11.11 telecommunications standard.

EMV specification

→*EMV*

End-to-end link

Direct communication between two parties using the communication paths of one or more other entities that do not alter the information content of the actual data exchange. If the messages exchanged by the two originating parties are cryptographically secured, the term → *tunneling* is used. A typical example of an end-to-end link is direct communication between an application provider and a SIM that is compliant with GSM 03.48.

Endianness

The term 'endianness' refers to the order of the bytes within a byte string. 'Big-endian' means that the most significant byte stands at the beginning of the byte string, which consequently means that the least significant byte stands at the end of the string. 'Little-endian' refers to the opposite order, which means that the least significant byte comes first and the most significant bit comes last.

Enrollment

The process of originally acquiring the biometric data of a → *cardholder* and entering it into the corresponding smart card. The data stored in the smart card then form the basis for subsequent biometric user identification.

Envelope stuffing

Automatically folding letters and inserting them into envelopes.

EP SCP

→*SMG9*

EPROM (erasable programmable read-only memory)

A type of non-volatile memory, which was formerly used in smart cards but has been fully supplanted by → *EEPROM* technology. Since EPROM can only be erased by ultraviolet light, it can only be used for WORM storage (write once, read multiple) in smart cards.[20]

Error counter

A counter that accumulates negative results and determines whether a particular secret (PIN or key) may continue to be used. If the error counter reaches its maximum value, the secret is blocked and can no longer be used. The error counter is normally reset to zero when the operation is completed successfully (positive result). Also called a retry counter.

ETS (European Telecommunication Standard)

Designation for standards issued by → *ETSI*, which are primarily concerned with European telecommunications.

ETSI (European Telecommunications Standards Institute) [ETSI]

The standards institute of the European telecommunication companies, with headquarters in Sophia Antipolis, France. ETSI is responsible for defining standards in the field of European telecommunications. The most important ETSI standards are the family of standards for GSM (e.g., GSM 11.11 for the SIM) and UMTS (e.g., TS 31.102 for the USIM). Meetings of the expert groups of the ETSI are usually held in a wide variety of (touristically attractive) locations in Europe and throughout the world, for which reason some people are convinced that the abbreviation 'ETSI' stands for 'European travel and sightseeing institute'.

[20] See also Section 3.4.2, 'Memory types'

etu (elementary time unit)

The duration of one bit in smart card data transmission. The length of the etu is not defined in absolute terms, but instead in terms of the frequency of the clock signal applied to the card and the value of the clock-rate conversion factor (divider).

Eurosmart [Eurosmart]

An organization founded in 1994 to represent the interests of European manufacturers of smart cards, with offices in Brussels. The functions of Eurosmart are promoting and standardizing (→ *standard*) → *smart cards* and smart card systems, providing a forum for exchanging market data and technical data, and forging links to national and international standards committees.

Evaluation

The unbiased, objective, repeatable and reproducible assessment of an information technology system (hardware and/or software) by a reliable body according to the specifications of a criteria catalog. The IT system to be evaluated is called the → *target of evaluation*. Commonly used international criteria catalogs for the evaluation of → *smart cards* are the → *ITSEC* and → *Common Criteria*.

f1, f2, f3, f4, f5 (function 1 – function 5)

Designations for cryptographic functions used in → *UMTS* for authenticating the network and the → *USIM* and establishing cryptographically secured data transmission on the air interface. The central element of these security functions is a symmetric → *cryptographic algorithm* that can be parameterized using supplementary linked initial values. As an example algorithm for f1–f5, the USIM specification proposes the MILENAGE algorithm, which is essentially based on the → *AES*.

Fab

A semiconductor fabrication facility.

Face

The face of a semiconductor chip is the side holding the functional structures produced using semiconductor fabrication processes. Consequently, an expression such as ‘face-to-face contacting’ means that two chips with suitably configured functional structures are placed together such that they are electrically connected to each other.

FAT (file allocation table)

A table used in a file management system in which the storage area to be managed is divided into sections, called ‘clusters’. Data related to the occupancy and addresses of these sections are stored and managed using the file allocation table.

Fault tree analysis

A test method in which every program execution path in the program code is traversed in order to search for possible errors.

FD/CDMA (frequency division / code division multiple access)

→*CDMA*

FDMA (frequency division multiple access)

Ag →*multiple-access method* for concurrently transferring data from several transmitters to a single receiver using several different frequency bands. Each transmitter is allocated a particular frequency band within the total available frequency spectrum, within which it may exclusively transmit. Many mobile telephone systems (such as the German C-Netz) use FDMA for the air interface between the mobile telephone and the basis station.[21]

FIB (focused ion beam)

A device for generating a focused beam of ions for removing or depositing material on a semiconductor device.

FID (file identifier)

A two-byte attribute of a file. Each MF, DF and EF has a FID. The FID of the MF is always '3F00'.[22]

File body

→ *file header*

[21] See also Section 13.1.1, ‘Multiple-access methods’
[22] See also Section 5.6, ‘Smart Card Files’

File header

Files in smart cards are usually divided into two separate parts, consisting of the file header (which holds information about the → *file structure* and → *access conditions*) and the file body, which is linked to the file header by a pointer and holds the modifiable user data.

File structure

The externally visible structure of an → *EF*. File structures allow user data to be stored in a logically structured and compact manner. The standard file structures defined by ISO/IEC 7816-4 are transparent, linear fixed, linear variable and cyclic.[23]

File type

Identifies the sort of file for purposes of file management within a smart card, i.e., whether it is a directory file (MF or DF) or a file for storing user data (EF).

FIPS (Federal Information Processing Standard)

US American standards issued by the → *NIST*.

Firewall

An entity (hardware or software) that provides a security barrier between particular → *applications* or other entities. For example, a firewall can separate two applications in a smart card such that they cannot access each other's data across the firewall. The name comes from a type of wall used in building construction to contain possible fires.

Flash

Commonly used short form for → *Flash EEPROM*.

Flash EEPROM (Flash electrically erasable programmable read-only memory)

A type of non-volatile memory, which will be used in smart cards in the future. A Flash EEPROM resembles an → *EEPROM* in terms of its functionality and semiconductor structure, but data storage in Flash EEPROM cells is based on hot-electron injection, instead of the Fowler–Nordheim effect as in regular EEPROMs. In the hot-electron injection process, 'fast' electrons are generated by a high potential difference between the source and the drain, and some of these fast electrons penetrate the tunnel oxide layer and are stored in the floating

[23] See also Section 5.6.4, 'EF file structures'

gate. This effect reduces the write time to approximately 10 µs. Due to their large memory pages (typically 128 bytes at present), Flash EEPROMs are quite suitable for replacing mask-programmed → *ROM*.[24]

Floor limit

Defines the level at which a purchase must be authorized (→ *authorization*) by a third party. Authorization is not required below the floor limit, but it must always be obtained above the floor limit, since otherwise payment may not be possible or guaranteed.

Footprint

More precisely, 'memory footprint': refers to the allocation of memory for a particular purpose.

Foundry

A semiconductor fabrication facility operating on a contract basis to manufacture semiconductor devices developed by third parties.

FPLMTS (Future Public Land Mobile Telecommunications Service)

→ *IMT-2000*

FRAM (ferroelectric random-access memory)

A type of non-volatile memory, which is very rarely used in → *smart cards*. A FRAM is divided into memory pages (the page size is also called the → *granularity*). Data storage in this type of memory is based on the properties of a ferromagnetic substance placed between the control gate and the floating gate. FRAM cells typically have a write time of 100 ns per page and do not require a special erase voltage. However, the number of erase cycles is limited, and manufacturing FRAM involves processes that are difficult to master. Consequently, it has been used only rarely in smart card microcontrollers up to now.

Frame

A sequence of data bits and optional error detection bits bounded by frame delimiters. Frames for contactless data transmission with smart cards are defined in ISO/IEC 14 433.

[24] See also Section 3.4.2, 'Memory types'

Full duplex

Data transmission method in which each of the communicating parties can transmit and receive concurrently. (→ *half duplex*)

Garbage collection

A function that collects memory no longer used by an → *application* and makes it available as free memory. In the past, garbage collection was implemented by interrupting regular program execution. In modern computer systems, garbage collection is a low-priority thread that constantly searches the memory for regions that are no longer needed and returns them to the free memory pool.

Geldkarte

Brand name of an electronic purse introduced in Germany in 1996. 'Geldkarte' refers to both the application in a → *multiapplication smart card* and the smart card itself. The smart card operating system used for the Geldkarte or debit functionality is → *SECCOS*.

Glitch

A very short voltage dropout or voltage spike.

Global Platform [Global Platform]

An internationally active association founded in 1999 by various smart card companies to standardize technologies for → *multiapplication smart cards*. The most important specification published by Global Platform is the Open Platform specification (→ *OP*).

Good case

The case in which a logical decision yields a favorable or intended result.

GPRS (General Packet Radio System)

An extension of → *GSM*, standardized by → *ETSI*, for achieving higher data transmission rates with mobile telephones. GPRS provides a packet-switched connection with a data transmission rate of up to 115.2 kbit/s by bundling the eight available time slots, each of which has a capacity of 14,400 bit/s. A mobile telephone with GPRS technology is constantly connected to the network with respect to data transport and thus always available for data transmission. The data transmission rate is dynamically adapted to the currently required capacity, so only the capacity actually needed is used. For this reason, GPRS is very suitable for discontinuous data transfers.

Granularity

A frequently used alternative term for expressing the page size of an → *EEPROM*. For example, an EEPROM with a granularity of 32 has a page size of 32 bytes.

Graybox test

A mixed form combining elements of blackbox and whitebox tests, in which the party performing the test knows some but not all of the internal processes, functions and mechanisms of the software being tested.

Graylist

A list in a database identifying all → *smart cards* or devices that are under observation. (→ *blacklist, hotlist, white list*)

GSM (Global System for Mobile Communications)

A digital, cellular, interoperable, transnational and ground-based second-generation (→ 2*G*) mobile telecommunication system. The frequency bands allocated to this mobile telecommunications system are 900 MHz (GSM 900), 1800 MHz (GSM 1800) and 1900 MHz (GSM 1900). The GSM system is defined by a family of specifications published by → *ETSI*. The alliance of the major network operators and manufacturers is the → G*SM Association*. Originally, GSM was only planned to be used in certain central European countries as a successor to country-specific analog mobile telephone systems. However, it has developed into an international standard for mobile telecommunication systems. Due to the low data transmission rates of the GSM system (9600 bit/s and 14,400 bit/s), improvements to the system have become necessary. The evolutionary path of the GSM system with respect to data transmission capacity thus envisages circuit-switched → *HSCSD* and packet-switched → *GPRS* as the next steps in the further development of the system. Afterwards, the GSM data transmission rate can be further increased using → *EDGE* technology. The designated successor to GSM is → *UMTS*.[25]

GSM Association [GSM Association]

An internationally active body for coordinating mobile telecommunications systems, with offices in Dublin and London. It was founded in Copenhagen in 1987 and is responsible for the development and use of → *GSM* standards. The GSM Association represents more than 500 network operators, manufacturers and suppliers in the GSM industry.

[25] See also Section 13.3, 'The UMTS System'

Guilloches

Decorative patterns of interwoven lines, usually circular or oval, found on many banknotes and share certificates. Due to their fine structures, these patterns can only be reproduced at high quality using printing techniques, so they are difficult to copy.

HAL (hardware abstraction layer)

An intermediate layer in an operating system, which is used to conceal all hardware-specific features of the target platform from the rest of the operating system. The objective of this is to markedly simplify porting of the operating system, since changing the hardware platform only requires modifications within the HAL.[26]

Half-byte

→ *nibble*

Half duplex

Data transmission method in which each of the communicating parties cannot concurrently send and receive data. A → *full-duplex* connection is required for concurrent transmission and reception.

Handover

In a mobile telecommunication network, the interruption-free transfer of a mobile telephone from one cell to the next. In GSM, a handover is always initiated by the network.

Happy-day scenario

Another expression for → *good case*.

Hard mask

The term 'hard mask' means that the entire → *program code* is predominantly stored in ROM (→ *ROM mask*). This saves space compared with a soft mask, since ROM cells are significantly smaller than EEPROM cells. However, it has the disadvantage that the full duration of the process of producing a customer-specific semiconductor device is required to generate hard-masked microcontrollers. Consequently, the lead time for a hard mask is significantly longer than for a soft mask. Hard masks are normally used with large numbers of chips for smart cards having largely common functionality. The opposite of a hard mask is a → *soft mask*, which involves storing essential functions in EEPROM.

[26] See also Section 5.2, 'Basics'

Hash function

A hash function is a procedure for compressing data using a one-way function such that it is not possible to recompute the original data. A hash function produces a fixed-length result for an input with any arbitrary length, and it is designed so that any change to the input data has a very high probability of affecting the computed hash value (output data). SHA–1 is a typical representative of hash algorithms. The result of a hash function is a hash value, which is often also referred to as a digital fingerprint.[27]

HBCI (Home Banking Computer Interface)

A standard defined by the German banking industry for the implementation of home banking in Germany, with optional smart card support.

Hologram

A photographic exposure made using a holographic process. It produces a three-dimensional image of the photographed object. The object in the photograph can thus be seen from different angles, depending on the viewing angle of the observer. The holograms normally used with smart cards are embossed holograms, which produce reasonably satisfactory three-dimensional images under normal lighting conditions.

Home net

With respect to a customer of a mobile telecommunications system, the mobile telecommunication network operated by the company for which he or she is a customer.

Home zone

In a mobile telecommunications network, a → *location-based service* in which calls are charged at a significantly lower rate (normally the fixed-network rate) within a certain region (usually the immediate vicinity of the user's residence). As a result, the subscriber may not need to have a connection to the fixed telephone network.

Horizontal prototype

→ *prototype*

Hotlist

A database list of → *smart cards* and devices that probably have been manipulated and must not be accepted under any circumstances. (→ *blacklist, graylist, white list*)

[27] See also Section 5.2, 'Hash Functions'

HSCSD (High-Speed Circuit-Switched Data)

The circuit-switched HSCSD technology is an extension to the GSM standard for increasing the data transmission rate over the air interface to a theoretical value of 76,800 bit/s (8 × 9600 bit/s) for uplink or downlink by supplementary utilization of existing time slots. Existing GSM networks can be extended to support HSCSD at a relatively low cost by upgrading the base stations and using special mobile telephones. The drawback is that the demand for transmission channels can increase by as much as factor of eight.

HSM (hardware security module, host security module)

→ *security module*

HTML (hypertext markup language)

A logical markup language for hypertext documents in the WWW, which is conceptually based on XML. (→ *WML, WWW, XML, hypertext*)

Hybrid card

A card having two different card technologies. Cards having both magnetic stripes and chips, and smart cards with optical storage on the card surface, are typical examples.

Hypertext

Compared with normal text, hypertext has supplementary cross-references (hyperlinks) to other locations in the text or to other documents. These cross-references can be invoked by suitable user actions (usually by clicking on them). As opposed to normal linearly structured text, such as in books, hypertext allows any desired interlinking of texts to be achieved using cross-references. Typical examples of markup languages for hypertext documents are → *HTML* and → *WML*.

ICC (integrated chip card)

The official ISO name for a card with a chip, which may be a memory chip or a microcontroller chip.

ID-l card

Standard format for → *smart cards* as specified by ISO 7810 (length ≈85.6 mm, width ≈54 mm, thickness ≈0.76 mm).[28] However, the ID-000 (plug-in) format is predominately used in the mobile telecommunications area.

Identification

The process of verifying the authenticity of a device or a person by comparing a password provided by the device or person to a stored reference password. Identification can be considered to be a special case of → *authentication*, in which the identity of a person is authenticated. The method used for identification is sometimes referred to as the → *cardholder verification method*.

IEC (International Electrotechnical Commission) [IEC]

The IEC was founded in 1906 and is based in Geneva, Switzerland. Its function is to generate international standards for electrical and electronics technology.

IFD (interface device)

The official ISO name for a smart card terminal.

Implanter

A production machine for smart cards whose function is to insert modules in the cavities of smart cards, which is called 'implanting' in trade jargon.

Implementation

In the context of software development, producing a program on the basis of a software architecture defined in the → *design* stage. Implementation also includes debugging, but not testing (→ *test*), which occurs in the subsequent stage in a sequential software development project.

IMSI catcher

A device that taps GSM conversations by setting up its own cell. An IMSI catcher works by interposing itself between the mobile telephone and the base station; it represents itself as a base station with respect to the mobile telephone and as a mobile telephone with respect to the base station.

[28] See also Section 3.1.1, 'Card formats'

IMT-2000 (International Mobile Telecommunication 2000)

A concept of the → *ITU* for third-generation (→ *3G*) mobile telecommunications systems operating in the 2000-MHz frequency band. IMT-2000 arose in 1995 as a successor to the Future Public Land Mobile Telecommunication Service (FPLMTS), a mobile telecommunications concept initiated by the ITU in 1985 that failed to be translated into reality as an international standardized system in its original form. One possible realization of IMT-2000 is → *UMTS*.

Individualization

→ *personalization*

Initializer

An entity that performs →*initialization*.

Initialization

The process of loading the fixed, person-independent data of an → *application* into EEPROM. A synonym for initialization is 'pre-personalization'.

Instrumenting

Introducing special → *program code* into a program in order to allow the procedures and calls of the program to be analyzed for test purposes.[29]

Intelligent memory card

A memory card having additional logic circuitry for supplementary security functions that monitor memory accesses.

Internal foil

A foil located inside the stack of foils laminated together to make a card body; synonymous with 'core foil'. Normally, an internal foil is laminated between two outer (cover) foils, with these three foils together forming the card body. The internal foil often carries security features or electrical components, such as the coil for a contactless smart card.

[29] See also Section 9.3.3, 'Dynamic testing of operating systems and applications'

Interoperable

This adjective is used in the smart card world to designate solutions that are not tailored to a particular smart card → *application* or the equipment of a particular manufacturer. An → *open smart card operating system* is usually interoperable. The opposite of an interoperable solution is a → *proprietary* solution. An example of an interoperable smart card is the SIM, which can be used equally well in all types of GSM mobile telephones without compatibility problems.

Interpreter

A program that translates the instructions of a programming language such as Basic or Java into machine-language instructions that can be executed by a microprocessor, and immediately executes each instruction after it has been translated. Interpreted programs always run more slowly than compiled → *program code*, since the translation occurs at run time. However, a significantly higher level of hardware independence in programming is possible with interpreted code than with compiled code.

ISDN (Integrated Services Digital Network)

Designation for an internationally standardized digital telephone network that supports both telephone conversations and data transmission. An ISDN link consists of two base channels, each having a transmission rate of 64 kbit/s, and a control channel with a transmission rate of 16 kbit/s.

ISO (International Organization for Standardization) [ISO]

ISO was founded in 1947 and is based in Geneva, Switzerland. Its function is to support the generation of international standards in order to promote the free exchange of goods and services. The first ISO standard was published in 1951 and deals with temperatures with regard to length measurements.

ITSEC (Information Technique System Evaluation Criteria)

A catalog of criteria for the → *evaluation* and certification of the security of information technology systems in Europe, published in 1991. The → *Common Criteria* resulted from refining the ITSEC and combining the ITSEC with various national criteria.

ITU (International Telecommunications Union)

An international organization for the coordination, standardization and development of global telephone services, based in Geneva. It is the successor to the CCITT.

Java

A hardware-independent, object-oriented programming language (→ *object-oriented programming*) developed by the Sun Corporation, which is widely used on the Internet. Java source code is translated by a compiler into standardized bytecode, which is then usually interpreted by a virtual machine based on the target hardware (Intel, Motorola, etc.) and operating system (Windows, MacOS, Unix, etc.) platforms. There are also microprocessors (such as picoJava) that can directly execute Java bytecode.

Java card, Java Card

A Java card is a → *smart card* with a → *microcontroller* containing a → *Java Card virtual machine* and a → *Java Card runtime environment*. Java cards are → *multiapplication smart cards* incorporating the Java Card operating system, which can manage and run programs written in Java. Strictly speaking, Java Card is not a true → *operating system*, in part because the original specification does not include file management. However, in practice Java Card is considered to be the archetype of an → *open smart card operating system*.

Java Card Forum [JCF]

An internationally active organization founded by several smart card companies in 1997 to promote Java Card technology and develop related specifications (→ *Java Card*).

Java Card runtime environment (JCRE)

The Java Card runtime environment essentially consists of the → *Java Card virtual machine* (JCVM) and the Java Card API.

Java Card virtual machine (JCVM)

(→ *virtual machine*) A simulation of a microprocessor (usually implemented in software) whose function is to execute Java bytecode and manage Java classes and objects. The Java Card virtual machine also ensures application separation by means of firewalls and allows common utilization of data. In principle, it can be regarded as a type of interpreter. A Java VM implemented using publicly accessible information, i.e. without using additional information subject to a licensing agreement with Sun, is called a 'cleanroom VM'. Cleanroom implementations of the Java VM are generally considered to be free of any obligation to pay licensing fees to Sun.

Java development kit (JDK)

A collection of software tools supporting the development of Java software.

Kerckhoff's principle

A principle named after August Kerckhoff (1835–1903) that asserts that the entire security of a cryptographic algorithm should be based exclusively on the confidentiality of its key, rather than the confidentiality of the algorithm.

Kernel

The central part of a → *operating system*, which provides basic operating system functions to the overlying layers of the operating system.

Key

For a → *cryptographic algorithm*, the parameter that individualizes the encryption or decryption process. With a symmetrical cryptographic algorithm that is used to ensure security, the key must be secret, but the public key of an asymmetric cryptographic algorithm may be generally known.

Key fault presentation counter

→*error counter*

Key management

Collectively, all administrative functions used for generating, distributing, storing, updating, destroying and addressing cryptographic keys.

Kinegram

A kinegram shows different images when viewed at different angles. It can show an apparently 'moving' image that changes in jerks, or it can show completely unrelated images at different viewing angles. Kinegrams are similar to holograms, which show three-dimensional images, but are not identical to them.

Lamination

The process of gluing together thin sheets of material using heat and pressure. Cards are generally laminated from several plastic foils.

Laser cutter

A device for drilling and cutting, preferably on a semiconductor chip, with a precision of a fraction of a micrometer using a high-energy laser beam.

Laser engraving

A process for blackening special plastic layers by 'burning' them with a laser beam. This is also colloquially referred to as 'lasing'.

Lead-frame module

A type of low-cost module having contacts stamped from a copper alloy electroplated with a gold film and held together by a plastic mold body. A chip is placed on the lead-frame module by a pick-and-place robot and electrically bonded to the rear surfaces of the contacts using wire bonding. After this, the chip is covered by a blob of opaque epoxy resin for its protection.

Lead-frame process

Currently one of the least expensive ways to produce modules without incurring penalties with regard to mechanical stability.

Lead time

In semiconductor fabrication, the time between when the mask is provided (→ *ROM mask*) and the time when the first samples are ready.

Life cycle

The aggregate of the stages in the life of a → *smart card*, beginning with the production of the chip and the card, progressing through → *personalization* and use and ending with the logical or physical end of the card's life. The individual stages in the smart card life cycle are used to define specific security measures and functionalities. An example of the partitioning of the life cycle of a card is the→ *Open Platform* specification.

Life cycle model

A model, sometimes referred to as a process model, that specifies, in abstract form, the organizational framework, work processes and activities of a development process, including the associated prerequisites and results. The objective is to achieve a uniform, general-purpose approach to software development. Some examples of life-cycle models are the waterfall model, the V model and cyclic development models.[30]

[30] See also Section 15.7, 'Life-Cycle Models'

Linker

The function of a linker is to convert the symbolic memory addresses of compiled or assembled program code into absolute or relative memory addresses.

Little-endian

→*endianness*

Load agent

An entity that loads electronic money into an electronic purse. In a manner of speaking, a load agent is the counterpart of a service provider.

Loader

A program that can be used to load other programs (→ *boot loader*), for example via a serial interface.

Location-based services

Value-added services for mobile telephone subscribers that are based on knowledge of the subscriber's current geographic position. Some examples are local weather forecasts, city maps that are dynamically adapted to the user's current location and integrated location data for service calls.

Logical channels

Logical channels allow data to be exchanged concurrently and independently with several → *applications* in a smart card. Although communication with the smart card still takes place via the single serial interface in the card, logical channels allow the applications in the smart card that receive the → *APDUs* to be individually addressed.[31]

M-commerce (mobile commerce)

Collective term for all types of services, trade and associated financial transactions using mobile terminals (such as mobile telephones and PDAs). If fixed terminals are used, the term → *e-commerce* is used.

[31] See also Section 6.7, 'Logical Channels'

M/Chip

The name given to an → *EMV*-compliant implementation of a chip-based debit/credit card from Europay and MasterCard. The M/Chip Select version uses both symmetric and asymmetric cryptographic algorithms and is a superset of M/Chip, which is a simplified version that uses only symmetric cryptographic algorithms.

MAC (message authentication code)

A cryptographic checksum for data that allows manipulation of the data during transmission to be detected. An equivalent checksum used to protect stored data is called a CCS (→ *cryptographic checksum*).

Magnetic card

A commonly used but technically incorrect short form of → *magnetic-stripe card*.

Magnetic-stripe card

A card with a magnetic stripe for recording and subsequently reading data. The magnetic stripe usually has three data tracks with different data recording densities. Tracks 1 and 2 are used only for reading after the card has been issued, but data may also be written to track 3 during normal use. The magnetic substance in the stripe may have either a high-coercivity characteristic or a low-coercivity characteristic.

Maosco

→ *Multos*

Mask

An abbreviated form of → *ROM mask*.

Memory card

A card with a chip that has a simple logic circuit along with memory that can be read and/or written. Memory cards can also have supplementary security logic units, which for example can allow the card to be authenticated.

Memory footprint

The structure of memory allocation in a computer system.

Merchant card

In an electronic payment system, a → *smart card* located in a merchant terminal and serving as a security module.

Method

In the context of → *object-oriented programming*, a function used to alter the values of the → *attributes* of an → *object*, which is generated by the → *class* of the object.

MexE (Mobile Station Execution Environment)

A Java framework for integrating a Java virtual machine (JVM) into a mobile telephone. It allows Java programs to be loaded into the mobile telephone and executed. This allows supplementary applications to be implemented directly in the mobile telephone, rather than in the SIM (as in current practice).

MF (master file)

The master file of a smart card file system is a special type of DF. It is the root directory of the file tree and is automatically selected after the smart card has been reset.

Microbrowser

→ *browser*

Microcontroller

A microcontroller consists of a → *microprocessor*, volatile memory (→ *RAM*), non-volatile memory (→ *ROM*, → *EEPROM*, → *Flash EEPROM*) and suitable interfaces for off-chip communications, all integrated into a single chip. It is thus a self-contained and fully functional computer on a single chip. Microcontrollers are primarily used in smart cards and control technology.

Microprocessor

The most important component of a → *microcontroller*. The microprocessor resolves the machine instructions specified by the program code into microinstructions and executes the microinstructions. A microprocessor contains the registers needed for instruction processing, a control mechanism and a processing unit. The actual processing unit of a microprocessor is sometimes simply called the ‘processor’. The term ‘central processing unit’ (CPU) is often used as a synonym for ‘microprocessor’.

Microprocessor card

A card containing a → *microcontroller* with a CPU, volatile memory (RAM) and non-volatile memory (→ *ROM*, → *EEPROM* etc.). A microprocessor card may also contain a numeric coprocessor (→ *cryptoprocessor*) to quickly execute public-key cryptographic algorithms. Such a card is sometimes called a cryptocard or cryptocontroller card.

MILENAGE algorithm

The symmetrical sample algorithm for the f1–f5 (→ *f 1*) functions of → *USIM*. The kernel of the MILENAGE algorithm is based on the → *AES*.

MKT (*Multifunktionales Kartenterminal*)

The German abbreviation (and name) of a specification for multifunctional smart card → *terminals* and the connections to such terminals using the → *CT-API* interface specification. It supports both → *memory cards* and → *microprocessor cards*. The specification is published by Teletrust Deutschland.

Module

→ *chip module*

Module manufacturer

An entity that attaches dice to blank modules and electrically connects each die to the module contacts.

Mondex [Mondex]

An → *electronic purse* system using smart cards that allows → *purse-to-purse transactions*.

Mono-application smart card

A smart card containing only one → *application*.

Monofunctional smart card

A microprocessor card whose operating system supports only one specific → *application*, and which may even be optimized for this application. Such cards provide little or no support for administrative functions, such as file creation and deletion.

Monolayer card

A card composed of only one layer of plastic (→ *multilayer card*).

MoU (Memorandum of Understanding)

The common legal basis for all GSM network operators. The organization behind the MoU is the → *GSM Association*.

Multiapplication smart card

A smart card containing several → *applications*, such as a bank card with a phone-card function.

Multifunctional card (MFC)

Usually, a microprocessor card that supports multiple → *applications* and has corresponding administrative functions for storing and deleting applications and files.

Multilayer card

A card made up of several layers of plastic foil, consisting of the outer or cover foils (overlay foils) and the inner foils (core foils). (→ *monolayer card*)

Multiple-access method

Any of several methods used in radio communications and information technology to make a limited frequency bandwidth concurrently or quasi-concurrently available to the largest possible number of users. The four commonly used multiple-access methods are frequency division multiple access (→ *FDMA*), time division multiple access (→ *TDMA*), code division multiple access (→ *CDMA*) and space division multiple access (→ *SDMA*).[32]

Multiple-copy sheet

In printing, a collection of small items (such as cards) printed on a single large sheet, which is divided into individual items after printing. This allows the printing process to be technically optimized, since many items can be printed in one pass on a large sheet instead of in several separate passes. For instance, a typical multiple-copy sheet for printing cards holds 42 cards on a large plastic sheet.

[32] See also Section 13.1.1, 'Multiple-access methods'

Multitasking

A computer system that supports multitasking allows several programs to be run quasi-concurrently. Each of the concurrently running programs is usually located in a separate address space that is protected against access by other programs, and it can exchange data with other programs only by means of special mechanisms. Multitasking is not the same as multithreading, in which a single program performs several different tasks quasi-concurrently. A computer system may support both multitasking and multithreading.

Multithreading

A computer system that supports multitasking allows a single program to perform several different tasks quasi-concurrently. The individual threads of a program normally use a common address space. Multithreading is not the same as multitasking, in which several different programs run concurrently, each with its own separate address space. A computer system may support both multitasking and multithreading.

Multos

Brand name of an open, multiapplication → *smart card operating system* (→ *open smart card operating system*).[33] The Maosco Consortium [Maosco] publishes the specification, licenses the software and operates the certification services for Multos.

Name space

A set of names in which all of the names are unique.

Native code

A program whose instructions are in the specific machine language of the microprocessor that executes the program.

NBS (National Bureau of Standards)

The name of the → *NIST* prior to 1988.

NCSC (National Computer Security Center) [NCSC]

The NCSC is a subagency of the US National Security Agency (NSA). It is responsible for testing security products and publishing criteria for secure computer systems, including the TCSEC.

[33] See also Section 5.14.2, 'Multos'

Negative file

→*blacklist*

Negative result

→*bad case*

Nibble

The four most significant or least significant bits of a byte; also called a half-byte.

NIST (National Institute of Standards and Technology) [NIST]

A section of the US Department of Commerce responsible for US national standards for information technology. The NIST, which was called the NBS until 1988, publishes the FIPS standards.

Noiseless

A property of a → *cryptographic algorithm* that always takes the same amount of time to encrypt or decrypt data, irrespective of the → *key*, plaintext and ciphertext involved. If a cryptographic algorithm is not noiseless, the size of the key space can be markedly reduced by analyzing the processing-time characteristics of the algorithm. This allows the key to be determined significantly faster than by using a brute-force attack.

Non-repudiation

A usually cryptographic method to ensure that the recipient of a message cannot refuse to acknowledge (repudiate) receipt of the message, thus enabling the sender of the message to prove that the intended recipient actually received the message. Non-repudiation is similar to a registered letter with return receipt in an ordinary postal system.

Non-volatile memory

A type of memory (such as ROM, EPROM or EEPROM) that retains its content even in the absence of power.

NPU (numeric processing unit)

→*cryptoprocessor*

NSA (National Security Agency) [NSA]

The official communications security agency of the US government. It reports directly to the Department of Defense, and one of its functions is to monitor and decode foreign communications. Developing new cryptographic algorithms and restricting the use of existing algorithms also fall under the authority of this agency.

Null PIN

→ *0−PIN*

Numbering

Embossing or printing a number on a smart card; typically used in the manufacturing of anonymous prepaid phone cards to give each card a visible, unique number so it can be unambiguously identified.

Object

In the context of → *object-oriented programming*, a software structure that is built according to the instructions defined by a → *class* and contains data, which means that it has → *attributes* that can be read and altered using the → *methods* defined in the class.

Object-oriented programming

Object-oriented programming is based on storing all of the data of a software application in → *objects*, which also provide → *methods* that can be used to read or modify the data. Objects are defined by → *classes*. A key aspect of object-oriented programming is that it focuses on the data to be processed, rather than on the processes as does → *procedural programming*. Some typical object-oriented programming languages are C++ and → *Java*.

OCF (Open Card Framework) [OCF]

The Open Card Framework specification describes a platform-independent, Java-based interface for integrating smart cards into any desired application on a PC. It presupposes the availability of a suitable driver for each type of terminal to be used with the PC in question, and that the smart cards are OCF-compatible.

Offcard application

→ *application*

Oncard application

→ *application*

Oncard matching

The ability of a → *smart card* to compare biometric data measured either oncard or offcard with reference stored in the smart card for the purpose of user → *identification*.

One-way function

A one-way function is a mathematical function that is easily computed but whose inverse function requires a large amount of computational effort.

OP (Open Platform)

Previously Visa Open Platform (VOP); an interface in a smart card operating system, originally specified by Visa International, that supports the management of smart card applications. The specification encompasses, among other things, downloading smart card applications, securing the application life cycle and linking a smart card application to the smart card operating system. The OP specification is effectively the international industry standard for multiapplication smart cards and application management. The current publisher of the OP standard is the Global Platform association.

Open application

An → *application* in a smart card that is available to a variety of service providers (such as merchants and vendors of services) without requiring a mutual legal relationship.

Open platform

→*open smart card operating system,* → *OP*

Open purse

An instance of an open → *application* for an → *electronic purse*. It can be used for general payment transactions with various service providers.

Open smart card operating system

A → *smart card operating system* is characterized as being open if it is possible for third parties to load applications and programs into the smart card and run them in a secure environment, all without the involvement of the → *operating system producer*. The three best-known open

smart card operating systems are → *Multos*, → *Java Card* and → *Windows for Smart Cards*. Open smart card operating systems are usually → *interoperable*, rather than → *proprietary*. The term 'open platform' is also used to refer to an open smart card operating system, but it should not be confused with Open Platform (→ *OP*), which is an interface for managing applications in smart cards.

Operating system (OS)

An operating system encompasses all of the programs of a digital computer system that, in combination with the hardware features of the computer system, form the basis for its possible operational modes, in particular monitoring and controlling the execution of programs.[34]

Operating system producer

An entity that programs and tests an → *operating system*.

Optical memory card

A card in which information is 'burnt' into a reflective surface layer (similar to a CD).

OTA (over-the-air)

In → *GSM* and → *UMTS* systems, OTA refers to the possibility of establishing an → *end-to-end link* between the background system and the → *SIM* via the air interface between the base station and the mobile station. Such a link makes it possible to (for example) send a command directly and transparently from the background system to the SIM. OTA is also one of the foundations for all → *value-added services* in the SIM, since such services can also exchange data directly and transparently with higher-order systems via the air interface. The Short Message Service (→ *SMS*) is frequently used as the transport service (→ *bearer*) for OTA.

Package

Ag →*name space* in Java Card, and the smallest entity in the Java language. A package may have classes and interfaces.[35]

Packet-switched

With a packet-switched link, the sender partitions the data to be exchanged into packages, which are then transmitted individually to the recipient, possibly via separate paths. The recipient

[34] Based on the text of the German DIN 44 300 standard
[35] See also Section 5.14.1, 'Java Card'

then reassembles the packages to recover the original data. Charges for a packet-switched link usually depend on the amount of data exchanged, rather than the duration of the connection. Some typical examples of packet-switched links are X.25 and GPRS.

Padding

Extending a data string with filler data in order to bring it to a particular length. This is necessary if the length of the string must be an integral multiple of a certain block size (such as 8 bytes) to allow it to be further processed, for example by a cryptographic algorithm.

Page-oriented

A set of bytes in a memory that can only be written or erased as a group. In → *smart card microcontrollers*, only EEPROM and Flash EEPROM are page-oriented. Typical page sizes are 4, 32, 64 and 128 bytes. However, there are now microcontrollers with page sizes that are variable within a certain range, such as 1–128 bytes, instead of fixed.

Parallel data transmission

The concurrent transmission of several data bits (e.g. 8, 16 or 32) using a corresponding number of data lines. (→ *serial data transmission*)

Parity bit

Probably the best-known type of error detection code (EDC) is a parity bit appended to the byte to be protected. Before the parity bit can be calculated, it is necessary to specify whether even or odd parity is to be used. With even parity, the value of the parity bit is chosen such that the total number of bits with a value of 1 in the combined data byte and parity bit is an even number. With odd parity, the total number of bits with a value of 1 must be an odd number. With a single parity bit, one incorrect bit per byte can be reliably detected. However, it is not possible to correct a bit error, since the parity bit does not provide any information about the location of the altered bit.

Passivation

A protective layer on top of a semiconductor chip that screens it against oxidation and other chemical processes. The passivation layer must be partially or fully removed before the semiconductor can be physically manipulated.

Patch

In software development, a small program, sometimes written in machine code, that extends or alters the functionality of an existing program. Patches are commonly used to make quick,

simple corrections to program errors. They can be implemented either as → *work-arounds* or as → *bug fixes*.

Patent

A document granting an inventor the right to the exclusive exploitation of an invention for a limited period in one or more countries. The maximum term of a patent is usually 20 years.

Pay before

This expression refers to money flow for cards used in payment systems. With pay-before, the real money flows out of the cardholder's account before the goods or services are actually purchased. A typical example of a pay-before card is an → *electronic purse*, which the user must load with electronic money before making purchases. In the telecommunications sector, this form of payment is called → *prepaid*.

Pay later

This expression refers to money flow for cards used in payment systems. With pay later, the real money flows out of the cardholder's account only some time after the goods or services are actually purchased. A typical example of a pay-later card is a credit card, for which it may take up to several weeks after a purchase before the money is transferred from the account of the purchaser to the account of the merchant.

Pay now

This expression refers to money flow for cards used in payment systems. With pay now, the real money flows out of the cardholder's account at the same time as the goods or services are purchased. A typical example of a pay-now card is a debit card, such as the Eurocheque card, which allows the money to be transferred from the account of the purchaser to the account of the merchant at the time that the purchase is made.

PC/SC (Personal Computer/Smart Card) [PC/SC]

The PC/SC specification describes an interface for integrating smart cards into any desired application, independent of the platform and programming language used. The prerequisites are that a suitable driver must be available for the terminal used with the PC, and the smart card must be PC/SC-compatible. Version 1.0 of the 'Interoperability Specification for ICCs and Personal Computer Systems' was published in December 1997.[36]

[36] See also Section 11.4.1, 'PC/SC'

PCD (proximity coupling device)

A card terminal for communicating with a contactless card. (→ *PICC*)

Persistent

Attribute of an object that continues to exist after its run time (as opposed to a → *transient* object). A persistent object thus continues to exist after the end of a session, as well as after a sudden loss of power, without any loss of data or data inconsistency.

Personalizer

An entity that performs → *personalization*.

Personalization

The process of associating a card with a person. This can be done using physical personalization (e.g. embossing or laser engraving) as well as by electronic personalization (loading personal data in the memory of the smart card). The term 'individualization' would be a more exact description of this process, since it is not always necessary to enter personal data into the chip when electronic personalization is performed, for instance in the production of anonymous → *prepaid SIMs*.

Phase 1, Phase 2, Phase 2+

These phases mark the successive evolutionary stages in the development of the GSM system. In Phase 1, the basic services were realized (including speech transmission, call forwarding, → *roaming* and → *SMS*). In Phase 2, which began in 1966, the Phase 1 services were augmented by additional services, including conference calls, call handoff, calling number conveyance and GSM in the 1800-MHz band. In Phase 2+, these services were extended with the functions of the → *SIM Application Toolkit*, HSCSD (High-Speed Circuit-Switched Data) and → *GPRS*, among other things.

PICC (proximity integrated-circuit card)

A contactless smart card with a range of approximately 10 cm.

PIN (personal identification number)

A secret number, usually consisting of four digits, used for the → *identification* of a person. In the telecommunications world, the designation 'CHV' (cardholder value) is usually used for the PIN.

PIN pad

Originally, a data-entry keypad with special mechanical and cryptographic protection for use in a terminal. In general usage, the entire terminal is often called a PIN pad.

PKCS #1/2/. . . /15 (Public Key Cryptographic Standard Number 1/2/. . . /15)

Public-key cryptography specifications published by RSA Inc. that focus on the use of asymmetric cryptographic algorithms, such as the RSA algorithm.[37]

PKI (public key infrastructure)

All of the facilities and systems needed to exchange and manage data using asymmetric cryptographic protection, including a → *certification authority*, a → *registration authority*, a → *directory service* for blacklists (→ *certificate revocation list*), a time-stamp service (→ *time stamp*) and → *signature cards*.

PLMN (public land-mobile network)

Technical term for a terrestrial mobile telecommunications system.

Plug-in card

A small-format smart card as specified in GSM 11.11 and TS 102.221, primarily used in the mobile telecommunications sector. The official ISO designation for this format is 'ID000', in contrast to the larger ID-1 format (→ *ID-1 card*) used for common smart cards. A plug-in card has a length of ≈25 mm, a width of ≈15 mm and a thickness of ≈0.76 mm.[38]

Polling

Periodic program-driven querying of an input channel in order to detect an incoming message. Depending on the repetition rate of the queries, polling can require significant processing capacity, for which reason it is usually avoided in favor of hardware-supported querying using interrupts. An example of polling is in mobile telephones, where it is used in connnection with the → *SIM Application Toolkit* to allow the → *SIM* to send proactive commands (→ *proactivity*) to the mobile telephone.

POS (point of sale)

The location where a particular item or service is sold.

[37] See also Section 4.7.2, 'Asymmetric cryptographic algorithms'
[38] See also Section 3.1.1, 'Card formats'

Positive result

→ *good case*

Postpaid

Refers to money flow for cards used in the telecommunications sector in which the real money of the cardholder flows only after the service (usually a telephone call or data transmission) has been received. With regard to their payment function, postpaid cards are comparable to credit cards. In payment systems, this form of payment is called → *pay later*.

Power-on reset

→ *reset*

Pre-personalization

Another name for → *initialization*.

Prepaid

Refers to money flow for cards used in the telecommunications sector in which the real money of the cardholder flows before the service (usually a telephone call or data transmission) is received. With regard to their payment function, postpaid cards are comparable to electronic purses. In payment systems, this form of payment is called → *pay before*.

Prepaid SIM

A prepaid and usually reloadable SIM. All billing and reloading functions are usually provided by the background system, so they have no effect on data objects or functions in the SIM. The opposite of this is a → *postpaid* SIM.

Proactivity

A transaction mechanism for smart cards that allows a smart card to independently initiate actions in the terminal. This circumvents the rigid master–slave relationship between the terminal and the smart card. Proactivity is realized by cyclic polling of the smart card by the terminal, with the polling interval being configurable in advance by the smart card. Proactivity originated with SIMs, and it is still predominantly used to allow SIMS to effectively assume control of certain functions of the mobile telephone in accordance with GSM 11.14.

Probabilistic

Designates a process or an algorithm that yields varying results from identical input conditions; the opposite of → *deterministic*.

Procedural programming

A programming method based on formulating a program as a series of instructions for a → *microprocessor*. For purposes of simplification, the program flow can be broken down into functions, with the necessary data being held in variables. A key aspect of procedural programming is that it focuses on the processes of the program, rather than on the data to be processed as does object-oriented programming. Some typical programming languages used for procedural programming are Basic and C.

Process model

Another term for → *life-cycle model*.

Processor

→ *microprocessor*

Processor card

A short form of → *microprocessor card*.

Program code

Designation for a program that can be directly executed by an → *interpreter* or → *microprocessor*. (→ *native code*)

Proprietary

An adjective used in the smart card world, often in a deprecatory sense, to refer to a company-specific solution whose specifications are not fully public or belong to a single company. The opposite of a proprietary solution is an open solution, which can also be used by third parties. However, these terms are used in a far from unambiguous manner. Seen objectively, many 'open' smart card operating systems are rather proprietary and dependent on a single company. An example of a proprietary smart card → *application* would be an electronic purse system for use in a specific area that does not comply with relevant specifications and that has been developed by a particular company as a special solution.

Protection profile (PP)

In the context of an → *evaluation*, an implementation-independent set of security requirements (→ *security target*) adapted to particular application areas for specific → *targets of evaluation*.

Proton [Proton]

Brand name of an internationally used electronic purse system with approximately 50 million issued cards (as of spring 2002). The specifications for Proton also define a multiapplication → *smart card operating system*.

Prototype

A (software) prototype is an executable model of the ultimate product with restricted functionality. It is used to experimentally investigate specific properties of the ultimate product. A horizontal prototype implements only one or more specific layers of the software, while a vertical prototype implements a specific portion of the software across all of the layers.

Pseudonymization

The process of modifying person-specific data using an assignment rule such that it is afterwards not possible to associate the data with the original persons without knowing the assignment rule. The term is based on the fact that in the simplest case, the original name of each person is replaced by a unique pseudonym. A separate assignment table (the assignment rule) can be used to restore the links between the pseudonyms and the original names. (→ *anonymization*)

PSTN (public switched telephone network)

Designates the regular public wire-bound telephone network.

Public-key algorithm

→ *cryptographic algorithm*

PUK (personal unblocking key)

A special → *PIN* for resetting a PIN error counter that has reached its maximum value. A PUK is usually longer than a PIN (e.g., 8 digits), since users do not need the PUK unless they have forgotten the PIN, at which time they can search for it in their documents. If the PUK is successfully used, a new PIN is established at the same time, since the old PIN is evidently no longer known to the user.

Pull technology

Information transfer resulting from fetching information from a higher-level system (such as a server) by a lower-level system (such as a mobile telephone). The opposite to pull technology is → *push technology*.

Purse holder

A person possessing a → *smart card* containing an electronic purse.

Purse provider

The entity responsible for the overall functionality and security of an electronic purse system. This is usually the issuer of the electronic money for the cards. The purse provider normally also guarantees the redemption of the electronic money.

Purse-to-purse transaction

Transfer of electronic monetary units from one electronic purse directly to another, without intervention by a third, higher-level system. Normally, such capability requires the purse system to operate anonymously and the electronic purses to use a single common key for this function.

Push technology

Information transfer resulting from sending information from a higher-level system (such as a server) to a lower-level system (such as a mobile telephone). The opposite to push technology is → *pull technology*.

Quick

Brand name of an electronic purse system introduced throughout Austria in 1995. The essential components of the Quick system are based on EN 1546, which is the European standard for interoperable electronic purse systems.[39]

Radicchio [Radicchio]

An international initiative of companies and organizations for developing mobile → *e-commerce* solutions using the → *PKI*.

[39] See also Section 12.3.1, 'The CEN EN 1546 standard'

RAM (random-access memory)

A type of volatile memory, which is used in smart cards as working memory. RAM loses its content in the absence of power. SRAM and DRAM are types of RAM with special technical properties.[40]

Record

A record (data set) is a specific quantity of data, similar to a string.

Redlist

→*hotlist*

Registration authority (RA)

An entity in the → *PKI* that receives requests for certification from requesting parties and forwards them to the → *certification authority* after verifying the authenticity of the requesting parties. A registration authority is thus the entity that generates a unique assignment of certificates to persons.

Remote applet management

The management (creation, deletion etc.) of → *applets* in a smart card by a background system. For example, in various → *GSM* systems applets can be loaded into a SIM or deleted from a SIM via the air interface.

Remote file management

The management (creation, deletion, writing, reading, modification of access conditions etc.) of files in a smart card by a background system. For example, various → *GSM* systems allow new files to be created in a SIM and data to be written to these files, all via the air interface.

Reset

Restoring a computer (in this case, a smart card) to a clearly defined initial state. A cold reset, or power-on reset, is initiated by switching the supply voltage off and then on again. A warm reset is initiated by a signal on the reset lead of the smart card without altering the supply voltage.

[40] See also Section 3.4.2, 'Memory types'

Response

→*command*

Response APDU

A reply sent by a → *smart card* in response to a → *command APDU* received from a terminal (→ *command*). It consists of optional response data and a mandatory 1-byte portion containing status words SW1 and SW2 (→ *APDU*).[41]

Reticule

→*ROM mask*

Retry counter

→*error counter*

Roaming

Accessibility of a mobile telephone in a network other than its → *home net*.

Roll back

Functionality of an operating system for maintaining data consistency in the event of an error or abnormal termination. With roll-back functionality, the data used in an improperly executed or aborted operation are replaced by the original data. This process can be initiated automatically or on demand, and in smart card operating systems it is often implemented using → *atomic operations*. Another strategy for maintaining data consistency is → *roll-forward* functionality.

Roll forward

Functionality of an operating system for maintaining data consistency in the event of an error or abnormal termination. With roll-forward functionality, in the event of an improperly executed or aborted operation the data that are available but inconsistent are fed back into the operation in such a way that on completion, they are again consistent. This process can be initiated automatically or on demand, but it is rarely implemented in smart card operating systems due to their high security requirements. Another strategy for maintaining data consistency is → *roll-back* functionality.

[41] See Section 6.5, 'Message Structure: APDUs'

ROM (read-only memory)

A type of non-volatile memory, which is used in smart cards. It is mainly used to store programs and static data, since the content of a ROM cannot be altered.[42]

ROM mask

In ordinary language, this term is used in a highly context-specific manner. The original meaning of 'ROM mask' is an exposure mask used in semiconductor fabrication to produce the ROM. However, the term 'mask' is only used when the mask is not reduced in scale when exposing the → *wafer*. If the structures are reduced in scale for imaging onto the wafer, the mask is referred to as a 'reticule'.

The expression 'mask' is also used in connection with → *smart card microcontrollers* to refer to the data content of the ROM, and in some cases it is even synonymous with the entire → *smart card operating system* (→ *soft mask,*→ *hard mask*).

ROMed application

A smart card application that is not located in the EEPROM, but instead is permanently located in the mask-programmed ROM of the → *smart card microcontroller*.

Round-trip engineering

A software development method in which the design and implementation activities are performed concurrently so that they influence each other. The software architecture and program code are automatically kept mutually consistent using software. This process is based on a formal modeling language (such as UML), from which at least the basic body of the program is generated using automatic program code generation. The insights and improvements obtained by refining and testing this program code flow back into the modeling of the program via a reverse engineering process. It is possible to produce software based on 'practical experience' in a relatively short time, with source code that is consistent with the software architecture, by cycling through this code generation / reverse engineering loop several times. Round-trip engineering is almost exclusively used with object-oriented languages (e.g. C++ and Java) in combination with UML.

RSA (Rivest, Shamir, Adleman)

The best known and most widely used asymmetric cryptographic algorithm. It was published by Ronald L. Rivest, Adi Shamir and Leonard Adleman in 1978, and its name comes from the initial letters of the last names of its authors. Its very simple operating principle is based on the arithmetic of large integers.[43]

[42] See also Section 3.4.2, 'Memory types'
[43] See also Section 4.7.2, 'Asymmetric cryptographic algorithms'

R-UIM (removable user identity module)

The usual designation for a CDMA-specific smart card. It is an optional security module that can be present in removable form in a mobile telephone of the CDMA 2000 mobile telecommunication system. The functionality of the R-UIM is similar to that of the → *SIM*, although the CAVE (cellular authentication, voice privacy and encryption) cryptographic algorithm is used for a large number of cryptographically secured functions in the R-UIM. A UIM Application Toolkit (UATK) based on the SIM Application Toolkit is also specified for the R-UIM.

Rule-based programming

A programming method based on formulating general rules to be applied to the problems to be solved. A computer can then independently solve these problems by using the rules. A key aspect of rule-based programming is that it does not focus on processes, as does → *procedural programming*, or the data to be processed, as does → *object-oriented programming*, but only on general rules. Some typical rule-based programming languages are Lisp and Prolog.

Salt

A random sequence used to extend a password in order to hinder dictionary attacks on stored passwords.

SAM (secure application module)

→*security module*

Sandbox

→*virtual machine*

SCOPE (Smart Card Open Platform Environment)

Specification for a type of → *HAL* (hardware abstraction layer) for → *Global Platform*.

Scrambling

A jumbled arrangement of the address, data and control busses on a microcontroller chip, such that it is not possible to recognize the functions of individual bus lines without inside information. With static scrambling, the busses of a given series of chips are all scrambled in the same way, while with dynamic scrambling, the busses are scrambled differently for each individual chip or even each individual session.[44]

[44] See also Section 8.2.4.1, 'Attacks at the physical level'

Scratch card

A card in the usual → *ID-1* format but thinner than usual, with a secret number printed underneath an opaque cover layer that can be scratched off. This cover layer acts as a seal that allows the integrity of the card to be visually checked before it is used. The functional purpose of a scratch card is similar to that of a PIN letter. Scratch cards are often used as vouchers for distributing one-time passwords for reloading → *prepaid SIMs*.

Script

Any interpreted program that is primarily used to implement a simple, short application or automate a frequently repeated procedure.

SDMA (space division multiple access)

A multiple-access method for concurrently transferring data from several transmitters to a receiver using a single frequency. For this purpose, the transmitters use directionally selective aerials aimed at the receiver in question. Due to the high cost of this method, in mobile telecommunication systems it can only be used with base stations, for instance using array aerials (adaptive aerials).[45]

SECCOS (Security Card Operating System)

A multiapplication → *smart card operating system* used for German Eurocheque cards with chips and → *Geldkarte*.

Secret-key algorithm

→ *cryptographic algorithm*

Secure messaging

All methods, protocols and cryptographic algorithms used to protect → *smart card* data transmissions against manipulation and tapping.[46]

Security environment (SE)

In a smart card, a designation for a logical container holding a set of fully defined security measures used by → *commands* related to security or used for → *secure messaging*. Security environments are very suitable for items such as technical measures used to ensure the security of

[45] See also Section 13.1.1, 'Multiple-access methods'
[46] See also Section 6.6, 'Securing Data Transmission'

the various stages of the → *life cycle* of a smart card. In the simplest case different security environments would be defined for the personalization and subsequent use of the card, so that different file → *access conditions* would be specified for the different stages of the smart card life cycle. Write access would be allowed to all files for personalization, but for normal use the access conditions would be specified according to the actual → *application*.

Security module

A component that is secured both mechanically and computationally and is used to store secret data and execute cryptographic algorithms. It is also known as a secure application module (SAM), hardware security module (HSM) or host security module (HSM).

Security target

In the context of an → *evaluation*, security targets describe the mechanisms to be tested for the → *target of evaluation*. They thus represent a sort of requirements catalog for the evaluation. The security targets for specific types of targets of evaluation and specific application areas for targets of evaluation can be described using → *protection profiles*.

Seed number (seed)

A random number used as the initial value for a pseudorandom number generator.

Sequence control

A method for specifying a compulsory sequence of activities. For example, the correct sequence of → *commands* for mutual authentication of a → *smart card* and a background system can be enforced using sequence control in the smart card. This is done by specifying the states and state transitions of a state machine in the → *smart card operating system* that defines the command sequence that must be followed.[47]

Serial data transmission

A type of data transmission in which individual data bits are sent sequentially along a data line. (→ *parallel data transmission*)

Service provider

In a smart card system, an entity offering services that are used and paid for by a user. In the case of an electronic purse system, a service provider is an entity that receives money from the electronic purse of a purse holder in exchange for goods or services.

[47] See also Section 5.8, 'Sequence Control'

Session

The time between the activation and deactivation sequences of a smart card, during which both the complete data exchange and the necessary computational mechanisms occur.

SET (Secure Electronic Transaction Standard)

A financial transaction protocol for secure payment via the Internet using credit cards, published by Visa and MasterCard in 1966. SET doe not compel the payer to have a smart card, since it can be implemented fully in software on a PC. An extension of SET called Chip-SET (C-SET) is presently only used inside France and not yet internationally standardized.

Shall, should & may

These auxiliary verbs are often found in international standards. Their meanings in this context are precisely defined and differ in part from their lax usage in common speech. 'Shall' means that the item in question must be implemented in accordance with the description. 'Should', although it may appear to be a recommendation, actually means that the described item is to be provided or complied with if at all possible. Only 'may' provides a true opportunity for choice with regard to implementation.

Shared secrets

A principle according to which no single person knows everything about a particular system. The intentional distribution of knowledge avoids making individual persons subject to attack, as well as preventing individual persons from acquiring excessive power over a system due to their knowledge. Distributing knowledge over several persons is a commonly used technique in the development of security components.

Short FID (SFI)

A 5-bit identifier for an EF that can have a value of 1 through 31. It is used with a write or read command (such as READ BINARY) to implicitly select an EF in a smart card.[48]

Shrink

Refers to reducing the surface area of a semiconductor chip by using a semiconductor technology with a smaller structure width. A smaller chip surface area allows a larger number of chips to be placed on an individual wafer. This in turn reduces the cost of the individual semiconductor chips, since the chip price is approximately proportional to the amount of space occupied by the chip on the wafer.

[48] See also Section 5.6.2, 'File names'

Shutter

A mechanical device in a terminal that severs any wires leading out of the terminal from the card. This is intended to prevent manipulation of communications. If the wires cannot be cut, the inserted smart card will not be electrically activated.

Signal burst

A cohesive data packet transmitted between a base station and a mobile station via the air interface. Frequently simply referred to as a burst.

Signature Act

In general, a legislative act that governs the use of → *digital signatures*. In Germany, this is understood to mean the *Signaturgesetz (SigG)*, or in full the *Gesetz über Rahmenbedingungen für elektronische Signaturen* of 22 May 2001. This Act prescribes the general conditions for the use of digital signatures in Germany,[49] which are given more concrete form in the → *Signaturverordnung*.

Signature card

A →*smart card* with a →*microcontroller* whose principal function is to secure the storage and use of secret keys for →*digital signatures*.

Signaturgesetz (SigG)

The legislative act that governs the use of digital signatures in Germany (→*Signature Act*).

Signaturverordnung (*SigV*)

The German *Signaturverordnung* (Digital Signature Ordinance) of 1997,8 October, translates the general conditions prescribed by the → *Signaturgesetz* into concrete terms to the extent necessary to allow lists of specific measures to be generated as recommendations for the practical use of digital signatures. For example, the *Signaturverordnung* describes the necessary procedure for generating signature keys and identification data, as well as the necessary security concepts and the necessary testing stages for the signature components according to the ITSEC.[50]

[49] See also Section 14.4, 'Digital Signatures'
[50] See also Section 14.4, 'Digital Signatures'

SIM (subscriber identity module)

The usual designation for a GSM-specific smart card.[51] It is a mandatory security module that is present in mobile telephones in an exchangeable form. It may be the same size as a standard credit card (ID-1 format), or it may be a small plug-in card in the ID-000 format. The SIM bears the identity of the subscriber, and its primarily function is to secure the authenticity of the mobile station with respect to the network. Additional functions include executing programs with protection against manipulation (authentication), user identification (using a PIN) and storing data, such as telephone numbers. The equivalent of the SIM in the UMTS is the → *USIM*.[52]

SIM Alliance [SIM Alliance]

A consortium founded in 1999 by Gemplus, G + D, ORGA and Schlumberger in order to allow services developed for WAP to also be used with non-WAP-capable mobile telephones. For this purpose, the SIM must have a SIM-Alliance-capable browser and the mobile telephone must support GSM Phase 2+. This allows the → *SIM* to control the mobile telephone via the → *SIM Application Toolkit* to the extent that the majority of WAP contents and their functionality can be reproduced on the mobile telephone.[53]

SIM Application Toolkit (SAT; also STK (uncommon and outdated))

An extension to the GSM 11.11 specification, resembling a construction set and standardized in GSM 11.14, that allows the SIM to assume an active role in controlling the mobile telephone. For example, with the SIM Application Toolkit a SIM can output items to be shown on the display, request keypad entries and send and receive messages via the air interface. The SIM Application Toolkit forms the basis for most supplementary applications in mobile telephones. The equivalent of the SIM Application Toolkit for the UMTS is the → *USIM Application Toolkit* (USAT),[54] and for the → *R-UIM* the equivalent is the UIM Application Toolkit (UATK). The future generic foundation for all application toolkits for smart cards used in mobile telecommunications will be the Card Application Toolkit (CAT) defined by the → *EP SCP* expert group.

SIM Lock

A technique that firmly links a particular → *smart card* (a → *SIM*) to a particular mobile telephone. It involves either having the mobile telephone read certain data from the SIM and compare them with data stored in the mobile telephone, or having the SIM read unique data from the mobile telephone and compare them with stored data. If the data match, the mobile telephone can be used. It is generally possible to disable the SIM Lock function via the air

[51] See also Section 13.2, 'The GSM System'
[52] See also Section 13.3, 'The UMTS System'
[53] See also Section 13.5, 'The WIM'
[54] See also Section 13.3, 'The UMTS System'

interface or by entering a secret key using the keypad of the mobile telephone, in order to allow other smart cards to subsequently be used. The SIM Lock function is used to bind a mobile telephone subsidized by a network operator to a particular smart card and its payment mode (→ *prepaid*) for a certain length of time.[55]

SIM toolkit

Short for → *SIM Application Toolkit.*

SIMEG (Subscriber Identification Module Expert Group)

SIMEG was an expert group founded in 1988 that developed the specification for the interface between the smart card and the mobile telephone (GSM 11.11) under the authority of the → *ETSI*. In 1994, the name of the group was changed to → *SMG9*.

Simulator

Software that imitates the operation of a device (a target system). By contrast, an imitation using hardware is called an → *emulator*. Simulators are frequently used in developing software for target systems that do not yet exist. For instance, a smart card simulator consists of software that fully imitates a real smart card on the logical level. Simulators are generally slower than emulators, which means that they often cannot simulate the target system in real time.

Single sign-on (SSO)

A technique in which several different user identities for various applications are replaced by a single central user identity. This is realized using software that sends the corresponding identification names (→ *identification*) and passwords to the associated identification authorities on successful completion of central user identification. This avoids the need for the user to remember many different passwords.

Skimming

A typical type of attack on magnetic-stripe cards. It involves illicitly reading the magnetic-stripe data from a card not belonging to the attacker and copying it to the magnetic stripe of a blank card, which can then be used in the same way as the original card with respect to its magnetic stripe.

[55] See also Section 13.2, 'The GSM System'

Smart card

Strictly speaking, the term 'smart card' is an alternate name for a microprocessor card, in that it refers to a chip card that is 'smart'. Memory cards thus do not properly fall into the category of smart cards. However, the expression 'smart card' is generally used in English-speaking countries to refer to all types of cards containing chips.

Smart card application

→ *application*

Smart card microcontroller

A → *microcontroller* specifically optimized for the needs of smart cards. These optimizations primarily relate to chip security aspects (e.g., protective layers and detectors), chip size and special functional units for requirements specific to smart cards (such as a UART for communications).

Smart card operating system

Often also referred to as 'card operating system' (COS). A specialized form of → *operating system* tailored to the needs of smart cards, encompassing all programs in a → *smart card microcontroller* that allow smart card → *applications* to be used and managed. For this purpose, the data, files, → *commands*, processes, states, mechanisms, algorithms and programs needed by one or more programs must be supported in a suitable manner. If a smart card operating system allows several applications to be run concurrently, it is called 'multiapplication capable'. The trend in the development of smart card operating systems is toward → *open smart card operating systems*. Some typical examples of smart card operating systems are → *Multos*, → *Java Card*, → *Windows for Smart Cards* and → *STARCOS*.

Smart label

A data storage medium with a thin construction using contactless data transmission for communications. With the simplest versions, many of which do not contain chips, it is only possible to read data from the smart label. More sophisticated types of smart labels also allow data to be written to the label and/or processed in the label, similar to the functionality of a → *smart card*.

Smart object

A → *smart card microcontroller* packaged in a form other than the usual card. Some examples of smart objects are USB plugs and rings fitted with smart card microcontrollers.

Smartcard [Groupmark]

The term ‘Smartcard’ is a registered trademark of the Canadian company Groupmark.

SMG9 (Special Mobile Group 9)

SMG9 was an expert group operating under the authority of the → *ETSI* that developed specifications for the interface between the smart card and the mobile telephone (e.g. GSM 11.11, GSM 11.14 and so on). It was composed of representatives of card manufacturers, mobile telephone manufacturers and network operators. It was previously called → *SIMEG*. In 2000, SMG9 was dissolved and its tasks were divided between two new expert groups. The 3GPP T3 expert group is responsible for the application-specific interface between the mobile telephone and the → *SIM* or → *USIM*, while the ETSI Smart Card Platform (EP SCP) expert group deals with all generic topics in the area of smart cards used in the telecommunications sector.

SMS (short message service)

A GMS service for sending short messages having a maximum length of 160 alphanumeric characters. SMS messages are sent via the signaling channel instead of the data channel, which means that they can also be sent and received during an active telephone conversation. SMS is used not only for conveying short messages for subscribers, but also as a → *bearer* service for transmitting data to the mobile telephone (e.g., → *WAP*) or the SIM (→ *OTA*).

Soft mask

The term ‘soft mask’ means that part of the program code of the → *smart card operating system* is located in EEPROM and built on top of the code stored in ROM. Routines stored in EEPROM can be easily modified by overwriting, which means that they are ‘soft’. The term ‘mask’ in this case is actually not correct, since it is not necessary to produce a semiconductor exposure mask for program code stored in EEPROM. Soft masks are typically not used for large quantities of cards, rapid → *prototyping* or extensions, but instead for applications such as field trials. The opposite of a soft mask is a → *hard mask*, which means that all of the essential functions are stored in the ROM.

Software specification

An unambiguous, complete and non-redundant description of a software item. Its content must not include anything subject to interpretation, and it must be comprehensible to all reader groups having various functions (developers, testers, QA officers etc.) within an acceptable length of time.

SPA (simple power analysis)

A method for attacking smart cards that involves measuring the current consumption of a microcontroller with high time resolution. Conclusions about the internal processes and the data processed within the microcontroller can be drawn from its current consumption. SPA was made known in June 1998 in a publication by Paul Kocher, Joshua Jaffe und Benjamin Jun [Kocher 98] (→ *DPA*).[56]

SPA/DPA-resistant

Property of a cryptographic algorithm that does not allow the secret key being used to be determined using → *SPA* or → *DPA*.

Specification

In this book, and generally speaking, the term *specification* is used to refer to any document that resembles a standard but is generated or issued by (for example) a company or an industrial group, rather than by a national or international standards authority. (→ *standard*)

SRAM (static random-access memory)

A static RAM needs a constant supply of power to retain its contents, but it does not have to be periodically refreshed like DRAM. The access time of SRAM is less than that of DRAM, but SRAM occupies more space on the chip and is thus more expensive.[57]

Stack

A data structure in which the most recently entered data object is the first to be retrieved (last in, first out – LIFO). Probably the best-known stack is the program stack, which is used to hold return addresses when subroutines are called.

Standard

A document containing technical descriptions and/or precise criteria used as rules and/or definitions of characteristics and features in order to ensure that materials, products, processes and services can be used for their intended purposes. In this book, the term 'standard' is consistently used in connection with a national or international standards authority (such as ISO, CEN, ANSI or ETSI).

[56] See also Section 8.2.4.1, 'Attacks at the physical level'
[57] See also Section 3.4.2, 'Memory types'

STARCOS

Brand name of a multiapplication → *smart card operating system* from Gieseke & Devrient [GD], available in various versions since 1991.

State machine

A part of a program that specifies a sequence of events by means of a predefined state diagram, which consists of specific states and state transitions.

Steganography

The objective of steganography is to conceal messages within other messages such that they cannot be perceived by a naïve observer (man or machine). For example, a text could be encoded and hidden in an image file in such a way that it only marginally modifies the image, so the changes to the image are practically invisible (→ *digital watermark*). With a suitable analysis program, the text message (such as a copyright text) hidden in the image file can subsequently be reconstructed and again made visible.

Super smart card

A smart card with integrated complex card elements, such as a display or keypad.

Symmetric cryptographic algorithm

→ *cryptographic algorithm*

Synchronous data transmission

A form of data transmission in which data transmission depends on a predefined timing reference. This timing reference may for example be derived from the clock signal applied to the chip. (→ *asynchronous data transmission*)

System on card

In the smart card realm, a designation for a smart card containing supplementary card components in addition to the chip module. Commonly used supplementary components include displays, power sources (batteries and solar cells), keypads, aerials, sensors for biometric user identification (e.g., fingerprint readers) and loudspeakers. These card components can be driven from within the chip in the module, but this is not mandatory. Another designation for such cards is ‘super smart card’, although this is used less often.

T = 0

A transmission protocol governing data transmission between a terminal and smart card. The T = 0 protocol was the first internationally standardized transmission protocol for smart cards. It is a byte-oriented half-duplex protocol that operates asynchronously and is designed for minimum memory usage and maximum simplicity. It is used internationally for GSM cards, and is thus the most widely used of all smart card protocols. The T = 0 protocol is specified in the ISO/IEC 7816-3 standard. Compatible specifications are present in GSM 11.11, TS 102.221 and the EMV specification documents.

T = 1

A transmission protocol governing data transmission between a terminal and smart card. It is a block-oriented half-duplex protocol that operates asynchronously and provides separation between the data transport and application layers. The T = 1 protocol is specified in the ISO/IEC 7816-3 standard. Compatible specifications are present in TS 102.221 and the EMV specification documents.

T3

→*SMG9*

Tag

Identifier for a data object, primarily used in ASN.1 coding.[58]

Tape out

The time at which the chip design is completed and the resulting design data are passed to mask generation (→ *ROM mask*). This is an important milestone in chip production. The term comes from the fact that the mask data were formerly output to magnetic tape.

Target of evaluation (TOE)

The IT system to be evaluated (→ *evaluation*), or in other words, the object under test. For example, a TOE could be a microcontroller smart card (→ *smart card microcontroller*) with integrated software that must meet certain → *security targets*.

TCSEC (Trusted Computer System Evaluation Criteria)

A catalog of criteria for the development and → *evaluation* of the security of information technology systems in the US, published in 1983 by the National Computer Security Center

[58] See also Section 4.1, 'Structuring Data'

(→ *NCSC*). The successor to the national TCSEC is the internationally applicable → *Common Criteria*.

TD/CDMA (time division / code division multiple access)

→*CDMA*

TDES

→*triple DES*

TDMA (time division multiple access)

A multiple-access method for the quasi-concurrent transfer of data from multiple transmitters to a receiver using a single frequency. For this purpose, each transmitter is allocated a particular time slot for its exclusive use, which requires very precise synchronization. TDMA is used together with FDMA in GSM systems for the air interface between mobile telephones and base stations.[59]

Terminal

The counterpart to a smart card. A device, possibly having a keypad and display, that provides electrical power to the smart card and enables it to exchange data. The official ISO designation for a smart card terminal is 'interface device' (IFD), while in the financial transaction realm the usual designation for a terminal is 'card accepting device' (CAD).

Test

Development stage in which an already debugged program is methodically tested for proper functionality and compliance with the requirements established in the → *analysis* stage. The primary objective is not searching for errors in the program, but instead verifying the required functions. Testing is thus not the same as → *debugging*.

TETRA (Terrestrial Trunked Radio; previously Trans-European Trunked Radio)

Specification for a digital trunked radio system operating in the 380–420-MHz band using → *TDMA*, published by ETSI. Like → *GMS*, TETRA envisages the use of a → *SIM*, usually called a TETRA SIM, for subscriber identification. However, the TETRA SIM is optional and thus can be implemented in the form of software in the mobile station.

[59] See also Section 13.1.1, 'Multiple-access methods'

TETRA SIM

→*TETRA*

Thread

→*multithreading*

Time stamp

An attestation generated by an agency and bearing the digital signature of that agency, to the effect that certain digital data were present at this agency at a particular time.

TLV format

Commonly used expression for → *BER*-coded data objects conforming to → *ASN.1*, in which a prefixed label (tag) and length parameter (length) are used to uniquely describe a data item (value).

TPDU

→*APDU*

Transaction

A set of related → *commands* sent sequentially to a smart card in order to perform a specific task. A typical example of a transaction is the sequence of commands used to load an electronic purse.

Transaction number (TAN)

In contrast to a PIN, a TAN is valid for only one transaction, which means it can be used only once. The user typically receives several TANs printed on a slip of paper (as a list of five-digit numbers, for example), and these numbers must be used exactly in the prescribed order for individual transactions or sessions.

Transfer card

A → *smart card* used as a transport medium to exchange data between two entities. It has a large data memory and usually contains authentication keys for verifying whether the data to be transferred are allowed to be read or written by the entity in question.

Transient

Property of an object that exists only during the run time of a process; the opposite of → *persistent*.

Transmission protocol

In the smart card world, 'transmission protocol' refers to the mechanisms used for transmitting and receiving data between a terminal and a smart card. A transmission protocol describes in detail the OSI protocol layers used, data exchange in the good case, error detection mechanisms and response mechanisms in the event of errors.[60]

Transport protocol

An alternate and less commonly used name for → *transmission protocol*.

Trap door

A mechanism or algorithm intentionally included in software that can be used to bypass security functions or protective mechanisms.

Triple-band mobile telephone

A mobile telephone that can work in three frequency bands (e.g., GSM 900, GSM 1800 and GSM 1900).

Triple DES

Also known as TDES and 3 DES; a modified form of DES encryption consisting of invoking the DES algorithm three times in succession with alternating encryption and decryption. If the same key is used for all three DES invocations, triple-DES encryption corresponds to normal DES encryption. However, if two or three different keys are used, triple DES encryption is significantly stronger than single DES encryption.[61]

Trivial PIN

A → *PIN* that is easily guessed, such as "1234" (→ *0-PIN*).

[60] See also Chapter 6, 'Smart Card Data Transmission'
[61] See also Section 4.7.1, 'Symmetric cryptographic algorithms'

Trojan horse

Historically, the wooden horse that allowed Odysseus to gain entry to the strongly fortified city of Troy. In modern usage, a program that performs a specific 'foreground' task, but which can also perform other functions unknown to the user. A Trojan horse is introduced purposely into a computer system or host program. In contrast to a virus, it cannot reproduce itself.

Trust center (TC)

Besides the → *signature card*, the essential component of a → *PKI*. A trust center is the entity that generates, distributes and administers certificates. Depending on its constitution, it thus provides the functions of a → *certification authority*, a → *registration authority*, a → *verification service* and/or a → *time stamp* service.

Trusted third party (TTP)

A party recognized by two or more other parties as trustworthy, which may for example issue → *certificates*.

Tunneling

A technique for establishing a cryptographically secured end-to-end link between two parties using the communications paths of one or more other parties that do not modify the information content of the actual data exchange.

UART (universal asynchronous receiver/transmitter)

A general-purpose component operating independently of a → *microprocessor* to asynchronously transmit and receive data. When a UART is used, it is not necessary for the microprocessor to handle communications at the bit and byte level. This leads to a simplification of the communications protocol, and it can also result in higher data transmission rates than what can be realized by the microprocessor using a pure software solution.[62]

UCS (Universal Character Set)

An extension of the ASCII and Unicode encodings of character sets, specified in the ISO/IEC 10 646 international standard. UCS uses 32 bits for character encoding, although only half of the available address space is used ($2^{32}/2 = 2{,}147{,}483{,}648$). This address space is sufficient to represent all characters of all of the languages in the world. UCS is defined such that → *Unicode* forms a subset of UCS, and the encoding of the first 128 characters corresponds to the ASCII encoding.[63]

[62] See also Section 3.4.3, 'Supplementary hardware'
[63] See also Chapter 4.2, 'Coding Alphanumeric Data'

UICC (universal integrated chip card)

A smart card having a → *smart card operating system* in accordance with ISO/IEC 7816 that is optimized for telecommunications applications. The UICC is based on the TS 102.221 standard, which is published by → *ETSI*. The UICC forms the basis for the → *USIM*. It may have the usual credit-card dimensions or be made as a small plug-in card in ID000 format.

UIM (user identity module)

An outdated term for → *USIM*.

UML (Unified Modeling Language) [OMG]

A graphically oriented, method-independent modeling language for abstractly describing the static and dynamic aspects of object-oriented programs. The current version of UML is 1.3. The foundations of the semantics and notation of UML were created in the 1990s by Grady Booch, James Rumbaugh und Ivar Jacobson. UML is independent of any particular → *life-cycle model* for software development.[64] The Object Management Group (OMG) is responsible for the ongoing development of UML.

UMTS (Universal Mobile Telecommunication System)

The European successor to GSM and a member of the → *ITM-2000* family. UMTS is a third-generation (→ 3*G*) digital, cellular, interoperable, transnational land-based mobile telecommunication system. The frequency band allocated to this mobile telecommunication system lies at 2000 MHz. The UMTS system is defined by a number of specifications generated under the auspices of the → *3GPP* and published by → *ETSI*. UMTS represents the next major evolutionary step for → *GSM*. The essential changes with respect to GSM are a new air interface using → *CDMA* technology and a significantly higher data transmission rate of up to 2 Mbit/s.[65]

Unicode [Unicode]

An extension of the well-known ASCII character code. In contrast to the 7-bit ASCII code, Unicode employs 16 bits for coding. This allows the characters of the most widely used languages of the world to be supported. The first 256 Unicode characters are identical to the ISO 8859-1 ASCII characters.[66]

[64] See also Section 15.7, 'Life-Cycle Models'
[65] See also Section 13.3, 'The UMTS System'
[66] See also Section 4.2, 'Coding Alphanumeric Data'

Uplink

A connection from a lower-level system (such as a mobile telephone) to a higher-level system (such as a base station); the opposite of → *downlink*.

Upload

Transferring data from a lower-level system (such as a terminal) to a higher-level system (such as a background system or host system); the opposite of → *download*.

URL (uniform resource locator)

A unique alphanumeric address in the → *WWW*.

User

A person who uses a → *smart card*; not necessarily the same as the → *cardholder*.

User data

All data directly needed by an → *application*.

USIM (universal subscriber identity module)

The common name of the smart card → *application* for UMTS,[67] which resides in a → *UICC*. However, in practice the term 'USIM' is also used to refer to the UMTS smart card as well as the application, although this is not entirely correct. The USIM bears the identity of the subscriber, and its primary function is to secure the authenticity of the mobile station with respect to the network and vice versa. Additional functions include executing programs with protection against manipulation (authentication), user identification (using a PIN) and storing data, such as the telephone numbers. The USIM is based on the TS 31.102 standard published by → *ETSI*. The equivalent of the USIM in the → *GSM* system is the → *SIM*.[68]

USIM Application Toolkit (USAT)

A collection of functions standardized by TS 31.111 that allow a USIM card to assume an active role in controlling a mobile telephone. For example, a USIM can use the USIM Application Toolkit to output items to be shown on the display, request inputs from the keypad and transmit or receive messages via the air interface. The USIM Application Toolkit forms the basis for most

[67] See also Section 13.3, 'The UMTS System'
[68] See also Section 13.2.4, 'The SIM'

supplementary applications in mobile telephones. The equivalent of the USIM Application Toolkit in GSM is the → *SIM Application Toolkit* (SAT).[69]

Value-added service (VAS)

A supplementary smart card → *application* present in a smart card in addition to the main application. Such services usually presuppose a → *multiapplication smart card*.

Vertical prototype

→ *prototype*

Virgin card

A card that has not yet been implanted with a chip or visually or electronically personalized. A virgin card is essentially a printed, non-specific → *card body*, as used in the mass production of cards.

Virtual machine (VM)

A software simulation of a → *microprocessor*, usually having its own opcodes for machine instructions as well as a simulated address space. It allows software to be generated that is independent of the features of specific hardware. For instance, the virtual address space of a VM can be many times larger than the address space provided by the hardware. In the Java environment, the closed environment of the VM is often called the sandbox.[70]

Virtual merchant card

→ *virtual smart card*

Virtual smart card

A software simulation of a smart card in a different system, such as in a security module or a mobile telephone. A virtual merchant card, which is the simulation of a smart card in a merchant terminal, is a special case of a virtual smart card.

Visa Cash

Visa brand name for several technically different electronic purse systems using smart cards.

[69] See also Section 13.2.4, 'The SIM'
[70] See also Section 5.14.1, 'Java Card'

Visa Easy Entry (VEE)

A method for easy migration from magnetic-stripe credit cards to credit cards with microcontroller chips. This is accomplished by storing the name of the cardholder and all of the data on the magnetic stripe in an EF under a DF that is reserved for Visa. When a payment is made using the credit card, the terminal reads the data needed for the transaction from the chip instead of from the magnetic stripe. The advantage of this approach is that it is only necessary to upgrade the POS terminals to include smart card contact units, while the entire background system can be used as before without any modifications.

Volatile memory

A type of memory (e.g. RAM) that retains its contents only as long as power is applied.

VOP

→ *OP*

Wafer

A thin disc of silicon on which chips are built using semiconductor fabrication techniques. Wafers typically have a diameter of 150 mm (6 inches), 200 mm (8 inches) or 300 mm (12 inches).

WAP (wireless application protocol)

A term used to refer to a number of specifications for creating a link between a mobile terminal (mobile telephone, PDA etc.) and a server via a wireless network, for the purpose of directly exchanging data. The usual application for WAP is implementing Internet services in mobile telephones in a manner that is largely independent of the mobile telecommunications standard used. Incidentally, the designation 'wireless application protocol' refers not only to the technology, but also to the protocol used between the terminal and the background system. The WAP Forum, founded in June 1997 by Phone.com, Ericsson, Motorola and Nokia, is the internationally active standards committee for WAP. It is composed of representatives of more than 350 companies.[71]

WAP Forum

→ *WAP*

[71] See also Section 13.5, 'The WIM'

Warm reset

→*reset*

WCDMA (wideband code division multiple access)

→*CDMA*

Whitelist

A list in a database indicating all smart cards and devices allowed to be used in a particular → *application.* (→ *blacklist,* → *graylist,* →*hotlist)*

White plastic

Refers to non-personalized blank cards used with fraudulent intent. The term originally comes from the typical blank cards made from white plastic that are used to produce test cards. However, it is now understood to also refer to cards that have been printed and have a wide variety of → *card components*, such as credit cards with magnetic stripes and holograms that have not yet been embossed.

Whitebox test

A test, also often also called a glassbox test, in which it is assumed that the party performing the test has complete knowledge of all of the internal processes and data of the software to be tested.

WIM (WAP identity module)

A security module for a → *WAP* terminal. The specification describes a PCKS #15-compatible smart-card → *application*. The principal functions of a WIM are generating and verifying digital signatures and encrypting data. A WIM may be either a separate, physical smart card or one of several applications in a multiapplication smart card. It is typically an application in a → *SIM* or → *USIM*.

Windows for Smart Cards [Microsoft]

An → *open smart card operating system* from Microsoft, also known as WfSC and WSC, that supports multiple → *applications* (→ *multiapplication smart card*) and downloadable programs. One of the special features of Windows for smart cards is that it uses a → *FAT*-based file system.[72]

[72] See also Section 5.7, 'File Management'

WML (wireless markup language)

A logical markup language based on XML used to generate applications for WAP. WML is very similar to HTML. WML applications stored in a WML site on a WAP server are translated on-the-fly into compact WML bytecode, which is transmitted via the wireless network to a the mobile terminal, where it is interpreted by a microbrowser (→ *browser*).

Work-around

In the context of software development, circumventing a known problem by 'programming around' it. A work-around avoids the negative effects of an error on the rest of the program, but it does not eliminate the actual error. For example, work-arounds in EEPROM are typically used to correct errors in ROM-based → *smart card operating systems* that are found after the chips have been produced, in order to prevent such errors from having negative effects on the operation of the operating system. However, it is entirely possible for the functionality of the operating system to be reduced relative to its original scope as a consequence of using work-arounds.

WWW, W3 (World-Wide Web)

A part of the international Internet, primarily characterized by its ability to link any desired documents using hyperlinks and the integration of multimedia objects into documents.

X.509

The X.509 standard published by the → *ITU* defines the structure and coding of → *certificates*. It is the most widely used standard for certificate structures (→ *PKI*) throughout the world.

XML (extended markup language)

A logical markup language that is both a successor to and an extension of HTML. XML can be used to define new language elements, which means that other markup languages, such as HTML and WML, can be defined using XML. XML is a subset of the powerful 'standard generalized markup language' (SGML), which is specified by an ISO standard.

ZKA (*Zentraler Kreditausschuss*)

The coordinating body for the electronic payment transactions of the German banks. The ZKA is composed of the following banking associations: the *Deutsche Sparkassen- und Giroverband* (DSGV), the *Bundesverband der Deutschen Volks- und Raiffeisenbanken* (BVR), the *Bundesverband deutscher Banken* (BdB) and the *Verbund öffentlicher Banken* (VÖB). The chairmanship of the ZKA is assumed by each of the four member associations in yearly rotation.

16.2 RELATED READING

The *Smart Card Handbook* focuses on smart cards and their applications. However, there are a large number of other disciplines that strongly affect smart cards and their further development, each of which has its own particular areas of interest and specialist literature. The authors of the *Smart Card Handbook* wish to maintain the focus of this book within its own field, rather than providing extensive descriptions of related disciplines, since that would vastly exceed the scope of this book. For readers who wish to increase their knowledge of these related subjects, we have prepared the following short list of related reading.

Subject	**Reference**
Operating systems	[Tanenbaum 02]
Smart card manufacturing	[Haghiri 02]
Java as a programming language	[Arnold 00]
Cryoptography	[Menezes 97], [Schneier 96]
RFID	[Finkenzeller 02]
Security of components and systems	[Anderson 01]
Software development	[Balzert 98]
Software development for Java Card	[Chen 00]

16.3 LITERATURE

The following publications are sorted first by the last name of the author and then in ascending order of publication date. 'Internet' is listed as the source of publications that appeared in newsgroups or discussion forums on the Internet.

[Anderson 01] Ross J. Anderson: *Security Engineering*, Wiley, Chichester 2001

[Anderson 92] Ross J. Anderson: *Automatic Teller Machines*, Internet, December 1992

[Anderson 96a] Ross J. Anderson, Markus G. Kuhn: *Improved Differential Fault Analysis*, Internet, November 1996

[Anderson 96b] Ross J. Anderson, Markus G. Kuhn: *Tamper Resistance – a Cautionary Note*, USENIX Workshop, November 1996

[Arnold 00] Ken Arnold, James Gosling, David Holmes: *The Java Programming Language*, 3rd edn, Addison Wesley, Boston 2000

[Balzert 98] Helmut Balzert: *Lehrbuch der Software-Technik*, Vol.2, 2nd edn, Spektrum Akademischer Verlag, Heidelberg 1998

[Bellare 95a] Mihir Bellare, Juan Garay, Ralf Hause, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner: *iKP – A Family of Secure Electronic Payment Protocols*, Internet, 1995

[Bellare 95b] Mihir Bellare, Philip Rogaway: *Optimal Asymmetric Encryption – How to Encrypt with RSA*, Internet, 1995

[Bellare 96] Mihir Bellare, Philip Rogaway: *The Exact Security of Digital Signatures – How to Sign with RSA and Rabin*, Internet, 1996

[Beutelsbacher 93] Albrecht Beutelsbacher: *Kryptologie*, 3rd edn, Vieweg Verlag, Braunschweig 1993

[Beutelsbacher 96] Albrecht Beutelsbacher, Jörg Schwenk, Klaus-Dieter Wolfenstetter: *Moderne Verfahren der Kryptografie*, Vieweg Verlag, Braunschweig 1996

[Biham 91] Eli Biham, Adi Shamir: *Differential Cryptoanalysis of DES-like Cryptosystems*, Journal of Cryptology, Vol. 4, No. 1, 1991

[Biham 93] Eli Biham, Adi Shamir: *Differential Cryptoanalysis of the Data Encryption Standard*, Springer-Verlag, New York 1993

[Biham 96] Eli Biham, Adi Shamir: *A New Cryptoanalytic Attack on DES*, Internet, 1996

[BIS 96] Bank for International Settlements: *Security of Electronic Money – Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries*, Basel, August 1996

[Blumtritt 97] Oskar Blumtritt: *Nachrichtentechnik*, 2nd edn, Munich, Deutsches Museum, 1997

[Boehm 81] Barry W. Boehm: *Software Engineering Economics*, Prentice Hall, Upper Saddle River, New Jersey 1981

[Boneh 96] Dan Boneh, Richard A. DeMillo, Richard J. Lipton: *On the Importance of Checking Computations*, Math and Cryptography Research Group, Bellcore 1996

[Bronstein 96] I. N. Bronstein, K. A. Semendjajew: *Taschenbuch der Mathematik*, 7th edn, B. G. Teubner Verlagsgesellschaft, Leipzig 1997

[Buchmann 96] Johannes Buchmann: *Faktorisierung großer Zahlen*, Spektrum der Wissenschaft, September 1996

[Chen 00] Zhiqun Chen: *Java Card Technology for Smart Cards*, Addison Wesley, Boston 2000

[CMM 93] Mark C. Paulk, Bill Curtis, Mary Beth Chrissis, Charles V. Weber: *Capability Maturity Model for Software, Version 1.1*, Software Engineering Institute, Pittsburg 1993

[Dhem 96] J. F. Dhem, D. Veithen, J.-J. Quisquater: *SCALPS: Smart Card Applied to Limited Payment Systems*, UCL Crypto Group Technical Report Series, Université Catholique de Louvain, 1996

[Dictionary of Computing 91] *Dictionary of Computing*, Oxford University Press, Oxford 1991

[Diffie 76] Whitfield Diffie, Martin E. Hellman: *New Directions in Cryptography*, Internet, 1976

[Dröschel 99] Wolfgang Dröschel, Manuela Wiemers: *Das V- Modell 97*, Oldenbourg Verlag, Munich 1999

[Eberspächer 97] Jörg Eberspächer, Hans-Jörg Vögel: *GSM – Global System for Mobile Communication*, B. G. Teubner Verlag, Stuttgart 1997

[EFF 98] Electronic Frontier Foundation: *Frequently Asked Questions (FAQ) about the Electronic Frontier Foundation's "DES Cracker" Machine*, Internet, 1998

[EC 91] Commission of the European Communities: *Information Technology Security Evaluation Criteria (ITSEC)*, Version 1.2, June 1991

[EC 98] Council of the European Communities: *Council Regulation (EC) No 2135 of 24 September 1998 Amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/85 and (EEC) No 3821/85*, Version 1.2, June 1991

[Fenton 96] Norman E. Fenton, Shari Lawrence Pfleeger: *Software Metrics*, Thomson Computer Press, London 1996

[Finkenzeller 02] Klaus Finkenzeller: *RFID-Handbuch*, 3rd edn, Carl Hanser Verlag, Munich/Vienna 2002

[Franz 98] Michael Franz: *Java – Anmerkungen eines Wirth-Schülers*, Informatik Spektrum, Springer-Verlag, Berlin 1998

[Freeman 97] Adam Freemann, Darrel Ince: *Active Java – Object Oriented Programming for the World Wide Web*, Addison-Wesley, Reading, MA 1997

[Fumy 94] Walter Fumy, Hans Peter Ries: *Kryptographie*, 2nd edn, R. Oldenbourg Verlag, Munich/Vienna 1994

[Gentz 97] Wolfgang Gentz: *Die elektronische Geldbörse in Deutschland*, Diplomarbeit an der Fachhochschule München, Munich 1997

[Glade 95] Albert Glade, Helmut Reimer, Bruno Struif: *Digitale Signatur*, Vieweg Verlag, Braunschweig 1995

[Gora 98] Walter Gora: *ASN.1 – Abstract Syntax Notation One*, 3rd edn, Fossil Verlag, Köln 1998

[Gosling 95] James Gosling, Henry McGilton: *The Java Language Environment – A White Paper*, Sun Microsystems, USA 1995

[Grün 96] Herbert Grün: *Card Manufacturing Materials and Environmental Responsibility*, Presentation at CardTech/SecurTech, Atlanta, GA, May 1996

[GSM 95] Proceedings of the Seminar for Latin America Decision Makers by GSM MoU Association and ECTEL: *Personal Communication Services based on the GSM Standard*, Buenos Aires 1995

[Guthery 02] Scott B. Guthery, Mary J. Cronin: *Mobile Application Development with SMS and the SIM Toolkit*, McGraw-Hill, New York 2002

[Gutmann 96] Peter Gutmann: *Secure Deletion of Data from Magnetic and Solid-State Memory*, USENIX Conferenz, San Jose, CA 1996

[Gutmann 98a] Peter Gutmann: *Software Generation of Practically Strong Random Numbers*, Internet, 1998

[Gutmann 98b] Peter Gutmann: *X.509 Style Guide*, Internet, 1998

[Haghiri 02] Yahya Haghiri, Thomas Tarantino: *Smart Card Manufacturing: A Practical Guide*, Wiley, Chichester 2002

[Hassler 02] Vesna Hassler, Martin Manninger, Mikhail Gordeev, Christoph Muller: *Java Card for E-Payment Applications*, Artech House, London 2002

[Hellmann 79] Martin E. Hellmann: *The Mathematics of Public-Key Cryptography*, Scientific American, August 1979

[Hillebrand 2002] Friedhelm Hillebrand (editor): *GSM and UMTS*, Wiley, Chichester 2002

[IC Protection 97] *Common Criteria for IT Security Evaluation Protection Profile – Smartcard Integrated Circuit Protection Profile*, Internet, 1997

[Isselhorst 97] Hartmut Isselhorst: *Betreiberorientierte Sichrheitsanforderungen für Chipkarten-Anwendungen*, Card-Forum, Lüneburg 1997

[Jones 91]. C. Jones: *Applied Software Measurement*, McGraw-Hill, New York 1991

[Jun 99] Benjamin Jun, Paul Kocher: *The Intel Random Number Generator*, Internet, 1999

[Kaliski 93] Burton S. Kaliski Jr.: *A Layman's Guide to a Subset of ASN.1, BER and DER*, RSA Laboratories Technical Note, Internet, 1993

[Kaliski 96] Burton S. Kaliski Jr.: *Timing Attacks on Cryptosystems*, RSA Laboratories, Redwood City, CA 1996

[Karten 97] Zeitschrift Karten: *Zur Sicherheit der ec-Karte PIN: Das Urteil des OLG Hamm*, Fritz Knapp Verlag, Frankfurt, August 1997

[Knuth 97] Donald Ervin Knuth: *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd edn, Addison-Wesley/Longman, Reading, MA 1997

[Kocher 95] Paul C. Kocher: *Timing Attacks on Implementations of Diffie-Hellmann, RSA, DSS, and Other Systems*, Internet, 1995

[Kocher 98 a] Paul C. Kocher, Joshua Jaffe, Benjamin Jun: *Introduction to Differential Power Analysis and Related Attacks*, Internet, 1998

[Kocher 98b] Paul C. Kocher, Joshua Jaffe, Benjamin Jun: *Differential Power Analysis: Leaking Secrets*, Internet, 1998

[Kömmerling 99] Oliver Kömmerling, Markus G. Kuhn, *Design Principles for Tamper-Resistant Smartcard Processors*, USENIX Workshop on Smartcard Technology, Chicago, USA, 10–11 May 1999

[Kuhn 97] Markus G. Kuhn: *Probability Theory for Pickpockets – ec-PIN Guessing*, COAST Laboratory, Purdue University, West Lafayette, Indiana 1997

[Kuhn] Markus G. Kuhn: *Attacks on Pay-TV Access Control Systems*, University of Cambridge, Internet, year unknown

[Lamla 00] Michael Lamla: *Hardware Attacks on Smart Cards – Overview*, Eurosmart Security Conference, Marseille, 13–15 June 2000

[Leiberich 99] Otto Leiberich: *Vom diplomatischen Code zur Falltürfunktion*, Spektrum der Wissenschaft, June 1999

[Lender 96] Friedwart Lender: *Production, Personalisation and Mailing of Smart Cards – A Survey*, Smart Card Technologies and Applications Workshop, Berlin, November 1996

[Levy 99] Steven Levy: *The Open Secret*, Wired, April 1999

[Lindholm 97] Tim Lindholm, Frank Yellin: *The Java Virtual Machine Specification*, 2nd edn, Addison-Wesley, Reading, MA 1999

[Massey 88] James L. Massey: *An Introduction to Contemporary Cryptology*, Proceedings of the IEEE, Vol. 76, No. 5, May 1988, pp 533–549

[Massey 97] James L. Massey: *Cryptography, Fundamentals and Applications*, 1997

[Meister 95] Giesela Meister, Eric Johnson: *Schlüsselmanagement und Sicherheitsprotokolle gemäß ISO/SC 27 – Standards in Smart Card-Umgebungen,* in: Albert Glade, Helmut Reimer, Bruno Struif: *Digitale Signatur*, Vieweg Verlag, Braunschweig 1995

[Menezes 93] Alfred J. Menezes: *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishing, Boston, MA 1993

[Menezes 97] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL 1997

[Merkle 81] Ralph C. Merkle, Martin E. Hellman: *On the Security of Multiple Encryption*, Internet, 1981

[Messerges 99] Thomas S. Messerges, Ezzy A. Dabbish, Robert H. Sloan: *Investigations of Power Analysis Attacks on Smartcards*, USENIX Workshop on Smartcard Technology, Chicago, USA, 10–11 May 1999

[Meyer 82] Carl H. Meyer, Stephen M. Matyas: *Cryptography*, Wiley, New York 1982

[Meyer 96] Carsten Meyer: *Nur Peanuts – Der Risikofaktor Magnetkarte*, c't, July 1996

[Montenegro 99] Sergio Montenegro: *Sichere und fehlertolerante Steuerungen*, Carl Hanser Verlag, Munich/Vienna 1999

[Moore 02] Simon Moore, Ross Anderson, Paul Cunningham, Robert Mullins, George Tayler: *Improving Smart Card Security using Self-timed Circuits*, Internet, May 2002

[Müller-Maguhn 97a] Andy Müller-Maguhn: *"Sicherheit" von EC-Karten,* Die Datenschleuder, Ausgabe 53, 1997

[Müller-Maguhn 97b] Andy Müller-Maguhn: *EC-Karten Unsicherheit*, Die Datenschleuder, Ausgabe 59, 1997

[Myers 95] Glenford J. Myers: *The Art of Software Testing*, 5th edn, Wiley, New York 1995

[Nebelung 96] Brigitte Nebelung: *Das Geldbörsen-Konzept der ec-Karte mit Chip*, debis Systemhaus, Bonn 1996

[Nechvatal 00] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback, NIST: *Report on the Development of the Advanced Encryption Standard (AES)*, Internet, 2000

[Odlyzko 95] Andrew. M. Odlyzko: *The Future of Integer Factorization*, AT&T Bell Laboratories, 1995

[Otto 82] Siegfried Otto: *Echt oder falsch? Die maschinelle Echtheitserkennung*, Betriebswirtschaftliche Blätter, Heft 2, February 1982

[Peyret 97] Patrice Peyret: *Which Smart Card Technologies will you need to Ride the Information Highway Safely?*, Gemplus, 1997

[Pfaffenberger 97] Bryan Pfaffenberger: *Dictionary of Computer Terms*, Simon & Schuster/Macmillan, New York 1997

[Piller 96] Ernst Piller: *Die "ideale" Geldbörse für Europa*, Card-Forum, Lüneburg 1996

[Pomerance 84] C. Pomerance: *The Quadratic Sieve Factoring Algorithm*, Advances in Cryptology – Eurocrypt 84

[Press 92] William H. Press, Saul A. Teukolsky, William T. Vetterling, Brian P. Flannery: *Numerical Recipes in C – The Art of Scientific Computing*, 2nd edn, Cambridge University Press, Cambridge 1992

[Rivest 78] Ronald L. Rivest, Adi Shamir, Leonard Adleman: *Method for Obtaining Digital Signatures and Public-Key Cryptosystems,* Internet, 1976

[Robertson 96] James Robertson, Suzanne Robertson: V*ollständige Systemanalyse*, Carl Hanser Verlag, Munich/Vienna 1996

[Rother 98a] Stefan Rother: *Prüfung von Chipkarten-Sicherheit,* Card-Forum, Lüneburg 1998

[Rother 98b] Stefan Rother: *Prüfung von Chipkarten-Sicherheit,* in *Tagungsband Chipkarten,* Vieweg Verlag, Braunschweig 1998

[RSA 97] RSA Data Security Inc.: *DES Crack Fact Sheet*, Internet, 1997

[Scherzer 00] Helmut Scherzer: *Chipkarten-Betriebssysteme – Gefahrenpotentiale und Sicherheitsmechanismen*, Forum IT-Sicherheit Smartcards, 14 March 2000

[Schief 87] Rudolf Schief: *Einführung in die Mikroprozessoren und Mikrocomputer*, 10th edn, Attempto Verlag, Tübingen 1987

[Schindler 97] Werner Schindler: *Wie sicher ist die PIN?*, speech presented at the 'Kreditkartenkriminalität'conference, Heppenheim, October 1997

[Schlumberger 97] Schlumberger: *Cyberflex – Programmers Guide*, Version 6d, April 1997

[Schneier 96] Bruce Schneier: *Applied Cryptography*, 2nd edn, Wiley, New York 1996

[Schneier 99] Bruce Schneier: *Attack Trees – Modeling Security Threats*, Dr. Dobb's Journal, December 1999

[Sedgewick 97] Robert Sedgewick: *Algorithmen*, 3rd edn, Addison-Wesley, Bonn/München/Reading, MA 1997

[SigG 01] Gesetz über Rahmenbedingungen für elektronische Signaturen, 22 May 2001

[Silverman 97] Robert D. Silverman: *Fast Generation of Random, Strong RSA Primes*, RSA Laboratories Crypto Byte, Internet, 1997

[Simmons 92] Gustavus J. Simmons (editor): *Contemporary Cryptology*, IEEE Press, New York 1992

[Simmons 93] Gustavus J. Simmons: *The Subliminal Channels in the U.S. Digital Signature Algorithm*, Proceedings of Symposium on the State and Progress of Research in Cryptography, Rome 1993

[Skorobogatov 02] Sergei Skorobogatov, Ross Anderson: *Optical Fault Induction Attacks*, Internet, May 2002

[Sommerville 90] Ian Sommerville: *Software Engineering*, Addison-Wesley, Wokingham 1990

[Steele 01] Raymond Steele, Chin-Chun Lee, Peter Gould:*GSM, cdmaOne and 3G Systems*, Wiley, Chichester 2001

[Stix 96] Gary Stix: *Herausforderung "Komma eins"*, Spektrum der Wissenschaft, February 1996

[Stocker 98] Thomas Stocker: *Java for Smart Cards,* in: *Tagungsband Smart Cards,* Vieweg Verlag, Braunschweig 1998

[Tanenbaum 02] Andrew S. Tanenbaum: *Moderne Betriebssysteme*, 3rd edn, Addison-Wesley Longman, Reading, MA 2002

[Thaller 93] Georg Erwin Thaller: *Qualitätsoptimierung der Software-Entwicklung. Das Capability Maturity Model (CMM)*, Vieweg Verlag, Braunschweig 1993

[Tietze 93] Ulrich Tietze, Christoph Schenk: *Halbleiter-Schaltungstechnik*, 10th edn, Springer-Verlag, Berlin 1993

[Vedder 97] Klaus Vedder, Franz Weikmann: *Smart Cards – Requirements, Properties and Applications*, ESAT-COSIC course, Catholic University of Leuven, 1997

[Walke 00] Bernhard Walke: *Mobilfunknetze und ihre Protokolle, Band 2: Bündelfunk, schnurlose Telefonsysteme, W-ATM, HIPERLAN, Satellitenfunk, UPT*, B. G. Teubner Verlag, Stuttgart 2000

[Weikmann 92] Franz Weikmann: *SmartCard-Chips – Technik und weitere Perspektiven*, Der GMD-Spiegel 1'92, Gesellschaft for Mathematik und Datenverarbeitung, Sankt Augustin 1992

[Weikmann 98] Franz Weikmann, Klaus Vedder: *Smart Cards Requirements, Properties and Applications*, in: *Tagungsband Smart Cards*, Vieweg Verlag, Braunschweig 1998

[Wiener 93] Michael J. Wiener: *Efficient DES Key Search*, Crypto 93, Santa Barbara, CA 1993

[Yellin 96] Frank Yellin: *Low Level Security in Java*, Internet, 1996

[Zieschang 98] Thilo Zieschang: *Differentielle Fehleranalyse und Sicherheit von Chipkarten*, Internet, 1998

16.4 ANNOTATED DIRECTORY OF STANDARDS AND SPECIFICATIONS

This section contains an extensively commented directory of international standards, industry standards and specifications relevant to cards with and without chips. This directory primarily focuses on international standards, rather than local, country-specific standards. It lists standards produced by official standards organizations (such ANSI, CEN, ETSI and ISO), as well as quasi-standards that are relevant to smart cards, such as the EMV specification and Internet RFCs.

In addition to the annotated directory, Table 16.1 provides a summary of potentially helpful compilations, summaries and sources of standards and specifications related to specific subjects. Industry standards in particular are often available free of charge on the WWW. Unfortunately, this is not generally the case with official standards published by standards organizations.

Table 16.1 Summary of the most important Web servers for downloading standards and information related to smart cards

Standards or specification organization	Web server	Remarks
ANSI	[ANSI]	—
CEN	[CEN]	—
DIN	[DIN]	—
EMV	[EMVCO]	The specification can be downloaded from the Web server free of charge.
ETSI	[ETSI]	All ESTI standards (including those for GSM and UMTS) can be downloaded from the Web server free of charge.
FIPS	[NIST]	All FIPS standards can be downloaded from the Web server free of charge.
Global Platform	[Global Platform]	The specification can be downloaded from the Web server free of charge.
IEEE	[IEEE]	—
ISO/IEC	[ISO]	—
ITU	[ITU]	—
Java Card Forum	[JCF]	The specification can be downloaded from the Web server free of charge.
RFC	[RFC]	The specification can be downloaded from the Web server free of charge.
RSA Inc.	[RSA]	The specification can be downloaded from the Web server free of charge.
SEIS	[SEIS]	The specification can be downloaded from the Web server free of charge.

All standards and specifications are listed below in order of the name of the issuing organization and the numerical designation, ignoring prefixes (such as 'pr') and status indications (such as 'DIS'). The date listed is the date at which the currently valid version first appeared. The most important standards for smart cards are marked with a '◆'.

A few brief remarks are in order regarding the naming of individual standards. First, extensions to ISO and ISO/IEC standards are usually contained in an amendment (Amd.). Each time a standard is revised, which normally takes place every five years, any amendments are incorporated into the main body of the standard as necessary. The title of a revised version of a standard thus differs from the title of its predecessor only by the year number and the sequential version number. New versions of CEN standards are identified in a similar manner. In the case of FIPS standards, the number of the revised edition forms part of the name of the standard (e.g., FIPS 140–2). Telecommunications standards from ETSI use a three-digit version number to distinguish different versions. In the case of industry standards, the revision level is indicated by a year number or a version number, depending on the publisher.

ANSI X9.8	Banking – Personal Identification Number Management and Security
– 1: 1995	Part 1: PIN Protection Principles and Techniques
– 2: 1995	Part 2: Approved Algorithms for PIN Encipherment
ANSI X 9.9: 1986	Financial Institution Message Authentication
ANSI X 9.17: 1985	Financial Institution Key Management
ANSI X 9.19: 1996	Financial Institution Retail Message Authentication
ANSI X 9.30	Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry
– 1: 1997	Part 1: The Digital Signature Algorithm (DSA)
– 2: 1997	Part 2: The Secure Hash Algorithm (SHA-1)
ANSI X 9.31: 1998	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry
ANSI X9.55: 1997	Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists
ANSI X9.84: 2001	Biometric Information Management and Security *This very comprehensive standard specifies the basic architectural principles of a wide variety of biometric identification methods, as well as the requirements for the use, management and security of biometric data.*
ANSI X 3.92: 1981	Data Encryption Algorithm *Describes the DES algorithm.*

ANSI X 3.106: 1983	American National Standard for Information Systems – Data Encryption Algorithm – Modes of Operation
ANSI / IEEE 829: 1991	Standard for Software Test Documentation *Describes the methods and necessary documentation for testing software.*
ANSI / IEEE 1008: 1987	Standard for Software Unit Testing *Describes basic methods for testing software.*
ANSI / IEEE 1012: 1992	Software Verification and Validation Plans *Specifies the necessary test activities and test plans for software development. This standard is based on the waterfall model for software development.*
CCITT Z.100: 1993	CCITT Specification and Description Language (SDL)
CEPS, Version 2.1.3: 2001	Joint Specification for Common Electronic Purse Cards *CEPS is an important standard for electronic purses and is based on EN 1546. It provides the foundation for the majority of present and future European purse systems.*
Common Criteria, Version 2.1: 1999	*Identical to ISO/IEC 15 408* (*q.v.*)
DIN 9781-10: 1985	Büro- und Datentechnik; Identifikationskarten aus Kunststoff oder kunststofflaminiertem Werkstoff; Anforderungen an Echtheitsmerkmale *This very short standard defines the terms used in the context of authenticity features and lists general requirements for such features.*
DIN 44 300 – 1 . . . 9: 1988	Informationsverarbeitung – Begriffe *Defines many information technology concepts.*
EMV 2000	Integrated Circuit Card Specification for Payment Systems ◆ *This is the most important family of standards for smart cards used in payment systems. It is jointly published by EMVCo [EMV]. The family consists of four parts, called 'books', which deal with smart cards, associated debit and credit payment applications and related terminals.*[73]

[73] See also Section 12.4, 'The EMV Application'

Book 1 Version 4.0: 2000	Application Independent ICC to Terminal Interface Requirements *This part contains the specifications for the mechanical and electrical properties of the smart cards and terminals, including definitions of the activation and deactivation sequences, data transmission at the electrical level, the ATR and its associated parameters. In addition, it specifies the $T = 0$ and $T = 1$ transmission protocols, the APDU structure, logical channels and several fundamental card commands and application selection mechanisms.*
Book 2 Version 4.0: 2000	Security and Key Management *This part describes static and dynamic data authentication, PIN encryption and secure messaging. It also contains general conditions for managing the public keys of a payment system and requirements for terminal security, including associated key management.*
Book 3 Version 4.0: 2000	Application Specification *This part of the EMV specification defines a number of commands needed for smart cards and smart card applications for debit and credit cards and specifies transaction procedures. The appendix includes descriptions of all of the data objects, including their coding, specifications for the TLV coding of data and general approaches to integrating EMV smart cards into SET-based payment systems.*
Book 4 Version 4.0: 2000	Cardholder, Attendant and Acquirer Interface Requirements *Book 4 lists the mandatory and optional requirements for terminals that support EMV-compliant smart cards. This includes conceivable configurations, functional and security requirements for terminals, possible and permitted user messages including the character set used, and the interface to the acquirer. This standard also defines the basic features of the architecture of the terminal software and a model of a terminal-resident interpreter for executable program code. The appendix contains a listing of data objects relevant to the terminal and*

	recommendations for the technical design of the terminal, as well as examples of point-of-sale, cash dispenser and goods dispenser terminals.
EN 726	Identification Card Systems – Telecommunications Integrated Circuit(s) Card and Terminals *Up until the mid-1990s, this family of standards occupied a leading position with regard to describing the functionality of smart card operating systems. However, it has now been completely supplanted by the ISO/IEC 7816 family of standards, the UICC standards and the EMV specifications, and is thus no longer significant.*
– 1: 1994	Part 1: System Overview
– 2: 1995	Part 2: Security Framework
– 3: 1994	Part 3: Application Independent Card Requirements ◆ *Defines file structures, commands, return codes and files for general-purpose applications, as well as basic mechanisms for smart cards for telecommunications applications. This standard is the ETSI counterpart of ISO/IEC 7816-4 and the corresponding framework for GSM 11.11.*
– 4: 1994	Part 4: Application Independent Card Related Terminal Requirements
– 5: 1999	Part 5: Payment Methods *Defines various payment methods and associated file structures, data elements and processes for smart cards. The payment methods are intended to be used for telecommunication applications.*
– 6: 1995	Part 6: Telecommunication Features
– 7: 1999	Part 7: Security Module
EN 753	Identification Card Systems – Intersector Thin Flexible Cards
– 1: 1997	Part 1: General Technical Specifications
– 2: 1997	Part 2: Magnetic Recording Technique
– 3: 1999	Part 3: Test Methods
EN 1038: 1995	Identification Card Systems – Telecommunication Applications – Integrated Circuit(s) Card Payphone *Defines basic considerations for using smart cards with public card phones. This standard primarily contains references to previous standards, and it*

	identifies the various places in the system where a security module can be effectively used to authenticate a phone card.
prEN 1105: 1995	Identification Card systems – General concepts applying to systems using IC cards in intersector environments – Rules for Inter-application Consistency *Defines the basic demands placed on a smart card in order to ensure interapplication use. It primarily contains references to prior standards, as well as various regulations for smart cards and terminals.*
prEN 1292: 1995	Additional Test Methods for IC Cards and Interface Devices *Defines tests for the general electrical parameters of smart cards and terminals and the basic data transfer between smart cards and terminals. This standard is an extension to ISO/IEC 10 373.*
EN 1332	Identification Card Systems – Man–Machine Interface
– 1: 1999	Part 1: Design Principles and Symbols for the User Interface
– 2: 1998	Part 2: Definition of a Tactile Identifier for ID-1 cards *Specifies a perceptible recess in ID-1 cards for detecting the orientation of the card.*
– 3: 1999	Part 3: Keypads
– 4: 1999	Part 4: Coding of User Requirements for People with Special Needs
EN 1362: 1997	Identification Card Systems – Device Interface Characteristics – Classes of Device Interfaces
EN 1387: 1996	Machine Readable Cards – Health Care Applications – Cards: General Characteristics
EN 1545-1: 1998	Identification Card Systems – Surface Transport Applications – Part 1: General
EN 1545-2: 1998	Identification Card Systems – Surface Transport Applications – Part 2: Transport Payment
prEN 1545-3: 1995	Identification Card Systems – Surface Transport Applications – Part 3: Tachograph

prEN 1545-4: 1995	Identification Card Systems – Surface Transport Applications – Part 4: Vehicle and Driver Licencing
EN 1546	Identification Card Systems – Inter-sector Electronic Purse
	◆ *The internationally most important standard for electronic purses, which forms the foundation for most purse systems. This family of standards has been kept relatively general, so it includes many options, but it is a very good and complete description of an electronic purse.*
– 1: 1999	Part 1: Definition, Concepts and Structures
	Defines terms used in the entire family of standards and describes the basic concepts and structures of intersector electronic purse systems.
– 2: 1999	Part 2: Security Architecture
	Describes the notation used for security mechanisms, the security architecture and associated procedures and mechanisms for intersector electronic purse systems.
– 3: 1999	Part 3: Data Elements and Interchanges
	Describes the data elements, files, commands and return codes used by all components of an intersector electronic purse system.
– 4: 1999	Part 4: Data Objects
	Describes the TLV mechanism for reading arbitrary data objects from files, and also provides a detailed presentation of the components and states of a state machine for a intersector electronic purse system. Also includes a list of tags for all data objects used.
EN 1867: 1997	Machine-readable Cards – Health Care Applications – Numbering System and Registration Procedure for Issuer Identifiers
EN 13 343	Identification Card Systems – Telecommunications IC Cards and Terminals – Test Methods and Conformance Testing for EN 726-3
– 1 prEN: 1998	Part 1: Implementation Conformance Statement (ICS) Pro-forma Specification
– 2 prEN: 1998	Part 2: Test Suite Structure and Test Purposes (TSS & TP)

– 3 prEN: 1998	Part 3: Abstract Test Suite (ATS) and Implementation Extra Information for Testing (IXIT) Pro-forma Specification
EN 13 344	Identification Card Systems – Telecommunications IC Cards and Terminals – Test Methods and Conformance Testing for EN 726-4
– 1 prEN: 1998	Part 1: Implementation Conformance Statement (ICS) Pro-forma Specification
– 2 prEN: 1998	Part 2: Test Suite Structure (TSS) and Test Purposes (TP)
– 3 prEN: 1998	Part 3: Abstract Test Suite (ATS) and Implementation Extra Information for Testing (IXIT) Pro-forma Specification
EN 13 345	Identification Card Systems – Telecommunications IC Cards and Terminals – Test Methods and Conformance Testing for EN 726-7
– 1 prEN: 1998	Part 1: Implementation Conformance Statement (ICS) pro-forma Specification
– 2 prEN: 1998	Part 2: Test Suite Structure and Test Purposes (TSS & TP)
– 3 prEN: 1998	Part 3: Abstract Test Suite (ATS) and Implementation extra Information for Testing (IXIT) pro-forma Specification
EN 1750: 1999	Identification Card Systems – Intersector Messages between Devices and Hosts – Acceptor to Acquirer Messages
EN 300812, Version 2.1.1: 2001	Terrestrial Trunked Radio (TETRA); Security Aspects; Subscriber Identity Module to Mobile Equipment (SIMME) Interface
ENV 1257	Identification Card Systems – Rules for Personal Identification Number Handling in Intersector Environments *Illustrates and explains security aspects related to using PINs, from transfering the PIN to the cardholder (PIN letter) to entering the PIN using a keypad (PIN pad).*
– 1 prENV: 1997	Part 1: PIN Presentation
– 2 prENV: 1997	Part 2: PIN Protection
– 3 prENV: 1997	Part 3: PIN Verification

ENV 13 729: 2000	Health Informatics – Secure User Identification – Strong Authentication using Microprocessor Cards
ETS 300 331: 1995	Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM) *Describes the smart card (DAM) for the DECT system. Includes all associated commands, files, access conditions and authentication methods. Also defines the dimensions of the mini-ID and plug-in card formats. This standard is strongly based on the GSM 11.11 specification.*
FIPS 46-3: 1999	Data Encryption Standard (DES) ◆ *Describes the DES and triple-DES algorithms.*
FIPS 74: 1981	Guidelines for Implementing and Using the NBS Encryption Standard
FIPS 81: 1980	DES Modes of Operation
FIPS 140-2: 2001	Security Requirements for Cryptographic Modules ◆ *A fundamental, internationally used standard with regard to security requirements for security modules, which includes smart cards. It defines four different security levels for security modules and describes in detail seven security-related requirement areas. The content of this standard is very practically oriented and also addresses technical implementation details, such as criteria for the quality of random number generators.*
FIPS 180-1: 1995	Secure Hash Standard (SHA-1) ◆ *Describes the SHA-1 hash function.*
FIPS 186-2: 2000	Digital Signature Standard (DSS) ◆ *Describes the DSS algorithm.*
FIPS 197: 2001	Advanced Encryption Standard (AES) ◆ *Describes the AES algorithm.*
GSM 01.02, Version 6.0.1: 2001	Digital Cellular Telecommunications System (Phase 2+) (GSM); General Description of a GSM Public Land Mobile Network (PLMN) *Forms the basis for the architecture of all GSM mobile telecommunications networks.*
GSM 01.04, Version 8.0.0: 1999	Digital Cellular Telecommunications Systems (Phase 2) (GSM); Abbreviations and Acronyms

GSM 01.60, Version 6.0.0: 1998	Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS) Requirements Specification of GPRS
GSM 02.09, Version 7.0.1: 1998	Digital Cellular Telecommunications Systems (Phase 2) (GSM); Security Aspects
GSM 02.17, Version 8.0.0: 1999	Digital Cellular Telecommunications Systems (Phase 2) (GSM); SIM Functional Characteristics *A short standard specifying the basic functionality required of a security module (SIM) for a GSM mobile telecommunications network. It is the GSM equivalent of the TS 21.111 standard for UMTS.*
GSM 02.19, Version 7.1.0: 1998	Digital Cellular Telecommunications System (Phase 2+) (GSM); Subscriber Identity Module Application Programming Interface (SIM API); Service Description; Stage 1 *A short standard listing all of the basic services of a language-independent API for executable program code (e.g., Java) in the SIM. Based on this standard, GSM 03.19 provides a detailed specification of a specific implementation to provide a Java Card API for SIMs.*
GSM 02.22, Version 7.0.0: 1999	Digital Cellular Telecommunications System (Phase 2+) (GSM); Personalization of GSM Mobile Equipment (ME); Mobile Functionality Specification *Describes mechanisms for personalizing and depersonalizing mobile equipment using specific data in the SIM (commonly known as SIM Lock).*
GSM 02.34, Version 6.0.0: 1997	Digital Cellular Telecommunications System (Phase 2+); High Speed Circuit Switched Data (HSCSD); Stage 1
GSM 02.48, Version 8.0.0: 2000	Digital Cellular Telecommunications System (Phase 2+) (GSM); Security Mechanisms for the SIM Application Toolkit; Stage 1 *A short standard describing the basic application-independent security mechanisms used with the SIM Application Toolkit as defined in GSM 11.14. Based on this standard, GSM 03.48 provides a detailed implementation specification.*
GSM 02.60, Version 6.3.0: 1997	Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 1

GSM 03.19, Version 8.2.0: 2001	Digital Cellular Telecommunications System (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card; Stage 2 ◆ *Specifies a Java Card variant for use as a SIM with the SIM Application Toolkit, based on the Java Card 2.1 specifications. This standard is the key document for using Java Card in GSM. The basis for this is provided by GSM 02.19.*
GSM 03.20, Version 8.1.0: 1999	Global System for Mobile Communication (GSM) (Phase 2+); Security Related Network Functions
GSM 03.38, Version 7.2.0: 1999	Digital Cellular Telecommunications System (Phase 2+) (GSM); Alphabets and Language-specific Information *Specifies a GSM character set based on ASCII.*
GSM 03.40, Version 7.4.0: 2000	Digital Cellular Telecommunications System (Phase 2+) (GSM); Technical realization of the Short Message Service (SMS)
GSM 03.48, Version 8.7.0: 2001	Digital Cellular Telecommunications System (Phase 2+); Security Mechanisms for the SIM Application Toolkit; Stage 2 ◆ *Contains specifications for all security mechanisms needed for a connection between the background system and the SIM that is secure against eavesdropping and manipulation. Also describes the basic mechanism of a remote file management system using the SIM. The basis for this document is provided by GSM 02.48.*
GSM 09.91: 1995	European Digital Cellular Telecommunications System (Phase 2); Interworking Aspects of the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface between Phase 1 and Phase 2
GSM 11.10 Version 8.2.0: 2000	Digital Cellular Telecommunications System (Phase 2+) (GSM) – Mobile Station (MS) Conformance Specification *A very comprehensive test specification for GSM mobile stations.*
GSM 11.11 Version 8.5.0: 2001	Digital Cellular Telecommunications System (Phase 2+) – Specification of the Subscriber

	Identity Module – Mobile Equipment (SIM – ME) Interface ◆ *Specifies the physical and logical properties of the SIM by means of a description of the interface between the SIM and the GSM mobile telephone. Defines the dimensions of ID-1 and plug-in cards and the general mechanical parameters of the card and the contacts. Specifies general electrical parameters and the the structures and contents of the ATR and PPS. Also defines the possible data structures, security mechanisms, commands and return codes. Lists all data elements and files necessary for a SIM, along with typical command sequences. This standard is the GSM equivalent of the TS 31.101 and TS 31.102 UMTS standards.*
GSM 11.12 Version 4.3.1: 1998	Digital Cellular Telecommunications System (Phase 2); Specification of the 3 Volt Subscriber Identity Module – Mobile Equipment (SIM–ME) Interface *Specifies 3-V SIMs, including a compatibility list for SIMs programmed according to previous specifications. It only includes differences and extensions relative to GSM 11.11 with regard to 3V SIMs.*
GSM 11.13 Version 7.2.0: 2000	Digital Cellular Telecommunications System (Phase 2+); Test Specification for SIM API for Java Card *Specifies the test environment, test applications, test procedures, test coverage and individual test cases for the SIM API for Java Card as specified in GSM 03.19. The described tests exclusively address the IT aspects of a Java Card SIM for GSM. This standard provides an excellent and comprehensive illustration of how tests for a Java card can be described, constructed and executed.*
GSM 11.14 Version 8.8.0: 2001	Digital Cellular Telecommunications System (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface *Defines and extensively describes the SIM Application Toolkit (SAT) for SIMs. SAT describes an interface between the mobile telephone and the SIM for the partial control of the mobile*

	telephone by SIM-resident supplementary applications. This standard introduces proactive commands for the SIM and defines many new commands related to controlling the mobile telephone, such as display output, keypad polling and sending short messages. The UMTS equivalent of this standard is TS 31.111.
GSM 11.17 Version 7.0.2: 1998	Digital Cellular Telecommunications System (Phase 2+) (GSM); Subscriber Identity Module (SIM) Conformance Test Specification *Specifies the test environment, test equipment, test hierarchy and individual test cases for testing SIMs. The described tests exclusively address the electrical and IT aspects. Tests covering these aspects are specified in detail, including electrical power, data transmission, file management, commands and typical processes used in the GSM application. This specification is a very good and extensive illustration of how GSM tests can be described, constructed and executed. The UMTS equivalent of this standard is TS 31.122.*
GSM 11.18 Version 7.0.1: 1998	Digital Cellular Telecommunications System (Phase 2 +); Specification of the 1.8 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface
GSM 11.19 Version 7.0.3: 1998	Digital Cellular Telecommunications System (Phase 2+) (GSM) – Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile
IEEE 828: 1990	Standard for Software Configuration Management Plans
IEEE 1363: 2000	Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography ◆ *A very extensive and comprehensive standard, which addresses almost all aspects of asymmetric cryptographic algorithms, including generating keys, using digital signatures, key exchange and encryption.*
ISO 639	Codes for the Representation of Names of Languages
– 1: 2001	Part 1: Alpha-2 Code
– 2: 1998	Part 2: Alpha-3 Code

ISO/IEC 646: 1991	Information Technology – ISO 7-bit Coded Character Set for Information Interchange
ISO 3166	Codes for the Representation of Names of Countries and their Subdivisions
– 1: 1997	Part 1: Country Codes
– 2: 1998	Part 2: Country Subdivision Code
– 3: 1999	Part 3: Code for Formerly Used Names of Countries
ISO/IEC 4217: 1995	Codes for the Representation of Currencies and Funds
ISO 4909: 2000	Bank Cards – Magnetic Stripe Data Contents for Track 3
ISO/IEC 7501	Identification Cards – Machine Readable Travel Documents
– 1: 1997	Part 1: Machine Readable Passport
– 2: 1997	Part 2: Machine Readable Visas
– 3: 1997	Part 3: Official Travel Documents
ISO 7810: 1995	Identification Cards – Physical Characteristics *Describes the most important physical properties of cards without chips, and defines the ID-1, ID-2 and ID-3 card formats.*
ISO 7811	Identification Cards – Recording Technique *This family of standards is an important reference for the mechanical aspects of cards. It specifies the mechanical implementation of the essential card components.*
– 1: 1995	Part 1: Embossing *An exact definition of the 10 numeric characters and the basic method used to emboss cards.*
– 2: 2001	Part 2: Magnetic Stripe – Low Coercivity *Defines the size and position of the magnetic stripe on the card. Also specifies the physical properties of the magnetic material and the coding of the characters on the magnetic stripe.*
– 3: 1995	Part 3: Location of Embossed Characters on ID-1 Cards *Defines the possible locations for embossing on ID-1 cards.*

– 4: 1995	Part 4: Location of Read-only Magnetic Tracks – Tracks 1 and 2 *Defines the positions of the read-only tracks (tracks 1 and 2) on an ID-1card.*
– 5: 1995	Part 5: Location of Read–Write Magnetic Track – Track 3 *Defines the position of the read/write track (track 3) on an ID-1card.*
– 6: 2001	Part 6: Magnetic Stripe – High Coercivity
– 7 WD: 2001	Part 7: Magnetic Stripe – High Coercivity High Density
ISO 7812	Identification Cards
– 1: 2000	Part 1: Numbering System *Specifies a numbering scheme for manufacturers of ID cards.*
– 2: 2000	Part 2: Application and Registration Procedures *Defines the registration authority and a form for registering applications. Also contains an algorithm for generating a Luhn checksum (modulo-10 checksum).*
ISO 7813: 1995	Identification Cards – Financial Transaction Cards *Defines the basic physical properties, dimensions and embossing of ISO 7810-compliant ID-1 cards for use in the financial transaction field. Also defines the data contents of tracks 1 and 2 of the magnetic stripe.*
ISO/IEC 7816	Identification Cards – Integrated Circuit(s) Cards with Contacts ◆ *The most important family of ISO standards for microcontroller smart cards. The first three parts primarily focus on the card and chip hardware. The remaining parts specify all mechanisms and properties of applications and operating systems for smart cards, as well as the associated informatics aspects.*
– 1: 1998	Part 1: Physical Characteristics *Defines the physical characteristics of a card with a contact-type chip, as well as the tests to be used for such a card.*
– 2: 1999	Part 2: Dimensions and Location of the Contacts

	Defines the sizes and positions of the contacts of a smart card, as well as the possible arrangements of the chip, magnetic stripe and embossing. Also describes the method to be used to measure the positions of the contacts on the smart card.
– 3: 1997	Part 3: Electronic Signals and Transmission Protocols
	◆ *The most important ISO standard for the general electrical parameters of a microcontroller smart card. It specifies all basic electrical characteristics, such as the supply voltage (3-V and 5-V), stopping the clock and reset behavior (cold and warm reset). It also defines the parameters, structure and possible sequences for the ATR and PPS. A large part of this standard deals with basic aspects of data transmission at the physical level (such as the divider) and the definition of the two transmission protocols ($T = 0$ and $T = 1$), and it includes extensive examples of communications sequences.*
– 4: 1995	Part 4: Inter-industry Commands for Interchange
	◆ *The most important application-level ISO standard for smart cards. It defines the file organization, file structures, security architecture, TPDUs, APDUs, secure messaging, return codes and logical channels. The majority of this standard is taken up by an extensive description of commands for smart cards. Fundamental smart card mechanisms for general industrial applications are also described.*
– 4 Amd. 1: 1997	Part 4 – Amendment 1: Use of Secure Messaging
– 5: 1994	Part 5: Numbering System and Registration Procedure for Application Identifiers
	Defines the numbering scheme for uniquely identifying national and international applications in smart cards. Also defines the exact data structure of the AID and describes the procedure for registering applications.
– 5 Amd. 1: 1996	Part 5 – Amendment 1: Registration of Identifiers
– 6 CD: 2001	Identification cards – Integrated Circuit(s) Cards with Contacts – Part 6: Inter-industry Data Elements

	Defines the data objects (DOs) and associated TLV tags for general industrial applications, and describes the associated TLV structures and procedures for reading data objects from smart cards.
– 7: 1999	Part 7: Inter-industry Commands for Structured Card Query Language (SCQL) *Defines supplementary smart card commands as an extension to ISO/IEC 7816-4. Defines the basic principles of a database system based on SQL, and specifies the commands for the associated SCQL accesses to smart cards.*
– 8: 1999	Part 8: Security Related Inter-industry Commands *This part of the family of standards is fully dedicated to functions and commands related to security. As an extension to ISO/IEC 7816-4, it defines additional mechanisms for secure messaging, as well as numerous commands for cryptographic functions, such as digital signatures, hash computation, MAC computation and the encryption and decryption of data.*
– 9: 2000	Part 9: Enhanced Inter-industry Commands *This standard is divided into three parts. The first part describes the life cycle of a smart card application at the file level in terms of states. The large second part describes access control objects (ACOs) that can be used to govern file accesses. The extensive third part defines search commands for file contents and administrative commands for creating and deleting files, which are necessary for managing applications.*
– 10: 1999	Part 10: Electronic Signals Answer to Reset for Synchronous Cards *For memory cards, this is the counterpart to Part 3 of this family of standards. It specifies the essential electrical characteristics of memory cards and defines the parameters and structure of the ATR and possible ATR procedures for synchronous cards.*
– 11 CD: 2000	Part 11: Card Structure and Enhanced Functions for Multiapplication Use *Defines commands for biometric user indentification and the associated data objects. In*

	addition, the appendix illustrates the basic features of methods for recording biometric data in the card (enrollment) and describes a scenario for verifying this biometric information.
– 15 CD: 2001	Part 15: Cryptographic Information Application *This part of the family, which is based on the PKCS #15 standard, defines all necessary data objects for an interoperable smart card for digital signatures. It includes descriptions of all data objects, directories and files needed for signature cards, as well as ASN.1 descriptions of all of the certificates, keys and other administrative data stored in the files.*
ISO 8372: 1987	Information Processing – Modes of Operation for a 64-Bit Block Cipher Algorithm ◆ *Defines the four operating modes for encryption algorithms using a 64-bit block size (e.g., DES): electronic codebook (ECB), cipher block chaining (CBC), output feedback (OFB) and cipher feedback (CFB). The block encryption modes described in ANSI X 3.106 and FIPS 81 form a subset of this standard.*
ISO 8583	Financial Transaction Card Originated Messages – Interchange Message Specifications *Standard for data transmission between a terminal and its host system. In Germany, communications between debit card terminals and the background system are based on this standard.*
– 1 CD: 1998	Part 1: Messages, Data Elements and Code Values
– 2: 1998	Part 2: Application and Registration Procedures for Institution Identification Codes (IIC)
– 3: 1988	Part 3: Maintenance Procedures for Messages, Data Elements and Code Values
ISO 8730: 1990	Banking – Requirements for Message Authentication *Fundamentals of securing data transmission and generating and testing MACs. The appendix contains extensive numerical examples, as well as a description of a DES pseudorandom number generator.*
ISO 8731	Banking – Approved Algorithms for Message Authentication

– 1: 1987	Part 1: DEA *A very short standard in which DEA is described as being suitable for MAC computation. Also contains a brief description of parity calculation for DES keys.*
– 2: 1992	Part 2: Message Authenticator Algorithm *Defines a fast algorithm for MAC computation in banking applications. The appendix contains numerical examples as well as an exact description of the algorithm.*
ISO 8732: 1988	Banking – Key Management *Extensive standard addressing principles and methods for key management among two or more participating parties using symmetric cryptographic algorithms.*
ISO/IEC 8824	Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1) *Defines the basic ASN.1 coding rules.*
– 1: 1998	Part 1: Specification of Basic Notation
– 1: 1998 / Amd 1: 2000	Part 1 – Amendment 1: Relative Object Identifiers
– 1: 1998 / Amd 2: 2000	Part 1 – Amendment 2: ASN.1 Semantic Model
– 1: 1998 / Amd 3: 2000	Part 1 – Amendment 3: XML Value Notation
– 1: 1998 / Amd 4: 2000	Part 1 – Amendment 4: Version Number Support
– 2: 1998	Part 2: Information Object Specification
– 2: 1998 / Amd 1: 2000	Part 2 – Amendment 1: ASN.1 Semantic Model
– 2: 1998 / Amd 2	Part 2 – Amendment 2: XML Value Notation
– 3: 1998	Part 3: Constraint Specification
– 4: 1998	Part 4: Parameterization of ASN.1 Specifications
– 4: 1998 / Amd 1: 2000	Part 4 – Amendment 1: ASN.1 Semantic Model
ISO/IEC 8825	Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) *Defines the ASN.1 data description language.*
– 1:1998	Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
– 1:1998 / Amd 1:2000	Part 1 – Amendment 1: Relative Object Identifiers
– 2:1998	Part 2: Specification of Packed Encoding Rules (PER)

– 2:1998 / Amd 1:2000	Part 2 – Amendment 1: Relative Object Identifiers
– 3 FCD: 2001	Part 3: Specification of Encoding Control Notation (ECN)
– 3: FCD / Amd 1: 2001	Part 3 – Amendment 1: ASN.1 Extensibility Notation
– 4: WD 2000	Part 4: XML Encoding Rules (XER)
ISO/IEC 8859 - 1: 1998	Information Technology – 8-bit single-byte coded graphic character sets – Part 1: Latin Alphabet No. 1
ISO/IEC 9075	Information Technology – Database Languages – SQL2 *Defines the structured query language (SQL), database query language, which is a superset of the smart card database query language (SCQL).*
– 1: 1999	Part 1: Framework (SQL/Framework)
– 1: 1999 / Amd 1: 2001	Part 1 – Amendment 1: On-Line Analytical Processing (SQL/OLAP)
– 2: 1999	Part 2: Foundation (SQL/Foundation)
– 2: 1999 / Amd 1: 2001	On-Line Analytical Processing (SQL/OLAP)
– 3: 1999	Part 3: Call-Level Interface (SQL/CLI)
– 4: 1999	Part 4: Persistent Stored Modules (SQL/PSM)
– 5: 1999	Part 5: Host Language Bindings (SQL/Bindings)
– 5: 1999 / Amd 1: 2001	Part 5 – Amendment 1: On-Line Analytical Processing (SQL/OLAP)
– 9: 2001	Part 9: Management of External Data (SQL/MED)
– 10: 2000	Part 10: Object Language Bindings (SQL/OLB)
– 11: CD 2001	Part 11: Information and Definition Schemas (SQL/schemata)
– 12: AWI 2000	Part 12: Replication
– 13: FCD 2001	Part 13: Java Routines and Types (SQL/JRT)
– 14: WD 2001	Part 14: XML-Related Specifications (SQL/XML) ISO/IEC 9126: 1991 Information Technology – Software product evaluation – Quality Characteristics and Guidelines for their Use
ISO/IEC 9126	Software Engineering – Product Quality
– 1: 2001	Part 1: Quality Model
– 2: CD 2001	Part 2: External Metrics
– 3: CD 2001	Part 3: Internal Metrics
– 4: CD 2001	Part 4: Quality in Use Metrics

ISO 9564	Banking – Personal Identification Number Management and Security
– 1: 1991	Part 1: PIN Protection Principles and Techniques
	Fundamentals of PIN selection, PIN management and PIN protection for general banking applications. The appendices define general requirements for PIN entry devices, among other things, as well as recommendations for the layout of suitable keypads and advice regarding erasing sensitive data on various media, such as magnetic tape, paper and semiconductor memories.
– 2: 1991	Part 2: Approved Algorithm(s) for PIN Encipherment
	A very short standard that defines DES as an algorithm for PIN encryption.
– 3: 2002	Part 3: PIN Protection Requirements for Offline PIN Handling in ATM and POS Systems
ISO/IEC 9646-3: 1998	Information Technology – Open Systems Interconnection – Conformance Testing Methodology and Framework – Part 3: The Tree and Tabular Combined Notation (TTCN)
	An extensive standard that describes a general high-level language for specifying tests. TTCN is used in a few isolated cases in the smart card environment.
ISO/IEC 9796	Information Technology – Security Techniques – Digital Signature Scheme giving Message Recovery
	Defines methods for generating and verifying digital signatures with message recovery. The appendix contains several numerical examples of key generation, signature generation and signature verification.
– 1: 1999	Part 1: Mechanisms using Redundancy
– 2: 1997	Part 2: Mechanisms using a Hash Function
– 3: 2000	Part 3: Discrete Logarithm Based Mechanisms
ISO/IEC 9797	Information Technology – Security techniques – Message Authentication Codes (MACs)
– 1: 1999	Part 1: Mechanisms using a Block Cipher
– 2: 1999	Part 2: Mechanisms using a Dedicated Hash Function

ISO/IEC 9798	Information Technology – Security techniques – Entity Authentication ◆ *This family of standards contains detailed descriptions of various cryptographic methods for authenticating one, two or three participating parties. It is the most important reference on the subject of authentication.*
– 1: 1997	Part 1: General *Defines the terms and notation used in the other parts of this family of standards.*
– 2: 1999	Part 2: Mechanisms using Symmetric Encipherment Algorithms *Specifies authentication methods based on symmetric cryptographic algorithms.*
– 3: 1998	Part 3: Mechanisms using Digital Signature Techniques *Specifies authentication methods based on asymmetric cryptographic algorithms.*
– 4: 1999	Part 4: Mechanisms using a Cryptographic Check Function *Specifies authentication methods based on cryptographic check functions.*
– 5: 1999	Part 5: Mechanisms using Zero Knowledge Techniques *Specifies authentication methods based on zero-knowledge techniques.*
ISO 9807: 1991	Banking and Related Financial Services – Requirements for Message Authentication (retail)
ISO/IEC 9979: 1999	Information Technology – Security techniques – Procedures for the Registration of Cryptographic Algorithms
ISO 9992	Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device
– 1: 1990	Part 1: Concepts and Structures
– 2: 1998	Part 2: Functions, Messages (Commands and Responses), Data Elements and Structures *Defines commands, procedures, and data elements for smart cards used in financial transaction systems. Contains the definitions of*

	tags used in financial transaction systems and many cross-references to other standards in the ISO/IEC 7816 family.
– 4 DIS: 1993	Part 4: Common Data for Interchange
– 5 CD: 1991	Part 5: Organization of Data Elements
ISO/IEC 10 116: 1997	Information Technology – Security techniques – Modes of Operation for an *n*-bit Block Cipher Algorithm
	Describes the four standard opearting modes (ECB, CBC, CFB, OFD) for a block-oriented encryption algorithm. An appendix contains detailed comments regarding the use of each of the four modes, and another appendix contains corresponding numerical examples.
ISO/IEC 10 118	Information Technology – Security techniques – Hash Functions
	General principles of hash functions, as well as associated padding methods.
– 1: 2000	Part 1: General
– 2: 2000	Part 2: Hash Functions using an *n*-bit Block Cipher Algorithm
	Defines hash functions based on block-oriented encryption algorithms and describes algorithms with single-length and double-length keys. The appendix contains a numerical example for each type of key, based on the DES algorithm.
– 3: 1998	Part 3: Dedicated Hash Functions
– 4: 1998	Part 4: Hash Functions using Modular Arithmetic
ISO 10 202	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards
– 1: 1991	Part 1: Card Life Cycle
– 2: 1996	Part 2: Transaction Process
– 3: 1998	Part 3: Cryptographic Key Relationship
– 4: 1996	Part 4: Secure Application Modules
– 5: 1998	Part 5: Use of Algorithms
– 6: 1994	Part 6: Card holder Verification
– 7: 1998	Part 7: Key Management

	Defines general mechanisms for key management and key derivation. Both symmetrical and asymmetrical mechanisms are described.
– 8: 1998	Part 8: General Principles and Overview
ISO/IEC 10 373	Identification Cards – Test Methods
	◆ *Fundamental standard for card testing. Contains precise descriptions of test methods for card bodies and card bodies with implanted chips. The individual tests are described in detail, with many explanatory drawings.*
– 1: 1998	Part 1: General Characteristics Tests
– 2: 1998	Part 2: Cards with Magnetic Stripes
– 3: 2001	Part 3: Integrated Circuit(s) Cards with Contacts and Related Interface Devices
	Specifies the test environment, test methods and test procedures for electrical tests for contact-type smart cards. Also specifies detailed procedures for checking contact locations, electrical power, ATR and PPS data transmission and data transmission protocols.
– 4 CD: 1998	Part 4: Contactless Integrated Circuit Cards
– 5: 1998	Part 5: Optical Memory Cards
– 6: 2001	Part 6: Proximity Cards
– 7: 2001	Part 7: Vicinity Cards
ISO/IEC 10 536	Identification Cards – Contactless Integrated Circuit(s) Cards
	◆ *This standard descibes contactless smart cards whose application areas limit them to direct contact with the terminal.*
– 1: 2000	Part 1: Physical Characteristics
	Defines the physical characteristics of contactless smart cards and associated test methods.
– 2: 1995	Part 2: Dimension and Location of Coupling Areas
	Specifies the dimensions and locations of the coupling areas for contactless cards, and their use wih card terminals having card slots or surface interfaces.
– 3: 1996	Part 3: Electronic Signals and Reset Procedures
	Defines the electrical signals of the inductive and capacitive elements used to couple the smart card to the terminal.

– 4 CD: 1997	Part 4: Answer to Reset and Transmission Protocols *Specifies data transmission at the physical level, as well as the structure and parameters of the ATR and PPS for contactless smart cards. Defines the $T = 2$ data transmission protocol, with many sample scenarios for protocol procedures.*
ISO/IEC 10646	Information Technology – Universal Multiple-Octet Coded Character Set (UCS)
– 1: 2000	Part 1: Architecture and Basic Multilingual Plane
– 2: 2001	Part 2: Supplementary Planes
ISO 11 568	Banking – Key Management
– 1: 1994	Part 1: Introduction to Key Management
– 2: 1994	Part 2: Key Management Techniques for Symmetric Ciphers
– 3: 1994	Part 3: Key Life Cycle for Symmetric Ciphers
– 4: 1998	Part 4: Key Management Techniques for Public Key Cryptosystems
– 5: 1998	Part 5: Key Life for Public Key Cryptosystems
– 6: 1998	Part 6: Key Management Schemes
ISO/IEC 11 693: 2000	Identification Cards – Optical Memory Cards
ISO/IEC 11 694	Identification Cards – Optical Memory Cards and Devices – Linear Recording Method
– 1: 2000	Part 1: Physical Characteristics
– 2: 2000	Part 2: Dimensions and Location of the Accessible Optical Area
– 3: 2001	Part 3: Optical Properties and Characteristics
– 4: 1996	Part 4: Logical Data Structures
ISO/IEC 11 770	Information Technology – Security Techniques – Key Management
– 1: 1996	Part 1: Framework
– 2: 1996	Part 2: Mechanisms using Symmetric Techniques
– 3: 1999	Part 3: Mechanisms using Asymmetric Techniques
ISO/IEC 12 207: 1995	Information technology – Software Life Cycle Processes
ISO/IEC 13 239: 2000	Information Technology – Telecommunications and Information Exchange between Systems – High-level Data Link Control (HDLC) Procedures

ISO 13 491	Banking – Secure Cryptographic Devices
– 1: 1998	Part 1: Concepts, Requirements and Evaluation Methods
– 2: 2000	Part 2: Security Compliance Checklists for Devices used in Magnetic Stripe Card Systems
ISO/IEC 13 888	Information Technology – Security Techniques – Non-repudiation
– 1: 1997	Part 1: General
– 2: 1998	Part 2: Mechanisms using Symmetric Techniques
– 3: 1997	Part 3: Mechanisms using Asymmetric Techniques
ISO/IEC 14 443	Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards ◆ *This standard describes contactless smart cards that can be used at a distance of up to several tens of centimeters from a terminal.*
– 1: 2000	Part 1: Physical Characteristics
– 2: 2001	Part 2: Radio Frequency Power and Signal Interface
– 3: 2001	Part 3: Initialization and Anticollision
– 4: 2001	Part 4: Transmission Protocol
ISO/IEC 14 888	Information Technology – Security Techniques – Digital Signature with Appendix *This standard specifies basic mechanisms and methods for digital signatures with appendix. It is independent of any particular asymmetric cryptographic algorithm.*
– 1: 1998	Part 1: General
– 2: 1999	Part 2: Identity-based Mechanisms
– 3: 1998	Part 3: Certificate-based Mechanisms
ISO/IEC 15 292: 2001	Information Technology – Security Techniques – Protection Profile Registration Procedures
ISO/IEC 15 408	Information Technology – Security Techniques – Evaluation Criteria for IT Security
– 1: 1999	Part 1: Introduction and General Model
– 2: 1999	Part 2: Security Functional Requirements
– 3: 1999	Part 3: Security Assurance Requirements

ISO/IEC 15 693	Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards *This standard describes contactless smart cards that can be used at a distance of up to one meter from a terminal.*
– 1 CD: 2000	Part 1: Physical Characteristics
– 2 WD: 2000	Part 2: Air Interface and Initialization
– 3 WD: 2001	Part 3: Anticollision and Transmission Protocol
– 4 WD: 1996	Part 4: Extended Command Set and Security Features
ISO 15 782	Banking – Certificate Management for Financial Services
– 1 DIS: 2000	Part 1: Public Key Certificates
– 2: 2001	Part 2: Certificate Extensions
ISO/IEC 15 946	Information Technology – Security Techniques – Cryptographic Techniques based on Elliptic Curves
– 1 FDIS: 2001	Part 1: General
– 2 FDIS: 2001	Part 2: Digital Signatures
– 3 FDIS: 2001	Part 3: Key Establishment
– 4 CD: 2000	Part 4: Digital Signatures giving Message Recovery
ISO 17 090	Public Key Infrastructure
– 1 CD: 2001	Part 1: Framework and Overview
– 2 CD: 2001	Part 2: Certificate Profile
– 3 CD: 2001	Part 3: Policy Management of Certification Authority
ITU X.509: 2000	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework ◆ *Specifies the structure and coding of certificates. Internationally, it is the most commonly used basis for certificate structures, and it is identical to ISO/IEC 9594-8.*
Java Card 2.1: 2000	◆ *This industrial standard forms the basis for Java Card. It was generated by the Java Card Forum and published by the Sun Corporation. All of the standards in this family are mutually complementary and address various aspects of Java Card implementations.*

– Application Programming Interface

Specifies the complete interface (API) available to an applet in a Java Card environment. It esssentially consists of a comprehensive listing of all classes and interfaces of the Java Card API.

– Runtime Environment (JCRE) Specification

Specifies the Java Card runtime environment, which essentailly consists of the Java virtual machine and the Java Card API. It addresses the following topics in detail: the lifetime of the virtual machine, the lifetimes of applets, selecting applets, transient objects, sharing objects, transactions, the extent to which transactions are atomic and installing applets.

– Virtual Machine Specification

Specifies the Java Card virtual machine, including its detailed architecture, its instruction set and the format of CAP files

Multifunktionale Karten Terminals Spezification, Version 1.0: 1999	*The MKT specification, which is published by Teletrust Deutschland, is the quasi-standard in Germany for connecting terminals to PCs.*
– Part 1	MKT-Basiskonzept
– Part 2	CT-ICC-Interface – MKT-Schnittstelle für kontaktorientierte Chipkarten mit synchroner und asynchroner Übertragung
– Part 3	CT-API 1.1 – Anwendungsunabhängiges Card Terminal Applikation Programming Interface
– Part 4	CT-BCS – Anwendungsunabhängiges Card Terminal Basic Command Set
– Part 5	Chipkarten mit synchroner Übertragung – ATR und Datenbereiche
– Part 6	Chipkarten mit synchroner Übertragung – Übertragungsprotokolle
– Part 7	Chipkarten mit synchroner Übertragung – Anwendung von Interindustry Commands

OCF – API Docs V1.2: 2001

OCF – Programmer's Guide V 1.2: 2001

Open Platform Card Specification 2.1: 2001	
	◆ *The most important specification with regard to managing applications in multiapplication smart cards. This very comprehensive specification contains a detailed presentation of the software and security architectures of multiapplication smart cards and a thorough description of the commands needed for this purpose. The appendix includes the specification of an API for application management with Java Card, which has become the* de facto *standard for this type of smart card.*[74]
PC/SC V1.0: December 1997	Interoperability Specification for ICCs and Personal Computer Systems
	This extensive, detailed specification forms the basis for linking smart cards and terminals to the resource management system of 16-bit and 32-bit Microsoft operating systems.
– 1	Part 1: Introduction and Architecture Overview
– 2	Part 2: Interface Requirements for Compatible IC Cards and Readers
– 3	Part 3: Requirements for PC-Connected Interface Devices
– 4	Part 4: IFD Design Considerations and Reference Design Information
– 5	Part 5: ICC Resource Manager Definition
– 6	Part 6: ICC Service Provider Interface Definition
– 7	Part 7: Application Domain and Developer Design Considerations
– 8	Part 8: Recommendations for ICC Security and Privacy Devices
PKCS	*The Public Key Cryptography Standards (PKCS) are industry standards published by RSA Inc. that focus on the use of asymmetric cryptographic algorithms.*
– PKCS #1 V 2.1: 2001	RSA Encryption Standard
	◆ *Describes mechanisms for encryption and decryption using the RSA algorithm.*
– PKCS #3 V 1.4: 1993	Diffie–Hellman Key-Agreement Standard
	Describes the mechanism of a key exchange procedure between two parties using the Diffie–Hellman procedure.

[74] See also Section 5.11, 'Open Platform'

– PKCS #5 V 2.0: 1999	Password-Based Cryptography Standard *Contains recommendations for the implementation of encryption, key derivation and MAC generation based on keys generated from passwords.*
– PKCS #11 V 2.11: 2001	Cryptographic Token Interface Standard ◆ *The* de facto *international standard for an API for invoking cryptographic functions. This API is called 'Cryptoki' (cryptographic token interface) and includes functions such as RC2, RC4, RC5, MD5, SHA-1, DES, triple-DES, IDEA, RSA, DSA, MAC computation and key generation for a wide variety of cryptographic algorithms.*
– PKCS #13 V 1.0: 1998	Elliptic Curve Cryptography Standard
– PKCS #14 V 1.0 (Proposal: 1998)	Pseudorandom Number Generation Standard *This unfinished standard with a relatively small scope contains suggestions for the conceptual design of random number generators.*
– PKCS #15 V 1.1: 2000	Cryptographic Token Information Format Standard ◆ *Internationally, this is the* de facto *standard for the data objects needed for an interoperable smart card for digital signatures. It includes descriptions of all directories and files needed for a signature card and ASN.1 descriptions of all certificates, keys and administrative data stored in the files.*
RFC 1319: 1992	The MD2 Message-Digest Algorithm
RFC 1320: 1992	The MD4 Message-Digest Algorithm
RFC 1321: 1992	The MD5 Message-Digest Algorithm
RFC 1750: 1994	Randomness Recommendations for Security *Describes the operating principles of various types of random number generators, and based on these principles, recommends methods for designing high-quality pseudorandom number generators for PCs.*
RFC 2706: 1999	ECML V1: Field Names for E-Commerce
SET Book 1, Version 1.0: 1997	Secure Electronic Transaction Specification, Book 1: Business Description

SET Book 2, Version 1.0: 1997	Secure Electronic Transaction Specification, Book 2: Programmer's Guide
SET Book 3, Version 1.0: 1997	Secure Electronic Transaction Specification, Book 3: Formal Protocol Definition
TIA/EIA/IS-820: 2000	Removable User Identity Module (R-UIM) for TIA/EIA Spread Spectrum Standards
TIA/EIA/IS-820-1: 2001	Removable User Identity Module (R-UIM) for TIA/EIA Spread Spectrum Standards, Addendum 1
TIA/EIA/IS-839: 2000	R-UIM Overview, Operation, and File Structure Support in TIA/EIA-136
TR 33.900, V 1.2.0: 2000	3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security Architecture *An overview of the security architecture, available security functions and possible attack scenarios for 3G mobile telecommunications networks. Details related to security are described in the relevant standards (TS 33.102, TS 33.120 and TS 21.133).*
TS 21.111, Version 4.0.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM and IC card requirements *A short standard that specifies the basic functionality required for a security module (USIM) for a UMTS mobile communications network. This standard is the UMTS equivalent of the GSM 02.17 standard.*
TS 21.133, Version 4.0.0: 2001	Universal Mobile Telecommunications System (UMTS); 3G Security; Security Threats and Requirements
TS 22.038, Version 4.1.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM/SIM Application Toolkit (USAT, SAT); Service description; Stage 1
TS 22.112, Version 5.0.0: 2001	Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter – Stage 1
TS 23.038, V 4.3.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Alphabets and language-specific information *Specifies the character coding used for SMS and USSD and the character sets used for UMTS.*

TS 23.040, V 4.3.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Technical realization of the Short Message Service (SMS)
TS 23.048, Version 5.1.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Security Mechanisms for the (U)SIM Application Toolkit; Stage 2
TS 31.102, Version 4.2.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM Application ◆ *Specifies the logical characteristics of the USIM smart card application by describing the interface between the USIM and the UMTS mobile telephone. Includes detailed descriptions of all files and their data objects, definitions of several somewhat less UMTS-specific commands and examples of command sequences for typical processes. Together with TS 31.101, it is the UMTS equivalent of the GSM GMS 11.11 standard.*
TS 31.110, Version 4.0.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Numbering system for telecommunication IC card applications *Future versions of this standard will be published as TS 101.220.*
TS 31.111, Version 4.4.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT) *Defines and extensively describes the USIM Application Toolkit for USIMs. The USAT describes an interface between the mobile telephone and the USIM that allows supplementary applications in the USIM to assume partial control of the telephone. It introduces proactive commands for the USIM and defines many new commands related to control of the telephone for functions such as display output, keypad polling and sending short messages. The GSM equivalent of this standard is GSM 11.14.*
TS 31.112, Version 5.0.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter Architecture Description; Stage 2

TS 31.113, Version 5.0.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter Byte Codes
TS 31.114, Version 1.1.0: 2002	3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter Protocol and Administration
TS 31.121, Version 4.0.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-Terminal Interface; USIM Application Test Specification
TS 31.122, Version 3.0.0: 2000	3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Conformance Test Specification *Specifies the test environment, test equipment, test hierarchy and individual test cases for testing USIMs. The described tests exclusively address electrical and informatics aspects. Detailed specifications are provided for tests covering a wide range of subjects, such as electrical power, data transmission, file management, commands and typical processes in the UMTS application. This standard is a very good example of how USIM tests can be described, constructed and executed. It is the USIM equivalent of the GSM 11.17 standard for testing SIMs.*
TS 31.900, Version 3.1.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; SIM/USIM Internal and External Interworking Aspects
TS 33.102, Version 4.1.0: 2001	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture *A key standard for the entire security architecture of a UMTS mobile telecommunications network with regard to network access, authentication, confidentiality and data integrity. Includes complete descriptions, independent of any specific cryptographic algorithm, of network security functions, authentication protocols and encryption methods, as well as generating authentication vectors and the key derivations that are used.*
TS 33.103, Version 4.1.0: 2001	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines

TS 33.105, Version 4.1.0: 2001	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements
TS 33.120, Version 4.0.0: 2001	Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives
TS 35.205, Version 4.0.0: 2001	Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General
TS 35.206, Version 4.0.0: 2001	Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification
TS 35.207, Version 4.0.0: 2001	Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' Test Data
TS 35.208, Version 4.0.0: 2001	Universal Mobile Telecommunications System (UMTS); 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design Conformance
TS 35.909, Version 4.0.0: 2001	Universal Mobile Telecommunications System (UMTS); 3G security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP Authentication and Key Generation functions
TS 42.009, V4.0.0: 2001	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); Security aspects *Fundamental document containing an overview of the important security aspects of a PLMN.*

TS 51.011, Version 4.2.0: 2001	3rd Generation Partnership Project; Technical Specification Group Terminals; Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface *Identical to GSM 11.11 in the new ETSI numbering system.*
TS 101.220, V 4.0.0: 2001	Integrated Circuits Cards (ICC); ETSI numbering system for telecommunication application providers *Specifies the AIDs, PIX and TAR for the SIM, TETRA-SIM and USIM. Also defines the code space of the PIX for the various types of supplemenatary applications of this type of telecommunications smart card.*
TS 102.221, Version 4.4.0: 2001	Smart cards; UICC–Terminal interface; Physical and logical characteristics ◆ *Specifies the logical characteristics of a USIM by means of a description of the interface between the USIM and the UMTS mobile telephone. Includes definitions of the ID-1 and plug-in card formats and specifies the general mechanical parameters of the card and its contacts, as well as all general electrical parameters. It also specifies the structure and data content of the ATR and PPS and defines transmission protocols, file structures, security mechanisms, commands and return codes. In addition, it lists all files and associated data objects that are independent of any particular telecommunications application. This standard forms the basis for smart card operating systems for the USIM. It is complemented by TS 31.103, which addresses all application-specific components of a USIM. These two standards form the UMTS equivalent of the GMS 11.11 standard.*
TS 102.222, Version 3.3.0: 2001	Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications *Specifies the administrative commands for file management and associated security conditions for use with telecommunications smart cards.*

TS 102.223, Version 4.1.0: 2001	Smart Cards; Card Application Toolkit (CAT) *Defines and thoroughly describes a generic application toolkit for telecommunications smart cards. CAT describes an interface between the mobile telephone and the smart card that allows supplementary applications in the smart card to assume partial control of the telephone. This standard defines commands related to controlling the telephone for functions such as display output, keypad polling and sending short messages. It forms the basis for other standards, such as GSM 11.14 and TS 31.111.*
TS 102.224, Version 1.0.0: 2001	Smart Cards; Security mechanisms for the Card Application Toolkit; Functional requirements
TS 102.225, Version 1.0.0: 2001	Smart Cards; Secured packet structure for UICC applications
TS 102.226, Version 1.0.0: 2001	Smart Cards; Remote APDU Structure for UICC based Applications
TS 102.230, Version 4.0.0: 2001	Smart Cards; UICC-Terminal Interface; Physical, Electrical and Logical Test Specification *Specifies physical and electrical tests for UICCs, and describes basic tests for the communications link to the UICC and tests for the $T = 0$ and $T = 1$ transmission protocols.*
TS 102.240, Version 1.0.0: 2001	Smart Cards; UICC Application Programming Interface (UICC API); Service description
TS 102.241, Version 1.0.0: 2001	UICC Application Programming Interface (UICC API); UICC API for Java Card
TS 123.002, Version 4.4.0: 2002	Universal Mobile Telecommunications System (UMTS); Network architecture
Unicode Standard, Version 3.1.1: 2001	
Universal Serial Bus Specification, Revision 2.0, 2000	*This very comprehensive specification forms the basis for the USB interface.*
Wireless Application Protocol Identity Module Specification, Version 260: July 2001	*Specifies the physical and electrical properties of a WIM, which is the digital signature application for telecommunications smart cards. Lists all mechanisms, commands, data objects and files needed for a WIM application.*

16.5 CODING OF DATA OBJECTS

Additional tables of tags for data objects can be found in Chapter 5, which describes accesses to smart card resources in accordance with ISO/IEC 7816-9.

16.5.1 Data objects compliant with ISO/IEC 7816-4

Table 16.2 The coding of a number of important data objects as defined in ISO/IEC 7816-4

Tag	Data object	Template	Length (bytes)	Description
'62'	File control parameters (FCP) template	---	---	The FCP template contains file control parameters (FCP).
'64'	File management data (FMD) template	---	---	The FMD template contains file management data (FMD).
'6F'	File control information (FCI) template	---	---	The FCI template contains file control parameters (FCP) and file management data (FMD).
'80'	Number of data bytes in the file, excluding structure data	'62'	2	For EFs with transparent structure.
'81'	Number of data bytes in the file, including structure data	'62'	2	For all files.
'82'	File description	'62'	1–4	File access: °00-- ----°: file is not shareable (concurrent access via several logical channels not possible) °01-- ----°: file is shareable (concurrent access via several logical channels is possible) File type: °--00 0---°: working EF °--00 1---°: internal EF °--11 1---°: DF EF structure: °---- -000°: no data °---- -001°: transparent °---- -010°: linear fixed °---- -011°: linear fixed, content simple-TLV-coded °---- -100°: linear variable

Table 16.2 (*Cont.*)

				°---- -101°: linear variable, content simple-TLV-coded °---- -110°: cyclic °---- -111°: cyclic, content simple-TLV-coded
'83'	FID	'62'	2	For all files.
'84'	DF name	'62'	1–16	For DFs.
'86'	Security attribute	'62'	variable	
'88'	Short file identifier (SFI)	'62'	1	Definition of EFs from ISO/IEC 7816-9. SFI = b8 . . . b4 || °000°
'8A'	Life cycle status indicator (LCSI tag)	'62'	1	Bit coding specified in ISO/IEC 7816-9. °0000 0000°: no data °0000 0001°: creation state °0000 0011°: initialization state °0000 01x1°: operational state: activated °0000 01x0°: operational state: deactivated °0000 11xx°: termination state °yyyy xxxx°: y ≠ 0, proprietary

16.5.2 Data objects compliant with ISO/IEC 7816-6

Table 16.3 The coding of a number of important data objects as defined in ISO/IEC 7816-6

Tag	Data object	Template	Length (bytes)	Description
'4F'	AID	'61'/'6E'	5–16	—
'50'	Application name	'61'/'6E'	variable	
'59'	Card expiry date	'66'	3	Format: YYMMDD
'5B'	Name	'65'	39 max.	
'5F24'	Application expiry date	'6E'	3	Format: YYMMDD
'5F25'	Date of issue of the card	'6E'	3	Format: YYMMDD
'5F26'	Date of issue of the application	'66'	3	Format: YYMMDD
'5F28'	Country identifier	'66'	2	Format: 3 digits, coded per ISO 3166
'5F2A'	Currency identifier	'6E'	2	Format: 3 digits, coded per ISO 3166
'5F2B'	Date of birth	'65'	4	Format: YYYYMMDD
'5F42'	Address	'65'	variable	Address of a person
'5F4D'	Chip manufacturer	'66'	1	See Section 16.5.3.

16.5.3 Data objects for chip manufacturers as specified by ISO/IEC 7816-6

Table 16.4 Coding of data objects for chip manufacturers as defined in ISO/IEC 7816-6. This table provides a good overview of the manufacturers of smart card microcontrollers. The tag for chip manufacturers is '5F4D'.

Code	Company	Code	Company
'01'	Motorola	'0D'	Mitsubishi Electric
'02'	ST Microelectronics	'0E'	Samsung Electronics
'03'	Renesas	'0F'	Hyundai Electronics Industries
'04'	Philips Semiconductors	'10'	LG-Semiconductors
'05'	Infineon Semiconductors	'11'	Emosyn-EM Microelectronics
'06'	Cylinc	'12'	Inside Technologies
'07'	Texas Instrument	'13'	ORGA Kartensysteme
'08'	Fujitsu	'14'	Sharp Corporation
'09'	Matsushita Electronic	'15'	ATMEL
'0A'	NEC	'16'	EM Microelectronic-Marin
'0B'	Oki Electric	'17'	KSW Microtec
'0C'	Toshiba	'19'	Xicor

16.6 REGISTRATION AUTHORITIES FOR RIDs

The form for registering an RID is located in the appendix of the ISO/IEC 7816-5 standard. An application for an international RID is normally made via the relevant national authority, and there is a fee. The addresses of national registration authorities, as well as the registration procedures for RIDs, can usually be obtained from national standardization bodies.

Table 16.5 Registration authorities for RIDS compliant with ISO/IEC 7816-5

Region	Organization
International	TeleDanmark KTAS attn: ISO/IEC 7816-5 Registration Authority Teglholmsgade 1 1790 Copenhagen V Denmark
Germany	RID German National Registration Authority c/o GMD Bruno Struif Rheinstraße 75 D - 64 295 Darmstadt, Germany

16.7 SELECTED RIDS

Table 16.6 lists a number of examples of publicly known RIDs and AIDs. Unfortunately, RIDs are treated as confidential by registration authorities, so the list is not very long.

Table 16.6 Selected RIDs of typical smart card applications and organizations that use smart cards

Smart card applications	AID (application identifier) = RID || PIX
3GPP (UICC, USIM, USAT)	RID = 'A0 00 00 00 87' PIX = specific to the card issuer
Eurocheque card with chip in Germany	RID = 'D2 76 00 00 25' PIX = '45 50 01 00'
ETSI (SIM, SAT, Java Card SIM API, TETRA)	RID = 'A000000009'
FINEID (Finnish personal ID card)	RID = 'A0 00 00 00 63' PIX = '50 4B 43 53 2D 31 35'
Giesecke & Devrient	RID = 'D2 76 00 00 05'
PKCS #15	RID = 'A0 00 00 00 63' PIX = '50 4B 43 53 2D 31 35' = "PKCS-15"
WIM	RID = 'A0 00 00 00 63' PIX = '57 41 50 2D 57 49 4D' = "WAP-WIM"
Wolfgang Rankl	RID = 'D2 76 00 00 60'

16.8 TRADE FAIRS, CONFERENCES AND CONVENTIONS

Table 16.7 lists trade fairs, congresses and conventions that have smart cards or related subjects as at least one of their major themes. The listed places and dates are typical for the past several years, but they can change in the future, depending on the event organizer. As can be seen, a traveler with an interest in the subject can visit an event in a different country every month of the year.

Table 16.7 Selected annual events related to smart cards and cryptology

Event name	Place	Date
Asia Crypt	Asia	Fall
Card Tech / Secure Tech [CTST]	USA	September
Cards Africa	South Africa (Johannesburg)	November
Cards Asia	Singapore	February
Cards Australia	Australia (Melbourne)	August
Cards Latin America	Chile (Santiago de Chile)	July
Cartes	France (Paris)	October
CeBit	Germany (Hanover)	March
Crypto	USA (Santa Barbara, California)	Summer
Euro Crypt	Europe	Spring
GSM World Congress	France (Cannes)	February
Java One	San Francisco, USA	June
OmniCard	Germany (Berlin)	January
Smart Card	Great Britain (London)	February

16.9 WORLD WIDE WEB ADDRESSES

The following list of World Wide Web addresses does not claim to be complete. It should be seen as a cross-section of the various companies and institutions that are active in the field of smart cards. The listed addresses are thus entirely suitable for use as starting points for further research. Thanks to the hypertext structure of HTML documents, many of the listed sites contain links to other interesting documents and World Wide Web locations. Large collections of links are explicitly identified as 'link farms'.

When using this list, you should bear in mind that the Internet is very dynamic, so addresses can very quickly become outdated. This is also why we do not list specific documents, but have limited the listings to subdirectories. Even these are frequently changed when a Web server is reorganized, so in case of doubt we recommend that you use the address up to the organization or country code (**.com, *.de* and so on). After this, you can manually select currently valid directories on the Web server via the home page.

The classification of the Internet addresses and firms is based on their principal areas of activity. However, many of the listed firms are active in several of the indicated areas; this is normally shown explicitly. To the extent that it makes sense to do so, the country in which the firm or organization is located is also noted.

As a rule, you can find the postal address of a firm and the telephone number of a contact person on the home page of the firm. Consequently, postal addresses are not included in the list. If you have a specific need for particular information, we generally advise you to use appropriate search terms (keywords) and a powerful search engine to comb through the World Wide Web. This at least will ensure that you are working with a current cross-section of information.

Table 16.8 Summary of the descriptive categories used in the list of Web addresses

Category	Description
attacks	attacks on smart cards, smart card terminals, security modules etc.
card issuer	issuer of cards and/or smart cards
card manufacturer	manufacturer of cards with or without chips
card production machinery	machinery and equipment for producing cards
cryptography	cryptography related to smart cards
events	seminars, conferences and congresses related to smart cards
link farm	collection of links to other Internet sites
operating systems	operating systems for smart cards
patents	patents related to smart cards
publisher	journals and books related to smart cards
security technology	security technology related to smart cards
semiconductor manufacturer	manufacturer of semiconductors for smart cards, memory chips and/or microcontrollers
software	PC software for smart cards, smart card simulations
standards	standards related to smart cards and cryptography
terminal manufacturer	manufacturer of terminals for cards with or without chips
university	university or technical institute

[3GPP] **3GPP**
standards
http://www.3gpp.org/

[3GPP2] **3GPP2**
standards
http://www.3gpp2.org/

[AC] **Austria Card, Austria**
card manufacturer
http://www.austriacard.at/

[ACG] **ACG, Germany**
chip merchant
http://www.acg.de/

[ActivCard] **ActivCard, USA**
card manufacturer
http://www.activcard.com/

[AltTech] **alt.technology.smartcards FAQ**
smart card FAQ site
http://www.scdk.com/atsfaq.htm

[AM] **American Magnetics, USA**
terminal manufacturer
http://www.magstripe.com/

[AmEx] **American Express, USA**
card issuer
http://www.americanexpress.com/

[Anderson] **Ross Anderson's Home Page, Great Britain**
information about attacks on smart cards
http://www.cl.cam.ac.uk/users/rja14/

[ANSI] **ANSI, USA**
standards
http://www.ansi.org/

[ARM] **ARM Ltd., Great Britain**
processor core for smart card microcontrollers
http://www.arm.com/

[ASM] **ASM Lithography, The Netherlands**
machinery for semiconductor manufacturing
http://www.asml.com/

[Atmel] **Atmel, USA**
smart card microcontrollers
http://www.atmel.com/

[Basiccard] **Basic Card**
smart card operating systems
http://www.basiccard.com/

[BSI] **Bundesamt for Sicherheit in der Informationstechnik (BSI), Germany**
information about security
http://www.bsi.bund.de/

[Card Forum] **Card Forum, Germany**
publisher in the smart card field
http://www.card-forum.com/

[Cardshow] **The Smart Card Cyber Show, France**
http://www.cardshow.com/

[CC] **Common Criteria**
http://www.commoncriteria.org/

[CCC] **Chaos Computer Club e.V., Germany**
attacks on smart cards and cryptographic algorithms
http://www.ccc.de/

[CDG] **CDMA Development Group (CDG)**
information about CDMA
http://www.cdg.org/

[CEN] **CEN**
standards
http://www.cenorm.be/

[CEPS] **CEPSCO**
information about CEPS
http://www.cepsco.com/

[Certicom] **Certicom Corp., Canada**
cryptography, ECC
http://www.certicom.ca/

[Counterpane] **Counterpane, USA**
cryptography
http://www.counterpane.com/

[CR] **Cryptography Research**
attacks
http://www.cryptography.com/

[CTST] **CardTech/SecurTech Conference, USA**
events relating to smart cards
http://www.ctst.com/

[Dai Nippon] **Dai Nippon Printing Co. Ltd., Japan**
smart card manufacturer
http://www.dnp.co.jp/

[Dallas Semi] **Dallas Semiconductor, USA**
semiconductor manufacturer; security processors
http://www.dalsemi.com/

[Datacard] **Datacard, USA**
production machinery for smart cards
http://www.datacard.com/

[De La Rue] **De La Rue Card Systems, Great Britain**
smart card manufacturer
http://www.delarue.com/

[DIN] **Deutsches Institut für Normung e.V. (DIN), Germany**
standards
http://www.din.de/

[DPA] **Deutsches Patentamt, Germany**
patents
http://www.deutsches-patentamt.de/

[Drexler] **Drexler Technology Corp., USA**
cards with optically writeable and readable regions
http://www.lasercard.com/

[ECBS] **European Committee for Banking Standards**
standards and specifications
http://www.ecbs.org/

[ECC] **The Error Correcting Codes (ECC) Home Page, Japan**
link farm for error detection and correction codes
http://www.csl.sony.co.jp/person/morelos/ecc/codes.html

[Emosyn] **Emosyn**
manufacturer of smart card microcontrollers
http://www.emosyn.com/

[EMV] **EMVCO**
information about EMV
http://www.emvco.com/

[Entrust] **Entrust, Canada**
cryptography
http://www.entrust.com/

[ETSI] **ETSI**
standards
http://www.etsi.org/

[Europay] **Europay International, Belgium**
card issuer
http://www.europay.com/

[Eurosmart] **Eurosmart**
information about smart cards
http://www.eurosmart.com

[FINEID] **FINEID, Finland**
information about FINEID
http://www.fineid.fi/

[GD] **Giesecke & Devrient GmbH, Germany**
smart cards; operating systems; terminals
http://www.gieseckedevrient.com/
http://www.gi-de.com/

[Gemplus] **Gemplus S.C.A., France**
smart cards, operating systems, terminals
http://www.gemplus.com/

[Global Platform] **Global Platform**
information about Global Platform
http://www.globalplatform.org/

[Groupmark] **Groupmark Ltd., Canada**
smart card manufacturer
http://www.groupmark.com/

[GSM] **GSM MoU Association**
link farm relating to GSM
http://www.gsmworld.com/

[Gutmann] **Peter Gutmann's Security and Encryption Links**
http://www.cs.auckland.ac.nz/~pgut001/

[Hanser] **Carl Hanser Verlag GmbH, Germany**
pubisher (*Handbuch der Chipkarten*, *The Smart Card Simulator*)
http://www.hanser.de/

[Hypercom] **Hypercom Corp., USA**
terminals
http://www.hypercom.com/

[ICMA] **ICMA – International Card Manufacturers Association**
information about smart cards
http://www.icma.com/

[IEC] **IEC**
standards
http://www.iec.ch/

[IEEE] **IEEE**
standards
http://www.ieee.org/

[Infineon] **Infineon AG, Germany**
semiconductor manufacturer
http://www.infineon.com

[Ingenico] **Ingenico, France**
terminal manufacturer
http://www.ingenico.com/

[Integri] **Integri, Belgium**
testing smart card operating systems
http://www.integri.com/

[Iridium] **Iridium, USA**
information about the Iridium mobile telecommunications network
http://www.iridium.com/

[ISO] **ISO**
standards
http://www.iso.ch/

[ITU] **ITU**
standards
http://www.itu.ch/

[JavaPOS] **JavaPOS**
Java for POS terminals
http://www.javapos.com/

[Javasoft] **Javasoft, USA**
Java for smart cards
http://www.javasoft.com/

[JCF] **Java Card Forum, USA**
Java, specifictions for Java in smart cards
http://www.javacardforum.org/

[JTC1] **ISO, Joint Technical Committee One**
international standardization
http://www.jtc1.org/

[Logika] **Logika Comp Spa, Italy**
personalization systems
http://www.logika.it/

[MagTek] **MagTek Inc., USA**
terminals
http://www.magtek.com/

[Maosco] **Maosco Ltd., Great Britain**
smart card operating system
http://www.multos.com/

[MasterCard] **MasterCard International, USA**
card issuer
http://www.mastercard.com/

[Microsoft] **Microsoft, USA**
Crypto-API, PC/SC
http://www.microsoft.com/

[MIPS] **MIPS**
manufacturer of processors
http://www.mips.com/

[MobM] **Mobile Mind, USA**
smart card company
http://www.mobile-mind.com

[Mondex] **Mondex International Ltd., Great Britain**
electronic purse system
http://www.mondex.com/

[Mühlbauer] **Mühlbauer GmbH, Germany**
card production machinery
http://www.muehlbauer.de/

[MUSCLE] **MUSCLE (Movement for the Use of Smart Cards in a Linux Environment)**
MUSCLE project for linking smart cards to Linux systems
http:// www.linuxnet.com/

[NIST] **National Institute of Standards and Technology (NIST), USA**
standards
http://www.nist.gov/

[NSA] **National Security Agency (NSA), USA**
information about security and cryptography
http://www.nsa.gov/

[Oberthur] **Oberthur Smart Cards, USA**
smart card manufacturer
http://www.oberthur.com/

[OCF] **OCF**
OCF specification
http://www.opencard.org/

[Oki] **Oki, Japan**
manufacturer of smart card microcontrollers and terminals
http://www.oki.com/
http://www.oki.co.jp/

[OMA] **Open Mobile Alliance**
successor to the WAP Forum
http://www.openmobilealliance.org

[Omni] **Omnikey**
smart card terminals
http://www.omnikey.com

[Orga] **Orga GmbH, Germany**
smart card manufacturer
http://www.orga.com/

[PC/SC] **PC/SC Working Group, USA**
PC/SC specification
http://www.smartcardsys.com/

[Philips] **Philips, Germany**
manufacturer of smart card microcontrollers
http://www.philips.com/
http://www.semiconductors.philips.com/

[Protechno] **Protechno Card GmbH, Germany**
manufacturer of desktop personalization machinery
http://www.protechno-card.com/

[Proton] **Proton**
Proton electronic purse system
http://www.protonworld.com/

[Radicchio] **Radicchio**
PKI
http:// www.radicchio.org/

[Rankl] **Home page of Wolfgang Rankl**
errata lists for the *Handbuch der Chipkarten*, the *Smart Card Handbook* and the *Smart Card Simulator* (available as HTML documents)
http://www.wrankl.de

[Renesas] **Renesas Technology Corporation, Japan**
smart card microcontrollers, terminals
http://www.renesas.com/

[RFC] **RFC Server**
Internet standards; RFC
http://www.rfc.net/

[RFID] **RFID Handbook**
information about RF ID
http://www.RFID-handbook.de

[RSA] **RSA Inc., USA**
cryptography, PKCS specifications
http://www.rsa.com/

[SCA] **Smart Card Allliance**
information about smart cards
http://www.smartcardallilance.org

[SCARD] **Smart Card Developer Association, USA**
attacks, software
http://www.scard.org/

[SCDK] **Smart Card Developer's Kit**
book
http://www.scdk.com/

[Schlumberger] **Schlumberger Ltd., France**
smart card manufacturer
http://www.slb.com/

[SET] **Secure Electronic Transaction LLC, USA**
SET home page
http://www.setco.org/

[SETEC] **SETEC, Finland**
smart card manufacturer
http://www.setec.fi/

[Siemens] **Siemens, Germany**
smart card operating system
http://www.siemens.com/

[SIM Alliance] **SIM Alliance**
S@T browser
http://www.simalliance.org/

[Smart Card Club] **The Smart Card Club**
http://www.smartcardclub.co.uk/

[Smarttrust] **Smarttrust**
microbrowser technology for smart cards
http://www.smarttrust.com/

[SOSSE] **Simple Operating System for Smartcard Education**
smart card operating system
http://www.mbsks.franken.de/sosse

[STM] **ST Microelectronics, France**
manufacturer of smart card microcontrollers
http://www.st.com/

[Techno Data] **Techno Data, Germany**
magnetic-stripe cards, smart cards
http://www.technodata-ibk.com/

[Teletrust] **Teletrust, Germany**
http://www.teletrust.de/

[TETRA] **TETRA**
information about TETRA
http://www.tetramou.com/

[TI] **Texas Instruments Inc., USA**
semiconductor manufacturer
http://www.ti.com/

[TIA] **Telecommunications Industry Association**
standards
http://www.tiaonline.org/

[TNO] **TNO (Netherlands Organization for Applied Research), The Netherlands**
hardware testing of microcontrollers
http://www.tno.nl/

[Topac] **Topac GmbH**
holograms
http://www.topac.de/

[Ubiq] **UbiQ Inc., USA**
personalization
http://www.ubiqinc.com/

[UCL] **UCL Microelectronics Laboratory, Belgium**
cryptography
http://www.dice.ucl.ac.be/

[UCL-LL] **UCL Microelectronics Laboratory – smart card link list**
link farm
http://www.dice.ucl.ac.be/crypto/card.html

[UMTS Forum] **UMTS Forum**
information about UMTS
http://www.umts-forum.org/

[USB] **USB**
http://www.usb.org/

[Verifone] **Verifone Inc., USA**
terminal manufacturer
http://www.verifone.com/

[Visa] **Visa International, USA**
card issuer
http://www.visa.com/
http://www.visa.de/

[WAP] **WAP Forum**
information about WAP
http://www.wapforum.org/

[Wiley] **John Wiley & Sons, Inc., Great Britain**
publisher (*Smart Card Handbook)*
http://www.wiley.co.uk/

[Zeitcontrol] **Zeitcontrol Cardsystems GmbH, Germany**
smart card manufacturer
http://www.zeitcontrol.de/

16.10 CHARACTERISTIC DATA AND TABLES

16.10.1 ATR interval

Table 16.9 Time interval within which the ATR must be sent following a reset

Clock rate	Minimum time (400 clocks)	Maximum time (40,000 clocks)
1.0000 MHz	0.400 ms	40.000 ms
2.0000 MHz	0.200 ms	20.000 ms
3.0000 MHz	0.133 ms	13.333 ms
3.5712 MHz	0.112 ms	11.201 ms
4.0000 MHz	0.100 ms	10.000 ms
4.9152 MHz	0.081 ms	8.138 ms
5.0000 MHz	0.080 ms	8.000 ms
6.0000 MHz	0.067 ms	6.667 ms
7.0000 MHz	0.057 ms	5.714 ms
8.0000 MHz	0.050 ms	5.000 ms
9.0000 MHz	0.044 ms	4.444 ms
10.0000 MHz	0.040 ms	4.000 ms

16.10.2 ATR parameter conversion tables

The following tables are based on the definition of the ATR parameters CWT and BWT in the ISO/IEC 7816-3 standard. The indicated times are for a clock rate of 3.5712 MHz with various values of the clock rate conversion factor (divider) F.

Table 16.10 CWI/CWT conversion table (all times are based on a 3.5712-MHz clock with D = 1)

		F = 4	F = 8	F = 16	F = 31	F = 93
work etu:		1.120 µs	2.240 µs	4.480 µs	8.681 µs	26.042 µs
CWI	CWT (etu)	CWT (ms)				
0	12	0.013	0.027	0.054	0.104	0.313
1	13	0.015	0.029	0.058	0.113	0.339
2	15	0.017	0.034	0.067	0.130	0.391
3	19	0.021	0.043	0.085	0.165	0.495
4	27	0.030	0.060	0.121	0.234	0.703
5	43	0.048	0.096	0.193	0.373	1.120
6	75	0.084	0.168	0.336	0.651	1.953
7	139	0.156	0.311	0.623	1.207	3.620
8	267	0.299	0.598	1.196	2.318	6.953
9	523	0.586	1.172	2.343	4.540	13.620
10	1,035	1.159	2.319	4.637	8.984	26.953
11	2,059	2.306	4.612	9.225	17.873	53.620
12	4,107	4.600	9.200	18.401	35.651	106.953
13	8,203	9.188	18.376	36.752	71.207	213.620
14	16,395	18.364	36.727	73.454	142.318	426.953
15	32,779	36.715	73.430	146.859	284.540	853.620

Table 16.11 BWI/BWT conversion table (all values are based on a 3.5712-MHz clock with D = 1)

		F = 4	F = 8	F = 16	F = 31	F = 93
work etu:		1.120 µs	2.240 µs	4.480 µs	8.681 µs	26.042 µs
BWI	BWT (ms)	BWT (etu)				
0	100	89,291	44,651	22,331	11,531	3,851
1	200	178,645	89,323	44,661	23,051	7,684
2	400	357,131	178,571	89,291	46,091	15,371
3	800	714,251	357,131	178,571	92,171	30,731
4	1,600	1,428,491	714,251	357,131	184,331	61,451
5	3,200	2,856,971	1,428,491	714,251	368,651	122,891
6	6,400	5,714,005	2,857,003	1,428,501	737,291	245,764
7	12,800	11,427,925	5,713,963	2,856,981	1,474,571	491,524
8	25,600	22,855,765	11,427,883	5,713,941	2,949,131	983,044
9	51,200	45,711,445	22,855,723	11,427,861	5,898,251	1,966,084

16.10.3 Determining the data transmission rate

Table 16.12 Data transmission rate in bit/s for various clock frequencies in MHz with a clock rate conversion factor (F) of 372 and various values of the bit rate adjustment factor (D)

	D = 1	D = 2	D = 4	D = 8	D = 12	D = 16	D = 20	D = 32
F/D	372.00	186.00	93.00	46.50	31.00	23.25	18.60	11.63
Frequency								
1.0000	2,688	5,376	10,753	21,505	32,258	43,011	53,763	86,022
2.0000	5,376	10,753	21,505	43,011	64,516	86,022	107,527	172,043
3.0000	8,065	16,129	32,258	64,516	96,774	129,032	161,290	258,065
3.5712	9,600	19,200	38,400	76,800	115,200	153,600	192,000	307,200
4.0000	10,753	21,505	43,011	86,022	129,032	172,043	215,054	344,086
5.0000	13,441	26,882	53,763	107,527	161,290	215,054	268,817	430,108
6.0000	16,129	32,258	64,516	129,032	193,548	258,065	322,581	516,129
7.0000	18,817	37,634	75,269	150,538	225,806	301,075	376,344	602,151
8.0000	21,505	43,011	86,022	172,043	258,065	344,086	430,108	688,172
9.0000	24,194	48,387	96,774	193,548	290,323	387,097	483,871	774,194
10.0000	26,882	53,763	107,527	215,054	322,581	430,108	537,634	860,215

Table 16.13 Data transmission rate in bit/s for various clock frequencies in MHz with a clock rate conversion factor (F) of 512 and various values of the bit rate adjustment factor (D)

	D = 1	D = 2	D = 4	D = 8	D = 12	D = 16	D = 20	D = 32
F/D	512.00	256.00	128.00	64.00	42.67	32.00	25.60	16.00
Frequency								
1.0000	1,953	3,906	7,813	15,625	23,438	31,250	39,063	62,500
2.0000	3,906	7,813	15,625	31,250	46,875	62,500	78,125	125,000
3.0000	5,859	11,719	23,438	46,875	70,313	93,750	117,188	187,500
3.5712	6,975	13,950	27,900	55,800	83,700	111,600	139,500	223,200
4.0000	7,813	15,625	31,250	62,500	93,750	125,000	156,250	250,000
5.0000	9,766	19,531	39,063	78,125	117,188	156,250	195,313	312,500
6.0000	11,719	23,438	46,875	93,750	140,625	187,500	234,375	375,000
7.0000	13,672	27,344	54,688	109,375	164,063	218,750	273,438	437,500
8.0000	15,625	31,250	62,500	125,000	187,500	250,000	312,500	500,000
9.0000	17,578	35,156	70,313	140,625	210,938	281,250	351,563	562,500
10.0000	19,531	39,063	78,125	156,250	234,375	312,500	390,625	625,000

16.10.4 Sampling times for serial data

Table 16.14 is based on data transmission in compliance with the ISO/IEC 7816-3 standard. The indicated times have been calculated for a clock rate of 3.5712 MHz.

Table 16.14 Serial bit sampling times for data transmission with a divider value of 372

	Start	Lower limit	Midrange	Upper limit	End
Start bit	0 clocks 0.000 µs	112 clocks 31.250 µs	186 clocks 52.083 µs	260 clocks 72.917 µs	372 clocks 104.167 µs
Data bit 1/8	372 clocks 104.167 µs	484 clocks 135.417 µs	558 clocks 156.250 µs	632 clocks 177.083 µs	744 clocks 208.333 µs
Data bit 2/7	744 clocks 208.333 µs	856 clocks 239.583 µs	930 clocks 260.417 µs	1004 clocks 281.250 µs	1116 clocks 312.500 µs
Data bit 3/6	1116 clocks 312.500 µs	1228 clocks 343.750 µs	1302 clocks 364.583 µs	1376 clocks 385.417 µs	1488 clocks 416.667 µs
Data bit 4/5	1488 clocks 416.667 µs	1600 clocks 447.917 µs	1674 clocks 468.750 µs	1748 clocks 489.583 µs	1860 clocks 520.833 µs
Data bit 5/4	1860 clocks 520.833 µs	1972 clocks 552.083 µs	2046 clocks 572.917 µs	2120 clocks 593.750 µs	2232 clocks 625.000 µs
Data bit 6/3	2232 clocks 625.000 µs	2344 clocks 656.250 µs	2418 clocks 677.083 µs	2492 clocks 697.917 µs	2604 clocks 729.167 µs
Data bit 7/2	2604 clocks 729.167 µs	2716 clocks 760.417 µs	2790 clocks 781.250 µs	2864 clocks 802.083 µs	2976 clocks 833.333 µs
Data bit 8/1	2976 clocks 833.333 µs	3088 clocks 864.583 µs	3162 clocks 885.417 µs	3236 clocks 906.250 µs	3348 clocks 937.500 µs
Parity bit	3348 clocks 937.500 µs	3460 clocks 968.750 µs	3534 clocks 989.583 µs	3608 clocks 1010.417 µs	3720 clocks 1041.667 µs
Guard time/ Stop bit 1	3720 clocks 1041.667 µs	3832 clocks 1072.917 µs	3906 clocks 1093.750 µs	3980 clocks 1114.583 µs	4092 clocks 1145.833 µs
Guard time/ Stop bit 2	4092 clocks 1145.833 µs	4204 clocks 1177.083 µs	4278 clocks 1197.917 µs	4352 clocks 1218.750 µs	4464 clocks 1250.000 µs

16.10.5 The most important smart card commands

The following tables list the most important smart card commands with brief descriptions of their functions. These commands are taken from the following standards and specifications: ISO/IEC 7816-4, -7, -8, -9, EMV, GSM (GSM 11.11 & GSM 11.14), UICC (TS 31.111, TS 102.221, TS 102.222, TS 102.223), OP (Open Platform) and EN 1546.

Table 16.15 Summary of important standard smart card commands

Command	Function	INS	Standard
ACTIVATE FILE	Reversibly unblock a file.	'44'	ISO/IEC 7816-9
APPEND RECORD	Insert a new record in a file with a linear fixed structure.	'E2'	ISO/IEC 7816-4
APPLICATION BLOCK	Reversibly block an application.	'1E'	EMV
APPLICATION UNBLOCK	Unblock an application.	'18'	EMV

Table 16.16 (*Cont.*)

ASK RANDOM	Request a random number from the smart card.	'84'	EN 726-3
CHANGE CHV	Change the PIN.	'24'	GSM 11.11
CHANGE REFERENCE DATA	Change the data used for user identification (e.g., a PIN).	'24'	ISO/IEC 7816-8
CLOSE APPLICATION	Reset all attained access condition levels.	'AC'	EN 726-3
CONVERT IEP CURRENCY	Convert currency.	'56'	EN 1546-3
CREATE FILE	Create a new file.	'E0'	ISO/IEC 7816-9
CREATE RECORD	Create a new record in a record-oriented file.	'E2'	EN 726-3
CREDIT IEP	Load the purse (IEP).	'52'	EN 1546-3
CREDIT PSAM	Pay from IEP to the PSAM.	'72'	EN 1546-3
DEACTIVATE FILE	Reversibly block a file.	'04'	ISO/IEC 7816-9
DEBIT IEP	Pay from the purse.	'54'	EN 1546-3
DECREASE	Reduce the value of a counter in a file.	'30'	EN 726-3
DECREASE STAMPED	Reduce the value of a counter in a file that is protected using a cryptographic checksum.	'34'	EN 726-3
DELETE	Delete a uniquely identifiable object (such as a load file, application or key).	'E4'	OP
DELETE FILE	Delete a file.	'E4'	ISO/IEC 7816-9
DISABLE CHV	Disable PIN queries.	'26'	GSM 11.11 EN 726-3
DISABLE VERIFICATION REQUIREMENT	Disable user identification (e.g., PIN queries).	'26'	ISO/IEC 7816-8
ENABLE CHV	Enable PIN queries.	'28'	GSM 11.11 EN 726-3
ENABLE VERIFICATION REQUIREMENT	Enable user identification (e.g., PIN queries).	'28'	ISO/IEC 7816-8
ENVELOPE	Embed a second command in a smart card command.	'C2'	EN 726-3 ISO/IEC 7816-4
ERASE BINARY	Set the content of a file with a transparent structure to the erased state.	'0E'	ISO/IEC 7816-4
EXECUTE	Execute a file.	'AE'	EN 726-3
EXTEND	Extend a file.	'D4'	EN 726-3
EXTERNAL AUTHENTICATE	Authenticate the outside world with respect to the smart card.	'82'	ISO/IEC 7816-4
GENERATE AUTHORISATION CRYPTOGRAM	Generate a signature for a payment transaction.	'AE'	EMV-2
GENERATE PUBLIC KEY PAIR	Generate a key pair for an asymmetric cryptographic algorithm.	'46'	ISO/IEC 7816-8

Table 16.15 (*Cont.*)

GET CHALLENGE	Request a random number from the smart card.	'84'	ISO/IEC 7816-4
GET DATA	Read TLV-coded data objects.	'CA'	ISO/IEC 7816-4
GET PREVIOUS IEP SIGNATURE	Repeat the computation and output of the last signature received IEP.	'5A'	EN 1546-3
GET PREVIOUS PSAM SIGNATURE	Repeat the computation and output of the last signature received from the PSAM.	'86'	EN 1546-3
GET RESPONSE	Request data from the smart card (used with the T = 0 transmission protocol).	'C0'	GSM 11.11 ISO/IEC 7816-4
GET STATUS	Read the life-cycle state information of the card manager, application and load file.	'F2'	OP
GIVE RANDOM	Send a random number to the smart card.	'86'	EN 726-3
INCREASE	Increase the value of a counter in a file.	'32'	GSM 11.11 EN 726-3
INCREASE STAMPED	Increase the value of a counter in a file that is protected using a cryptographic checksum.	'36'	EN 726-3
INITIALIZE IEP	Initialize IEP for a subsequent purse command.	'50'	EN 1546-3
INITIALIZE PSAM	Initialize PSAM for a subsequent purse command.	'70'	EN 1546-3
INITIALIZE PSAM for Offline Collection	Initialize PSAM for offline booking of the amount.	'7C'	EN 1546-3
INITIALIZE PSAM for Online Collection	Initialize PSAM for online booking of the amount.	'76'	EN 1546-3
INITIALIZE PSAM for Update	Initialize PSAM for changing the parameters.	'80'	EN 1546-3
INSTALL	Install an application by invoking various oncard functions of the card manager and/or security domain.	'E6'	OP
INTERNAL AUTHENTICATE	Authenticate the smart card with respect to the outside world.	'88'	ISO/IEC 7816-4
INVALIDATE	Reversibly block a file.	'04'	GSM 11.11 EN 726-3
ISSUER AUTHENTICATE	Verify a signature of the card issuer.	'82'	EMV-2
LOAD	Load an application by transferring the load file.	'E8'	OP
LOAD KEY FILE	Load keys in files using cryptographic protection.	'D8'	EN 726-3
LOCK	Irreversibly block a file.	'76'	EN 726-3
MANAGE CHANNEL	Control the logical channels of a smart card.	'70'	ISO/IEC 7816-4
MANAGE SECURITY ENVIRONMENT	Change the parameters for using cryptographic algorithms in the smart card.	'22'	ISO/IEC 7816-8

Table 16.15 (*Cont.*)

MUTUAL AUTHENTICATE	Mutually authenticate the smart card and the terminal.	'82'	ISO/IEC 7816-8
PERFORM SCQL OPERATION	Execute an SCQL instruction.	'10'	ISO/IEC 7816-7
PERFORM SECURITY OPERATION	Execute a cryptographic algorithm in the smart card.	'2A'	ISO/IEC 7816-8
PERFORM TRANSACTION OPERATION	Execute an SCQL transaction instruction.	'12'	ISO/IEC 7816-7
PERFORM USER OPERATION	Manage users in the context of SCQL.	'14'	ISO/IEC 7816-7
PSAM COLLECT	Execute PSAM online booking of an amount.	'78'	EN 1546-3
PSAM COLLECT Acknowledgement	End PSAM online booking of an amount.	'7A'	EN 1546-3
PSAM COMPLETE	End paying the IEP against the PSAM.	'74'	EN 1546-3
PSAM VERIFY COLLECTION	End PSAM offline booking of an amount.	'7E'	EN 1546-3
PUT DATA	Write TLV-coded data objects.	'DA'	ISO/IEC 7816-4
PUT KEY	Write one or more new keys or replace existing keys.	'D8'	OP
REACTIVATE FILE	Unblock a file.	'44'	ISO/IEC 7816-9
READ BINARY	Read from a file with a transparent structure.	'B0'	GSM 11.11 ISO/IEC 7816-4
READ BINARY STAMPED	Read data from a file with a transparent structure that is secured with a cryptographic checksum.	'B4'	EN 726-3
READ RECORD / READ RECORD(S)	Read data from a file with a record-oriented structure.	'B2'	GSM 11.11 ISO/IEC 7816-4
READ RECORD STAMPED	Read data from a file with a record-oriented structure that is secured with a cryptographic checksum.	'B6'	EN 726-3
REHABILITATE	Unblock a file.	'44'	GSM 11.11 EN 726-3
RESET RETRY COUNTER	Reset an error counter.	'2C'	ISO/IEC 7816-8
RUN GSM ALGORITHM	Execute a GSM-specific cryptographic algorithm.	'88'	GSM 11.11
SEARCH BINARY	Search for a text string in a file with a transparent structure.	'A0'	ISO/IEC 7816-9
SEARCH RECORD	Search for a text string in a file with a record-oriented structure.	'A2'	ISO/IEC 7816-9
SEEK	Search for a text string in a file with a record-oriented structure.	'A2'	GSM 11.11 EN 726-3
SELECT/ SELECT (FILE)	Select a file.	'A4'	GSM 11.11 ISO/IEC 7816-4

Table 16.15 (*Cont.*)

SET STATUS	Write life-cycle state data for the card manager, application and load file.	'F0'	OP
SLEEP	Obsolete command for placing the smart card in a power-saving state.	'FA'	GSM 11.11
STATUS	Read various data from the currently selected file.	'F2'	GSM 11.11 EN 726-3
TERMINATE CARD USAGE	Irreversibly block a smart card.	'FE'	ISO/IEC 7816-9
TERMINATE DF	Irreversibly block a DF.	'E6'	ISO/IEC 7816-9
TERMINATE EF	Irreversibly block an EF.	'E8'	ISO/IEC 7816-9
UNBLOCK CHV	Reset a PIN retry counter that has reached its maximum value.	'2C'	GSM 11.11 EN 726-3
UPDATE BINARY	Write to a file with a transparent structure.	'D6'	GSM 11.11 EN 726-3 ISO/IEC 7816-4
UPDATE IEP PARAMETER	Change the general parameters of a purse.	'58'	EN 1546-3
UPDATE PSAM Parameter (offline)	Modify the parameters in the PSAM (offline).	'84'	EN 1546-3
UPDATE PSAM Parameter (online)	Modify the parameters in the PSAM (online).	'82'	EN 1546-3
UPDATE RECORD	Write to a file with a linear fixed, linear variable or cyclic structure.	'DC'	GSM 11.11 ISO/IEC 7816-4
VERIFY	Verify the transferred data (such as a PIN).	'20'	ISO/IEC 7816-4 EMV-2
VERIFY CHV	Verify the PIN.	'20'	GSM 11.11 EN 726-3
WRITE BINARY	Write to a file with a transparent structure using a logical AND/OR process.	'D0'	EN 726-3 ISO/IEC 7816-4
WRITE RECORD	Write to a file with a record-oriented structure using a logical AND/OR process.	'D2'	EN 726-3 ISO/IEC 7816-4

16.10.6 Summary of utilized instruction bytes

Tables 16.16 through 16.18 identify the INS codes that are used with various class bytes. The odd-numbered codes in the shaded columns cannot be used to encode commands, since the T = 0 transfer protocol uses these codes to control the programming voltage.[75]

[75] See also Section 6.4.2,'The T = 0 transmission protocol'. There is a proposal to revise ISO/IEC 7816-3 to eliminate the possibility of controlling an external programming voltage via the instruction byte in the future

Table 16.16 Summary of the INS byte codes used with a class byte (CLA) of '00' as specified in the ISO/IEC 7816-4, -7, -8 and -9 standards. The suffix number of the corresponding standard is shown for each code that is used

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0y					9										4	
1y	7		7		7											
2y	4		8		8		8		8		8		8			
3y																
4y	9				9		8									
5y																
6y																
7y	4															
8y			4.8		4				4							
9y																
Ay	9		9		4											
By	4		4													
Cy	4		4								4					
Dy	4		4				4				4		4			
Ey	9		4		9		9		9							
Fy															9	

Table 16.17 Summary of the INS byte codes used with a class byte (CLA) of '80' as specified in the EMV, EN 1546 and OP standards. The initial letters of the corresponding standard are shown for each code that is used

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0y																
1y							OP		OP						OP	
2y					OP											
3y																
4y																
5y	EN		EN		EN		EN				EN					
6y																
7y	EN		EN		EN		EN		EN		EN		EN		EN	
8y	EN		EN,		EN		EN									
9y			EMV													
Ay									OP						OP,	
By															EMV	
Cy											OP					
Dy									OP							
Ey					OP		OP									
Fy	OP		OP													

Table 16.18 Summary of the INS byte codes used with a class byte (CLA) of '80' as specified in the GMS 11.11 standard

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0y					X											
1y	X		X		X											
2y	X				X		X		X				X			
3y			X													
4y					X											
5y																
6y																
7y																
8y									X							
9y																
Ay			X		X											
By	X		X													
Cy	X		X													
Dy							X		X							
Ey																
Fy			X								X					

16.10.7 Smart card command coding

Tables 16.19 through 16.24 show the most important codes for some sample smart card commands. For the sake of clarity, it is assumed that neither secure messaging nor logical channel addressing is used. Refer to the ISO/IEC 7816-4 standard for the complete coding of these and other smart card commands.[76]

Table 16.19 Coding of the Case 4 command SELECT FILE, with the principal options

Data element	Code	Remark	
CLA	'00'	Class byte reserved for ISO/IEC 7816 commands without secure messaging.	
INS	'A4'	Instruction byte for SELECT FILE, which is the command for selecting a file (MF, DF or EF).	
P1	...	P1 = '00' ∧ Lc = 0	Select the MF
		P1 = '00' ∧ Lc ≠ 0	Select a file using its FID (FID in DATA)
		P1 = '04'	Select a file using its DF name (DF name in DATA)
		P1 = '08'	Select a file by specifying a FID-based path from the MF (path in DATA)
		P1 = '09'	Select a file by specifying a FID-based path from the currently selected DF (path in DATA)
P2	...	P2 = '00'	Return optional FCI
		P2 = '04'	Return optional FCP
		P2 = '08'	Return optional FMD
Lc	...	Coding described under 'P1'	
DATA	...	Coding described under 'P1'	
Le	Le = 0	Return all data belonging to the selected item.	

[76] See also Section 6.5.1, 'Structure of the command APDU'

Table 16.20 Coding of the Case 2 command READ BINARY as specified by ISO/IEC 7816-4, with the principal options

Data element	Code	Remark	
CLA	'00'	Class byte reserved for ISO/IEC 7816 commands without secure messaging.	
INS	'B0'	Instruction byte for READ BINARY, which is the command for reading data from a file with a transparent structure.	
P1	...	P1.b8 = 0	Read data from the currently selected file using an offset. Offset = (P1.b7 ... P1.b1 || P2)
		P1.b8 = 1	After implicit file selection using a short FID, read data using an offset. Short FID = (P1.b5 ... P1.b1), offset = P2
P2	...	Coding described under 'P1'	
Le	...	Le = 0:	Read all data until the end of the file.
		Le > 0:	Le is the number of bytes to be read.

Table 16.21 Coding of the Case 3 command UPDATE BINARY as specified by ISO/IEC 7816-4, with the principal options

Data element	Code	Remark	
CLA	'00'	Class byte reserved for ISO/IEC 7816 commands without secure messaging.	
INS	'D6'	Instruction byte for UPDATE BINARY, which is the command for writing data to a file with a transparent structure.	
P1	...	P1.b8 = 0	Write data to the currently selected file using an offset. Offset = (P1.b7 ... P1.b1 || P2).
		P1.b8 = 1	After implicit file selection using a short FID, write data using an offset. Short FID = (P1.b5 ... P1.b1), offset = P2.
P2	...	Coding described under 'P1'	
Lc	...	Lc is the number of bytes to be written.	
DATA	...	The bytes to be written, with a length of Lc.	

Table 16.22 Coding of the Case 2 command READ RECORD as specified by ISO/IEC 7816-4, with the principal options

Data element	Code	Remark	
CLA	'00'	Class byte reserved for ISO/IEC 7816 commands without secure messaging.	
INS	'B2'	Instruction byte for READ RECORD, which is the command for reading data from a file with a record-oriented structure.	
P1	...	P1 = 0	Read the current record.
		P1 ≠ 1	Read the record number having the record number or record identifier given in P1.

Table 16.22 (*Cont.*)

P2	...	P2.b8 ... P2.b4 = °00000°	Read data from the currently selected file.
		P2.b8 ... P2.b4 ≠ °00000°	Read data after implicit file selection using a short FID. Short FID = (P1.b8 ... P1.b4)
		P2.b3 ... P2.b1 = °000°	Read the first record, using the record identifier passed via P1.
		P2.b3 ... P2.b1 = °001°	Read the last record, using the record identifier passed via P1.
		P2.b3 ... P2.b1 = °010°	Read the next record, using the record identifier passed via P1.
		P2.b3 ... P2.b1 = °011°	Read the previous record, using the record identifier passed via P1.
		P2.b3 ... P2.b1 = °100° ∧ P1 = 0	Read the current record.
		P2.b3 ... P2.b1 = °100° ∧ P1 ≠ 0	Read the record having the record number given in P1.
		P2.b3 ... P2.b1 = °101°	Read all records from the record number given in P1 until the end of the file.
		P2.b3 ... P2.b1 = °110°	Read all records from the end of the file back to the record number given in P1.
Le	...	Le = 0:	Read all bytes until the end of the record(s).
		Le > 0:	Le is the length of the record(s).

Table 16.23 Coding of the Case 3 command UPDATE RECORD as specified by ISO/IEC 7816-4, with the principal options

Data element	Code	Remark
CLA	'00'	Class byte reserved for ISO/IEC 7816 commands without secure messaging.
INS	'DC'	Instruction byte for UPDATE RECORD, which is the command for writing data to a file with a record-oriented structure.
P1	...	P1 = 0 Write the current record.
		P1 ≠ 0 Write the record having the record number given in P1.
P2	...	P2.b8 ... P2.b4 = °00000° Write data to the currently selected file.
		P2.b8 ... P2.b4 ≠ °00000° Write data following implicit file selection using a short FID. Short FID = (P1.b8 ... P1.b4).
		P2.b3 ... P2.b1 = °000° Write the first record.
		P2.b3 ... P2.b1 = °001° Write the last record.
		P2.b3 ... P2.b1 = °010° Write the next record.
		P2.b3 ... P2.b1 = °011° Write the previous record.
		P2.b3 ... P2.b1 = °100° Write the record having the record number given in P1.
Lc	...	Lc is the length of the record to be written.
DATA	...	The record to be written.

Table 16.24 Coding of the Case 3 command VERIFY as specified by ISO/IEC 7816-4, with the principal options

Data element	Code	Remark	
CLA	'00'	Class byte reserved for ISO/IEC 7816 commands without secure messaging.	
INS	'20'	Instruction byte for VERIFY, which is the command for comparing transferred data to reference data (typically a PIN).	
P1	'00'	—	
P2	...	P2 = '00'	No explicit data is transferred.
		P2.b8 = °0°	Reference data valid for the entire smart card (global reference data) is used.
		P2.b8 = °1°	Reference data valid for one or more specific applications (local reference data) is used.
		P2.b7 || P2.b6 =°00°	RFU bits.
		P2.b5 ... P2.b1	Reference data identification number.
Lc	...	Lc is the length of the transferred comparison value.	
DATA	...	The transferred comparison value (usually a PIN).	

16.10.8 Smart card return codes

The return codes described in Table 16.25 are classified according to the scheme used in the ISO/IEC 7816-4 standard.[77] The following status codes are used:

NP: process completed, normal processing
WP: process completed, warning processing
EE: process aborted, execution error
CE: process aborted, checking error

Table 16.25 Selected standard smart card return codes as specified by ISO/IEC 7816-4

Return code	Status	Meaning	Standard
'61xx'	NP	Command successfully executed; 'xx' bytes of data are available and can be requested using GET RESPONSE.	ISO/IEC 7816-4
'6281'	WP	The returned data may be erroneous.	ISO/IEC 7816-4
'6282'	WP	Fewer bytes than specified by the Le parameter could be read, since the end of the file was encountered first.	ISO/IEC 7816-4
'6283'	WP	The selected file is reversibly blocked (invalidated).	ISO/IEC 7816-4
'6284'	WP	The file control information (FCI) is not structured in accordance with ISO/IEC 7816-4.	ISO/IEC 7816-4
'62xx'	WP	Warning; state of non-volatile memory not changed.	ISO/IEC 7816-4

[77] See also Section 6.5.2, 'Structure of the response APDU'

Table 16.25 (*Cont.*)

'63Cx'	WP	The counter has reached the value 'x' ($0 \leq x \leq 15$) (the exact significance depends on the command).	ISO/IEC 7816-4
'63xx'	WP	Warning; state of non-volatile memory changed.	ISO/IEC 7816-4
'64xx'	EE	Execution error; state of non-volatile memory not changed.	ISO/IEC 7816-4
'6581'	EE	Memory error (e.g. during a write operation).	ISO/IEC 7816-4
'65xx'	EE	Execution error; state of non-volatile memory changed.	ISO/IEC 7816-4
'6700'	CE	Length incorrect.	GSM 11.11 ISO/IEC 7816-4
'67xx' . . . '6Fxx'	CE	Check errors.	ISO/IEC 7816-4
'6800'	CE	Functions in the class byte not supported (general).	ISO/IEC 7816-4
'6881'	CE	Logical channels not supported.	ISO/IEC 7816-4
'6882'	CE	Secure messaging not supported.	ISO/IEC 7816-4
'6900'	CE	Command not allowed (general)	ISO/IEC 7816-4
'6981'	CE	Command incompatible with file structure.	ISO/IEC 7816-4
'6982'	CE	Security state not satisfied.	ISO/IEC 7816-4
'6983'	CE	Authentication method blocked.	ISO/IEC 7816-4
'6984'	CE	Referenced data reversibly blocked (invalidated).	ISO/IEC 7816-4
'6985'	CE	Usage conditions not satisfied.	ISO/IEC 7816-4
'6986'	CE	Command not allowed (no EF selected).	ISO/IEC 7816-4
'6987'	CE	Expected secure messaging data objects missing.	ISO/IEC 7816-4
'6988'	CE	Secure messaging data objects incorrect.	ISO/IEC 7816-4
'6A00'	CE	Incorrect P1 or P2 parameters (general).	ISO/IEC 7816-4
'6A80'	CE	Parameters in the data portion are incorrect.	ISO/IEC 7816-4
'6A81'	CE	Function not supported.	ISO/IEC 7816-4
'6A82'	CE	File not found.	ISO/IEC 7816-4
'6A83'	CE	Record not found.	ISO/IEC 7816-4
'6A84'	CE	Insufficient memory.	ISO/IEC 7816-4
'6A85'	CE	Lc inconsistent with TLV structure	ISO/IEC 7816-4
'6A86'	CE	Incorrect P1or P2 parameter.	ISO/IEC 7816-4
'6A87'	CE	Lc inconsistent with P1 or P2.	ISO/IEC 7816-4
'6A88'	CE	Referenced data not found.	ISO/IEC 7816-4
'6B00'	CE	Parameter 1 or 2 incorrect.	GSM 11.11 ISO/IEC 7816-4
'6Cxx'	CE	Bad length value in Le; 'xx' is the correct length.	ISO/IEC 7816-4
'6D00'	CE	Command (instruction) not supported.	GSM 11.11 ISO/IEC 7816-4
'6E00'	CE	Class not supported.	GSM 11.11 ISO/IEC 7816-4

(*Cont.*)

Table 16.25 (*Cont.*)

'6F00'	CE	Command aborted – more exact diagnosis not possible (e.g., operating system error).	GSM 11.11 ISO/IEC 7816-4
'9000'	NP	Command successfully executed.	GSM 11.11 ISO/IEC 7816-4
'920x'	NP	Writing to EEPROM successful after 'x' attempts.	GSM 11.11
'9210'	CE	Insufficient memory.	GSM 11.11
'9240'	EE	Writing to EEPROM not successful.	GSM 11.11
'9400'	CE	No EF selected.	GSM 11.11
'9402'	CE	Address range exceeded.	GSM 11.11
'9404'	CE	FID not found, record not found or comparison pattern not found.	GSM 11.11
'9408'	CE	Selected file type does not match command.	GSM 11.11
'9802'	CE	No PIN defined.	GSM 11.11
'9804'	CE	Access conditions not satisfied, authentication failed.	GSM 11.11
'9835'	CE	ASK RANDOM or GIVE RANDOM not executed.	GSM 11.11
'9840'	CE	PIN verification not successful.	GSM 11.11
'9850'	CE	INCREASE or DECREASE could not be executed because a limit has been reached.	GSM 11.11
'9Fxx'	NP	Command successfully executed; 'xx' bytes of data are available and can be requested using GET RESPONSE.	GSM 11.11

16.10.9 Selected chips for memory cards

Table 16.26 lists a selection of various types of typical memory chips for smart cards, which makes no claim to being complete or entirely correct. The primary purpose of this table is to give a general idea of the very wide selection of available memory chips. Here we would like to explicitly state that tables of this sort quickly become outdated, due to ongoing technical progress. Current general technical specifications are best obtained directly from the web servers of the various manufacturers, such as Infineon [Infineon], Philips [Philips] and ST Microelectronics [STM]. Similar components are also available from a variety of other manufacturers.

Table 16.26 Summary of selected memory chips for smart cards

Manufacturer/type	Memory capacity		Additional information	
Infineon	ROM:	16 bits	Vcc:	5 V
SLE 4404	PROM:	144 bits	Icc:	3 mA
	EEPROM:	256 bits	W/E cycles:	100,000
			W/E time:	5 ms
			HW:	—

Table 16.26 (*Cont.*)

Infineon SLE 4406S	ROM: PROM: EEPROM:	24 bits 72 bits 32 bits	Vcc: Icc: W/E cycles: W/E time: HW:	5 V 1 mA 100,000 5 ms counter for ≈20,000 units
Infineon SLE 44R35	ROM: PROM: EEPROM:	— — 1 KB	Vcc: Icc: W/E cycles: W/E time: HW:	5 V 3 mA 100,000 2 ms PIN logic for extra write protection, unilateral authentication; for contactless memory cards
Infineon SLE 4442	ROM: PROM: EEPROM:	— 32 bits 256 bytes	Vcc: Icc: W/E cycles: W/E time: HW:	5 V 10 mA 100,000 2.5 ms —
Infineon SLE 5536	ROM: PROM: EEPROM:	24 bits 177 bits 36 bits	Vcc: Icc: W/E cycles: W/E time: HW:	5 V 2.5 mA 100,000 3 ms counter for ≈ 20,000 units, unilateral authentication
Infineon SLE 7736	ROM: PROM: EEPROM:	24 bits 177 bits 36 bits	Vcc: Icc: 1 mA W/E cycles: W/E time: HW:	3–5 V 100,000 3 ms counter for ≈20,000 units
Philips MF1 S70	ROM: PROM: EEPROM:	— — 4 KB	Vcc: Icc: W/E cycles: W/E time: HW:	☹ ☹ 100,000 ☹ 4-byte serial number, unilateral authentication, ISO/IEC 15 443A contactless I/F

(*Cont.*)

Table 16.26 (*Cont.*)

Philips I-Code SLI ICPCB 7960	ROM: PROM: EEPROM:	— — 896 bits	Vcc: Icc: W/E cycles: W/E time: HW:	☹ ☹ ☹ ☹ 8-byte serial number, unilateral authentication, ISO/IEC 15 693 contactless I/F
ST Microelectronics LR 1512	ROM: PROM: EEPROM:	— — 512 bits	W/E cycles: W/E time: HW:	100,000 5 ms ISO/IEC 15 693
ST Microelectronics M35101	ROM: PROM: EEPROM:	— — 2048 bits	W/E cycles: W/E time: HW:	100,000 5 ms ISO/IEC 14 443B
ST Microelectronics ST1335D	ROM: PROM: EEPROM:	16 bits — 272 bits	Vcc: Icc: W/E cycles: W/E time: HW:	5 V 500 µA 500,000 3.5 ms counter for 32,767 units, unilateral authentication

16.10.10 Selected microcontrollers for smart cards

Table 16.27 lists a selection of various types of typical microcontrollers for smart cards, which makes no claim to being complete or entirely correct. The primary purpose of this table is to give a general idea of the wide selection of available smart card microcontrollers. Here we would like to explicitly state that tables of this sort quickly become outdated, due to ongoing technical progress. Current general technical specifications are best obtained directly from the web servers of the various manufacturers, such as Atmel [Atmel], Renesas [Renesas], Infineon [Infineon], Philips [Philips] and ST Microelectronics [STM]. Similar components are also available from a variety of other manufacturers.

The following abbreviations are used in the table:

Vcc:	Supply voltage range
Clock:	Clock frequency range
Icc:	Current consumption of the chip at the stated clock frequency (first value: operating; second value: low-power state with clock; third value: low-power state without clock)
Size (optional):	Die size
Structure:	Minimum structure width on the chip
Page:	EEPROM page size

W/E cyc.: Guaranteed number of write/erase cycles per EEPROM page
W/E time: Cycle time for writing or erasing one EEPROM page
HW: Additional on-chip hardware
Timer: Timer for counting clock cycles
UART: Universal asynchronous receiver/transmitter (hardware-based data transmission)
CRC: CRC processing unit
PLL: Internal clock multiplier (phase-locked loop)
MMU: Memory management unit
RNG: Random number generator
DES: DES accelerator (generally includes triple-DES accelerator)
AES: AES accelerator
RSA: RSA accelerator (generally includes EC accelerator)
☹ No publicly available information for this item

Table 16.27 Summary of selected microcontrollers for smart cards

Manufacturer and type	Memory capacity		Additional information	
Atmel	Flash:	64 kB	CPU:	AVR
AT90	EEPROM:	64 kB	Vcc:	2.7–3.3 V, 4.5–5.5 V
SC6464C	RAM:	3 kB	Clock:	1–10 MHz
			Icc:	☹, ☹
			Size:	24 mm^2
			Structure:	0.35 µm
			EEPROM	
			Page:	1–128 bytes
			W/E cyc.:	500,000
			W/E time:	5 ms
			Flash EEPROM	
			Page:	128 bytes
			W/E cyc.:	500,000
			W/E time:	5 ms
			HW:	RISC CPU, two 16-bit timers, MMU, RNG, DES, RSA
Atmel	Flash:	192 kB	CPU:	AVR
AT90	EEPROM:	64 kB	Vcc:	2.7–3.3 V, 4.5–5.5 V
SC19264RC	RAM:	6 kB	Clock:	1–16 MHz
			Icc:	☹, ☹
			Size:	24 mm^2
			Structure:	0.35 µm
			EEPROM	
			Page:	1–128 bytes
			W/E cyc.:	500,000
			W/E time:	5 ms
			HW:	RISC CPU, two 16-bit timers, UART, CRC, PLL, MMU, RNG, DES, RSA

(*Cont.*)

Table 16.27 (*Cont.*)

Infineon SLE 66C160P	ROM:	64 kB	CPU:	8051 derivative
	EEPROM:	16 kB	Vcc:	2.7–5.5 V
	RAM:	2.3 kB	Clock:	1–10 MHz
			Icc:	☹, ☹
			Structure:	0.25 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	500,000
			W/E time:	4.5 ms
			HW:	Two 16-bit timers, UART, CRC, PLL, MMU, RNG, DES
Infineon SLE 66C640P	ROM:	136 kB	CPU:	8051 derivative
	EEPROM:	64 kB	Vcc:	2.7–5.5 V
	RAM:	4.3 kB	Clock:	1–10 MHz
			Icc:	$\leq$ 10 mA, ☹
			Structure:	0.22 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	500,000
			W/E time:	4.5 ms
			HW:	Two 16-bit timers, UART, CRC, PLL, MMU, RNG
Infineon SLE 66CX642P	ROM:	200 kB	CPU:	8051 derivative
	EEPROM:	64 kB	Vcc:	1.62–5.5 V
	RAM:	4.3 kB	Clock:	1–15 MHz
			Icc:	$\leq$ 10 mA, ☹
			Structure:	0.22 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	500,000
			W/E time:	4.5 ms
			HW:	Two 16-bit timers, UART, CRC, PLL, MMU, RNG, DES, RSA
Infineon SLE 88CX720P	ROM:	240 kB	CPU:	32-bit Infineon 88
	EEPROM:	80 kB	Vcc:	1.62–5.5 V
	RAM:	8 kB	Clock:	1–15 MHz
			Icc:	$\leq$ 30 mA, ☹
			Structure:	0.22 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	500,000
			W/E time:	4.5 ms
			HW:	Two 16-bit timers, UART, CRC, PLL ($\leq$ 55 MHz), MMU, RNG, DES, RSA

Table 16.27 (*Cont.*)

Philips	ROM:	32 kB	CPU:	8051
P8WE6004	EEPROM:	4 kB	Vcc:	2.7–5.5 V
	RAM:	768 bytes	Clock:	1–8 MHz
			Icc:	☹, ☹
			Structure:	0.35 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	100,000
			W/E time:	2 ms/2 ms
			HW:	Two 16-bit timers, UART, RNG, DES
Philips	ROM:	32 kB	CPU:	8051
P8RF6004	EEPROM:	4 kB	Vcc:	2.7–5.5 V
	RAM:	1280 bytes	Clock:	1–8 MHz; 13.56 MHz (for RF)
			Icc:	☹, ☹
			Structure:	0.35 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	100,000
			W/E time:	2 ms/2 ms
			HW:	Two 16-bit timers, UART for ISO/IEC 7816 and ISO/IEC 14 433A, MMU, RNG, DES
Philips	ROM:	64 kB	CPU:	8051
P8RF5016	EEPROM:	16 kB	Vcc:	2.7–5.5 V
	RAM:	2300 bytes	Clock:	1–8 MHz; 13.56 MHz (for RF)
			Icc:	☹, ☹
			Structure:	0.35 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	100,000
			W/E time:	2 ms/2 ms
			HW:	Two 16-bit timers, UART for ISO/IEC 7816 and ISO/IEC 14 433A, MMU, RNG, DES, RSA
Philips	ROM:	208 kB	CPU:	XA2
P16WX064	EEPROM:	64 kB	Vcc:	2.7–5.5 V
	RAM:	7 kB	Clock:	1–6 MHz
	Flash (opt.):	32 kB	Icc:	☹, ☹
			Structure:	0.18 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	100,000
			W/E time:	2 ms/2 ms
			HW:	Two 16-bit timers, UART, CRC, MMU, RNG, DES, RSA

(*Cont.*)

Table 16.27 (*Cont.*)

Philips	ROM:	320 kB	CPU:	MIPS
P9CC160	EEPROM:	64 kB	Vcc:	1.62–5.5 V
	RAM:	7 kB	Clock:	1–6 MHz
	Flash:	96 kB	Icc:	☹, ☹
			Structure:	0.18 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	100,000
			W/E time:	2 ms/2 ms
			HW:	Two 16-bit timers, UART, MMU, RNG, DES, AES, RSA
Renesas	ROM:	32 kB	CPU:	H8
H8/3166	EEPROM:	2.2 kB	Vcc:	2.7–5.5 V
	RAM:	1 kB	Clock:	1–10 MHz
			Icc:	$\leq$ 10 mA, $\leq$ 100 µA
			Structure:	0.35 µm
			EEPROM	
			Page:	32 bytes
			W/E cyc.:	100,000
			W/E time:	3 ms/1.5 ms
			HW:	RNG
Renesas	ROM:	48 kB	CPU:	AE-3
AE350	EEPROM:	32.5 kB	Vcc:	2.7–5.5 V
	RAM:	1280 bytes	Clock:	1–10 MHz
			Icc:	$\leq$ 10 mA, $\leq$ 100 µA
			Structure:	0.35 µm
			EEPROM	
			Page:	64 bytes
			W/E cyc.:	100,000
			W/E time:	3 ms/1.5 ms
			HW:	RNG
Renesas	ROM:	128 kB	CPU:	AE-4
AE45X-B/C	EEPROM:	36 kB	Vcc:	2.7–5.5 V
	RAM:	4.5 kB	Clock:	1–10 MHz
			Icc:	$\leq$ 10 mA, $\leq$ 100 µA
			Structure:	0.35 µm
			EEPROM	
			Page:	64 bytes
			W/E cyc.:	500,000
			W/E time:	3 ms/1.5 ms
			HW:	Two 16-bit timers, UART for ISO/IEC 7816 and ISO/IEC 14 433, PLL, MMU, RNG, DES, RSA

Table 16.27 (*Cont.*)

Renesas AE460	ROM:	96 kB	CPU:	AE-4
	EEPROM:	64.5 kB	Vcc:	2.7–5.5 V
	RAM:	3 kB	Clock:	1–10 MHz
			Icc:	$\leq$ 10 mA,$\leq$ 100 µA
			Structure:	0.35 µm
			EEPROM	
			Page:	128 bytes
			W/E cyc.:	100,000
			W/E time:	3 ms/1.5 ms
			HW:	MMU, RNG, DES
Renesas AE46C	ROM:	196 kB	CPU:	AE-4
	EEPROM:	68 kB	Vcc:	2.7–5.5 V
	RAM:	6.5 kB	Clock:	1–10 MHz
			Icc:	$\leq$ 10 mA, $\leq$ 100 µA
			Structure:	0.35 µm
			EEPROM	
			Page:	128 bytes
			W/E cyc.:	500,000
			W/E time:	3 ms/1.5 ms
			HW:	Two 16-bit timers, UART, PLL, MMU, RNG, DES, RSA
ST Micro ST16SF4x	ROM:	16 kB	CPU:	6805
	EEPROM:		Vcc:	2.7–5.5 V
	1.25/2/4/8/16	kB	Clock:	1–5 MHz
	RAM:	384 bytes	Icc:	☹, ☹
			Structure:	0.7 µm
			EEPROM	
			Page:	1–32 bytes
			W/E cyc.:	300,000
			W/E time:	2.5 ms
			HW:	MMU, RNG
ST Micro ST19RF08	ROM:	32 kB	CPU:	ST7
	EEPROM:	8 kB	Vcc:	2.7–5.5 V
	RAM:	960 bytes	Clock:	1–10 MHz
			Icc:	☹, ☹
			Structure:	0.6 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	100,000
			W/E time:	1 ms
			HW:	One 16-bit timer, UART for ISO/IEC 7816 and ISO/IEC 14 433B, CRC, MMU, RNG, DES

(*Cont.*)

Table 16.27 (*Cont.*)

ST Micro	ROM:	176 kB	CPU:	ST7
ST19WG34	EEPROM:	34 kB	Vcc:	1.6–5.5 V
	RAM:	6 kB	Clock:	1–10 MHz
			Icc:	☹, ☹
			Structure:	0.18 µm
			EEPROM	
			Page:	1–64 bytes
			W/E cyc.:	500,000
			W/E time:	2 ms
			HW:	Three 16-bit timers, CRC, MMU, RNG, DES
ST Micro	ROM:	224 kB	CPU: ST22	
ST22WJ64	EEPROM:	64 kB	Vcc:	2.7–5.5 V
	RAM:	8 kB	Clock:	1–30 MHz
			Icc:	☹, ☹
			Structure:	0.18 µm
			EEPROM	
			Page:	1–128 bytes
			W/E cyc.:	500,000
			W/E time:	4.5 ms
			HW:	Two 16-bit timers, UART, PLL ($\leq$ 30 MHz), MMU, RNG, DES