

15

Appendix

15.1 Glossary

1- μm , 0.8- μm , ... technology

In the manufacturing 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. Currently, the smallest possible structure width is around 0.18–0.25 μm . It is naturally always possible to make structures on the chip that are bigger than the minimum dimension.

μP card

This is another term for a microprocessor card (*qv*).

3DES

See Triple DES.

Acquirer

An entity that sets up and manages the data links and the data exchanges between the operator of a payment system and the individual service providers. The acquirer can combine the individual transactions that it receives, so that the operator payment system receives only collective certificates.

Administrative data

Data that are only used for the management of useful data and that have no other particular significance in an application.

AFNOR

The *Association Française de Normalisation* is a French standards organization based in Paris.

AID (application identifier)

The AID identifies an application in a Smart Card. It is defined in the ISO/IEC 7816-5 standard. A part of the AID can be registered nationally or internationally, in which case it

is reserved for the registered application and is unique in the entire world. The AID consists of two data elements: the RID (registered identifier) and the PIX (proprietary identifier). See also Section 5.6.1, 'File types'.

ANSI

The American National Standards Institute is an American standards organization based in New York.

Application

An application consists of the data, commands, procedures, states, mechanisms and algorithms located within a Smart Card to enable it to be used within the context of a particular system. An application and its associated data are usually located in a dedicated DF directly below the MF.

Application operator

An entity that runs an application on Smart Cards. Generally the same as the application provider.

APDU

An APDU (application protocol data unit) is a software data container that is used to package data so that they can be exchanged between a Smart Card and a terminal. An APDU is converted into a TPDU (transport protocol data unit) by the transmission protocol, and then sent via the serial interface to the Smart Card or the terminal. APDUs can be divided into command APDUs and response APDUs. See also Section 6.5, 'Message Structure: APDUs'.

API

An API (application programming interface) is a meticulously specified software interface within a program that provides third parties with standardized access to the functions of the program.

Applet

An applet is a program written in the Java programming language, which is executed in 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 Smart Card world, applets are sometimes called 'cardlets', and they usually correspond to Smart Card applications.

ASN.1

'Abstract syntax notation 1' is a data description language. It allows data to be clearly defined and presented independent of any particular computer system. ASN.1 is defined by ISO/IEC 8824 and ISO/IEC 8825.

Assembler

An 'assembler' is a program that translates assembly-language program code into machine language that can be executed by a processor. After the assembly process, it is usually necessary to link the resulting code using a linker program. However, the term 'assembler' is also often used as a short form of 'assembly language program code'.

ATR

An ATR (Answer to Reset) is a sequence of bytes sent by a Smart Card in response to a (hardware) reset. It includes various parameters relating to the transmission protocol for the Smart Card, among other things. See also Section 6.2, 'Answer to Reset (ATR)'.

Authentication

The process of proving the genuineness of an entity (such as a Smart Card) by means of a cryptographic procedure. Put simply, authentication amounts to using a fixed 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 carried out is known as 'authorization'. It amounts to giving 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 allowed limit and so on. The payment is then allowed if all checks are satisfactory. An authorization can be achieved by means of the authentication of the entity in question (such as a Smart Card). Put simply, an authorization amounts to giving someone permission to perform some particular action.

Auto-eject reader

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

Background system

Any sort of computer system that looks after the processing and management of data above the level of the terminals.

Bellcore attack

See Differential fault analysis.

Big-endian

See Endianness.

Binary-compatible program code

See Native code.

Black list

A list in a database that marks all cards that are no longer allowed to be used in a particular application.

Blackbox test

A blackbox test is based on the assumption that the entity performing the test has no knowledge of the internal processes, functions and mechanisms of the software to be tested.

Boot loader

A boot loader is a (usually small) program that is used to load other, larger programs, for example via a serial interface. A boot loader is usually used to load the actual program code in a new chip or a new piece of electronic equipment. In many cases, the boot loading process can be carried out only once.

Brute force attack

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

BSI

The German *Bundesamt für Sicherheit in der Informationstechnik* (BSI) was founded in 1990. It is the successor of the German *Zentralstelle für das Chiffrierwissen*. The BSI advises agencies and establishes general conditions for cryptographic applications in Germany. It also offers additional services, including the certification of the security features of computerized data systems.

Buffering

A typical type of attack on magnetic-strip cards. It consists of reading the data from the magnetic strip and writing it back again after it has been modified using the terminal (for example, with an altered value for the retry counter).

Bug fix

Additional program code that remedies a known software error (for example, a 'work around').

Bytecode

Bytecode is the name given to the code that a Java compiler produces from the source code. It is a sort of intermediate code that is executed by the Java Virtual Machine (JVM). Bytecode is standardized by the Sun Corporation.

CAP file

A CAP file (card application file) is the data exchange format used between the Java Offcard Virtual Machine and the Java Oncard Virtual Machine.

Cardlet

See Applet.

Classfile

A classfile stores a Java program that has been compiled (translated into bytecode) along with supplementary information. It is executed by the Java Virtual Machine after it has been loaded.

Card acceptor

An entity with which cards for a particular application can be used. A typical example is a merchant that accepts credit cards for making payments.

Card body

A plastic card that forms an intermediate product in the manufacturing of Smart Cards. It is further processed in subsequent production steps and receives additional functional elements, such as the embedded chip.

Card issuer

An entity that is responsible for issuing cards. With single-application cards, the card issuer is usually also the application provider, but this need not necessarily be the case.

Card manufacturer

An entity that produces card bodies and embeds modules in them.

Card owner

The card owner is the natural or legal person that has legal control over the card, and who can do as he wishes with the card. With credit and debit cards, the card owner is very often the bank that issues the card, and the customers who use the cards are only cardholders.

Cardholder

The cardholder is the person who has the actual right to possess and use the card. The cardholder need not necessarily be the (legal) card owner.

Card possessor

The person who has possession of a card.

Card reader

A device with relatively simple electrical and mechanical construction that can receive Smart Cards and make electrical contact with them. In contrast to a terminal, a card reader does not have a display or a keypad. In spite of the name, card readers usually can also be used to write data to the card.

Card user

The person using a card, who perforce possesses the card, but who need not necessarily be the legal owner of the card.

Cavity

The opening in the card body, usually produced by milling, that receives the implanted chip module.

CCITT

The *Comité Consultatif International Télégraphique et Téléphonique* was an international committee for telephone and telegraph services based in Geneva. It has now taken on more responsibilities and has been renamed as the ITU.

CCS

A CCS is a cryptographic checksum for data that can be used to detect manipulation of the data during storage. If data are protected by a CCS while being transferred, the term MAC (message authentication code) is used.

CEN

The European standards organization *Comité Européen de Normalisation*, located in Brussels, is composed of all national European standards organizations and is the official institution of the European Union for European standardization.

CEPT

The *Conférence Européenne des Postes et Télécommunications* is a European standards organization for the national telecommunications companies.

Certificate

A certificate is a signed public key issued by a trustworthy body that allows the key to be recognized as authentic. The most widely used and best known specification of the structure and coding of certificates is the X.509 standard.

Certification authority (CA)

A certification authority is entity that certifies public keys for digital signatures, which means that it guarantees that they are genuine. It does this by signing the user's public key using its own private key, and if necessary it makes the signed public keys available in a directory. The CA can itself generate the necessary key pairs (private and public).

Chip card

A general term for a card (usually plastic) that contains one or more semiconductor chips. It can be either a memory card or a microprocessor card. In English-speaking countries, the term 'Smart Card' is used instead of 'chip card'.

Clearing

In electronic payment systems, the process of settling the account between the entity that accepts an electronic payment (usually a merchant) and the associated bank.

Clearing system

A computer-based background system that carries out centralized account settlements in an application for electronic payments.

Clock-rate conversion factor

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

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 generally.

Closed purse

An implementation of a closed application for an electronic purse. A closed purse can be used only within the limits of what is allowed by the application operator, and not for general payment transactions.

Cold reset

See Reset.

Combicard

See Dual-interface card.

Command APDU

A command APDU is a command sent from a terminal to a Smart Card. It consists 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. The command APDU is described in detail in Section 6.5.1, 'Structure of the Command APDU'.

Common Criteria

The Common Criteria are a criteria catalog for the evaluation and certification of information technology systems. In the future, they should replace national and international criteria catalogs, such as TCSEC and ITSEC. Version 1.0 of the Common Criteria [www.commoncriteria.org] was published in 1996 by the NIST. Since then, they have been internationally standardized as ISO 15408. The currently valid revision is Version 2.0 of 1998.

Compiler

A compiler is a program that translates a program written in a language such as BASIC or C into machine language that can be executed by a processor. After the compilation process, it is normally necessary to link the code using a linker program.

Completion

Completing the operating system by loading the portion that is located in the EEPROM. This allows the operating system to be modified and adapted after the chips have been manufactured, without requiring the production of a new ROM mask. Identical data are written to each Smart Card during completion, so it is in principle a sort of initialization.

Core foil

See Internal foil.

COS

The designation 'COS' (card operating system) for a Smart Card operating system has taken root throughout the world, and it is frequently seen in product names such as STARCOS, MPCOS and the like. See also Chapter 5, 'Smart Card Operating Systems'.

CRC

A cyclic redundancy check (CRC) is a simple and widely used form of error detection code (EDC) for the protection of data. The CRC must be determined based on an initial value and a divider polynomial before it can be used.

Contactless Smart Card

Card with which energy and data are transferred without contact via electromagnetic fields.

Credit card

A card, with or without a chip, that indicates that the holder has been extended credit, and with which payment takes place some time after the goods or services have been received ('buy now, pay later'). Embossed credit cards are typical examples.

Cryptographic algorithm

A cryptographic algorithm is 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 private (secret) key for decryption.

Debit card

A card, with or without a chip, that indicates that the holder has been extended credit, but with which payment takes place when the goods or services are received ('pay now').

Debugging

Debugging means searching for and eliminating errors, with the objective of detecting and correcting as many errors in a software program as possible. Debugging is normally carried out by software developers, and is not the same thing as testing.

Delamination

Delamination is 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 printing overly large areas between the core and overlay foils with non-thermoplastic ink, such as typically used in offset printing.

Deterministic

A process or procedure is said to be deterministic if it always produces the same results for a given set of initial conditions. The opposite of this is 'probabilistic'.

DF name

The DF name, like the FID, is a characteristic of a DF. It has length of 1–16 bytes. It is used for selecting the DF, and it can contain a registered AID (application identifier) that is 5–16 bytes long and makes the DF internationally unique. See also Section 15.4, ‘Registration Authorities for RIDs’.

DF

A DF (dedicated file) is a directory in the file system of a Smart Card. The root directory (MF) is a type of DF.

Die, dice

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

Differential fault analysis (DFA)

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

Differential cryptoanalysis

Differential cryptoanalysis is a method for computing the value of a secret key by using plaintext–ciphertext pairs with certain differences but the same key. The manner in which these differences propagate with additional DES rounds is analyzed to determine the key.

Digital signature

A digital signature is used to establish the authenticity of an electronic message or document. Digital signatures are usually based on asymmetric cryptographic algorithms, such as the RSA algorithm. The legal validity of digital signatures is regulated by law in many countries (as by the *Signaturgesetz* in Germany, for example). Digital signatures are sometimes referred to as ‘electronic signatures’.

Digital fingerprint

This term is often used to refer to the hash value of a message (e.g. generated using SHA-1).

Divider

A commonly used short form for ‘clock-rate conversion factor’ (qv).

Download

Transferring data from a higher-level system (background or host system) to a lower-level system (e.g. terminal). The opposite of this is ‘upload’.

DRAM

Dynamic random access memory (DRAM) is a type of RAM that has a dynamic structure that requires both a constant power supply and periodic refreshing in order to preserve its contents. DRAM cells are effectively capacitors. DRAM takes up less space on the chip than SRAM and is thus less expensive, but SRAM has a shorter access time.

Dual-interface card

The term 'dual-interface card' refers to a Smart Card that has both contactless and contact-type interfaces for transferring data to and from the card. The term 'combicard' is also used.

Dual-slot cellphone

This refers to a mobile phone that has a second externally accessible contact unit for an ID-1 Smart Card, in addition to the user card (e.g. SIM). With a dual-slot cellphone, it is for example possible to use existing electronic purse Smart Cards with the phone to make payments via the cellular phone network.

Duplicate

This means transferring genuine data to a second card with the objective of producing one or more identical (cloned) cards. 'Duplicate' usually means the same thing as 'clone'.

ECC

An error correction code (ECC) is a checksum for data. With an ECC, errors in the data can be detected with a certain probability, and sometimes also fully corrected. The acronym ECC also stands for 'elliptic curve cryptosystem'.

e-commerce

This is an abbreviation of 'electronic commerce', which refers to all forms of service and trade that utilize public networks (primarily the Internet), as well as the payment traffic based on them.

EDC

An error detection code (EDC) is a checksum for data. With an EDC, errors in the data can be detected with a certain probability. Typical examples of EDCs are the XOR and CRC checksums used in various data transmission protocols.

EEPROM

EEPROM (electrically erasable programmable read-only memory) is a type of non-volatile memory that is used in Smart Cards. An EEPROM is divided into memory pages and its contents can be altered or erased, but there is a physically determined upper limit to the number of write or erase accesses.

EF

EFs (elementary files) represent the actual data storage elements of the file tree of a Smart Card. An EF can have either the property 'working' (for use by the terminal) or the property 'internal' (for use by the Smart Card operating system). An EF has an internal structure (transparent, linear fixed, linear variable, cyclic, ...).

Electronic purse (e-purse)

An electronic purse is a card with a chip that must be loaded with an amount of money before it can be used for making payments ('pay before'). Some typical examples are the German *Geldkarte*, the Visa Cash card and the Mondex card. Electronic purses may also allow purse-to-purse transactions.

Embossing

Part of the physical personalization process, in which raised characters are impressed into the plastic card body so that they stand proud of the surface of the card.

EMV (EMV specification)

General specifications for financial transaction cards with chips and their associated terminals, prepared by Europay, Mastercard and Visa. These specifications have achieved the status of international industry standards for credit and debit cards and electronic purses. In the financial transaction area, they are thus the counterpart to the GSM11.11 telecommunications standard.

Endianness

The term 'endianness' indicates the sequence 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.

EPROM

An EPROM (erasable programmable read-only memory) is a type of non-volatile memory that is now very rarely used in Smart Cards. It can only be erased by ultraviolet light, so it can be used only for WORM storage (write once, read multiple) in Smart Cards.

ETS

European Telecommunication Standard (ETS) refers to standards issued by ETSI. They are primarily concerned with European telecommunications.

ETSI

The European Telecommunications Standards Institute, based in Sophia Antipolis, France, is the standardization body of the European telecommunication companies. It looks after defining standards in the area of European telecommunications. The most important ETSI standard in the area of Smart Cards is the series of GSM standards (GSM 11.11 ff).

etu (elementary time unit)

An elementary time unit is the duration of one bit in a data transfer to a Smart Card. The absolute duration of an etu is not fixed; instead, it is defined in terms of the frequency of the clock signal applied to the card and the clock-rate conversion factor ('divider').

Fault tree analysis

Fault tree analysis refers to a testing method in which every program execution path in the program code is traversed in order to search for possible faults.

FID

The file identifier (FID) is a two-byte characteristic of a file. Each MF, DF and EF has a FID. The FID of the MF is always '3F00'. See also Section 5.6, 'Smart Card Files'.

FIPS

The term 'Federal Information Processing Standard' (FIPS) refers to American standards that are issued by the NIST.

Floor limit

A floor limit relates to the level of a purchase for which authorization by a third party is required. No authorization is necessary below this limit, but authorization must always be obtained for purchases above the limit, since otherwise payment may not be possible and is not guaranteed.

Garbage collection

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

Greybox test

A greybox test is a mixed form that combines elements of blackbox and whitebox tests, in which the entity performing the test knows some of the internal processes, functions and mechanisms of the software to be tested.

GSM

The 'Global System for Mobile Communications' is a specification for an international, terrestrial mobile telephone system. Although originally intended for use in a few countries of central Europe, it has developed into an international standard for mobile telephones. The designated successor of GSM will be UMTS (Universal Mobile Telecommunications System).

Hard mask

The term 'hard mask' means that the complete program code is largely contained in the ROM. This saves space in comparison to a soft mask, since ROM cells are significantly smaller than EEPROM cells. However, it has the disadvantage that an actual exposure mask must be generated for the semiconductor manufacturing process. The turnaround time is thereby increased considerably in comparison with a soft mask. Hard masks are normally used with large numbers of chips for Smart Cards that have largely identical functionality. The opposite of a hard mask is a soft mask, with which essential functions are in EEPROM.

Hash function

A hash function is a procedure for compressing data by means of a one-way function, so that it is not possible to recompute the original data. A hash function produces a fixed-length result for any arbitrary input value, and it is designed so that any change to the input data has a very high probability of effecting the computed hash value (output value). 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.

Hologram

A photographic exposure made using a holographic process is called a hologram. It is 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 that are normally used with Smart Cards are embossed holograms, which produce reasonably satisfactory three-dimensional images.

Hot list

A list in a database that notes all Smart Cards that probably have been manipulated and must not be accepted under any circumstances.

Hybrid card

Refers to a card with two different card technologies. Typical examples are cards with both magnetic strips and chips, or Smart Cards with optical storage layers on their surfaces.

ID-1 card

Standard Smart Card format (length \approx 85.6 mm, width \approx 54 mm, thickness \approx 0.76 mm).

Identification

Procedure for proving the genuineness of a device or a person by comparing a presented password to a stored reference password.

IEC

The International Electrotechnical Commission [IEC] was founded in 1906 and is based in Geneva. Its job is to establish international standards for electrical and electronics technology.

Initializer

A body that performs initialization.

Initialization

Loading the fixed, person-independent data of an application into the EEPROM. A synonym for this is 'pre-personalization'.

Intelligent memory card

A memory card with additional logic circuitry for extra security functions that monitor memory accesses.

Internal foil

An internal foil is one of the foils that is located inside the stack of foils that are laminated together to make a card. It is therefore sometimes also called a 'core foil'. Normally, the internal foil is laminated between two cover foils, and these three foils together form the card. The internal foil often carries security features or electrical components, such as the coils for contactless Smart Cards.

Interpreter

An interpreter is a program that carries out 'run-time' translation of the instructions of a program language such as BASIC or Java into machine language instructions that can be executed by a processor. Each translated instruction is executed immediately upon being translated. An interpreted program always runs more slowly than compiled program code, due to the fact that the translation takes place while the program is running. However, interpreters allow a significantly higher degree of hardware-independent programming than do compilers.

ISO

The International Organisation for Standardisation [ISO] was founded in 1947 and is based in Geneva. Its task is to support the establishment of international standards, in order to enable the free exchange of goods and services. The first ISO standard was published in 1951; it deals with temperatures with regard to length measurements.

ITSEC

The Information Technique System Evaluation Criteria (ITSEC), published in 1991, are a catalog of criteria for the evaluation and certification of the security of information technology systems in Europe. The further development of the ITSEC and its combination with various national criteria resulted in the Common Criteria.

ITU

The International Telecommunications Union (ITU) is an international organization for the coordination, standardization and development of global telephone services, based in Geneva. It is the successor to the CCITT [ITU].

Java

Java is a hardware-independent, object-oriented programming language developed by the Sun Corporation. It is widely used on the Internet. Java source code is translated into a standardized bytecode by a compiler, and the bytecode is then normally interpreted by a 'virtual machine' built on the target hardware (Intel, Motorola, ...) and operating system platform (Windows, MacOS, Unix, ...). There are already processors (such as PicoJava) that can directly execute Java bytecode.

Key fault presentation counter

See Retry counter.

Key management

This refers to all administrative functions relating to the generation, distribution, storage, updating, destruction and addressing of 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 two completely different images, depending on the viewing angle. Kinegrams are similar to holograms, which show three-dimensional images, but not identical to them.

Lamination

The process of gluing together thin sheets of material using heat and pressure.

Laser engraving

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

Linker

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

Little-endian

See Endianness.

Load agent

The load agent is the body that carries out the loading of electronic money into an electronic purse. It is in a manner of speaking the counterpart to the service provider, which can remove money from the purse in exchange for goods or services.

MAC

A MAC (message authentication code) is a cryptographic checksum for data that allows manipulation of the data during the transfer process to be recognized. If a MAC is used to protect stored data, the term CCS (cryptographic checksum) is used instead.

Magnetic card

A commonly used but technically incorrect short form of 'magnetic-strip card'.

Magnetic-strip card

A card with a magnetic strip on which data may be read and subsequently read. The magnetic strip normally holds three data tracks with differing data recording densities. Tracks 1 and 2 are only read after the card has been issued, while data may also be written to track 3 while the card is in normal use. The magnetic material in the strip may have either a high-coercivity characteristic or a low-coercivity characteristic.

Memory card

A card with a chip that has a simple logic circuit with additional memory that can be read and/or written. Memory cards can also have supplementary security logic blocks, which for example can make authentication possible.

MF

The MF, or master file, of a Smart Card file system is a special type of file. It is the root directory of the file tree and is automatically selected when the Smart Card is reset.

Microprocessor card

A microprocessor card is a card with a microcontroller chip, which contains a CPU, volatile memory (RAM) and non-volatile memory (ROM, EEPROM and the like). A

microprocessor card can also contain a numerical coprocessor (NPU) so that it can quickly execute public-key cryptographic algorithms. Cards of this type are sometimes referred to as 'cryptocards' or 'cryptocontroller cards'.

Module

The component that carries and supports a die, with a set of contact elements arranged on its surface, is called a module.

Module manufacturer

An entity that attaches dice to blank modules and produces the electrical connections between the die and the module contacts.

Mono-application Smart Card

A Smart Card that contains only one application.

Monofunctional Smart Card

A monofunctional Smart Card is a processor chip card whose operating system supports only one particular application, and which may even be optimized for this application. Management functions for applications, such as creating and deleting files, are supported either in a very limited form or not at all by such cards.

MoU

The Memorandum of Understanding (MoU) is the common legal basis for all GSM network operators.

Multi-application Smart Card

A multi-application Smart Card is one that contains more than one application, such as a bank card that also has a telephone function.

Multifunctional Smart Card

The term 'multifunctional Smart Card' normally refers to a processor chip card that supports more than one application and that has suitable management functions for loading and deleting applications and files. However, this term is used in such an inflated sense that nowadays there is hardly any Smart Card operating system that cannot be upgraded to be 'multifunctional'. Some humorists like to assert that every card is fundamentally multifunctional, since they all can at least be used to scrape the ice off a frosted windshield.

Multitasking

A computer system that supports multitasking allows several programs to be run quasi-simultaneously. Each of the programs that can be run in parallel is usually located in a separate address space that is protected against access by other programs. The programs that run in parallel can exchange data with each other only by means of special mechanisms. Multitasking is not the same as multithreading, in which a single program performs several different tasks quasi-simultaneously. 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-simultaneously. The individual threads of a program normally utilize a common address space. Multithreading is not the same as multitasking, in which several different programs run in parallel, each with its own separate address space. A computer system may support both multitasking and multithreading.

Native code

Native code means a program whose instructions are in the particular machine language of the processor that executes the program.

NBS

Before 1988, the NIST was known as the National Bureau of Standards (NBS).

NCSC

The American National Computer Security Center (NCSC) is a subagency of the NSA. It is responsible for testing security products, and it publishes criteria for secure computer systems, including the TCSEC.

Negative file

See Black list.

Negative result

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

Nibble

The four most significant or least significant bits of a byte.

NIST

The American National Institute of Standards and Technology (NIST) is a division of the US Department of Commerce and is responsible for the national standardization of information technology. It was known as the NBS until 1988. The NIST publishes the FIPS standards.

Noiseless

A property of a cryptographic algorithm that always takes the same amount of time to encrypt or decrypt data, regardless 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 behavior of the algorithm. This allows the key to be determined significantly faster than with a brute-force attack.

Non-repudiation

The non-repudiability of a message refers to a cryptographic procedure that ensures that the recipient of a message cannot refuse to acknowledge (repudiate) the contents of the message. The sender of the message can thereby prove that the person to whom the

message was sent actually received the message. Non-repudiation is thus equivalent to a registered letter with return receipt in ordinary postal systems.

Non-volatile memory

A type of memory (such as ROM or EEPROM) that retains its contents even without power.

NSA

The American National Security Agency (NSA) is the official US government institution for communication security. It reports directly to the Department of Defense, and one of its functions is to monitor foreign communications and decode them. The development of new cryptographic algorithms and the restriction of the use of existing algorithms also fall under the authority of this agency.

Numbering

Numbering is the process of embossing or printing numbers on a Smart Card. It is typically used in the production of anonymous prepaid phone cards in order to give each card a visible and unique identification number.

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.

Open application

An application in a Smart Card that is available to various service providers (such as merchants and vendors of services) without requiring a mutual legal relationship.

Open purse

The implementation of an open application for an electronic purse. It can be used for general payment transactions with various service providers.

Operating system producer

An entity that programs and tests an operating system.

Optical memory card

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

Padding

Padding means extending a data string with filler data in order to bring the string to a particular length. The length of the resulting string most often must be an integral product of a certain block size (such as 8 bytes) so that it can be further processed, for example by a cryptographic algorithm.

Page-oriented

Refers to memory structures in which a number of bytes are organized into a 'page', which can be written or erased only as a group. In Smart Card microcontrollers, only the EEPROM is page-oriented. The usual size of a memory page is 4 or 32 bytes. However,

nowadays there are microcontrollers that have a page orientation that can vary within certain limits, such as 1–32 bytes, instead of a fixed orientation.

Passivation

A passivation layer is a protective layer on top of a semiconductor chip that protects it against oxidation and other chemical processes. The passivation layer must be removed before the semiconductor can be manipulated.

Patch

In software development terms, a patch is a short program that extends or modifies the behavior of an existing program. It is often written in machine code. Patches are usually used to make quick and uncomplicated corrections to program errors.

Patent

A patent is a document that gives an inventor the right to the exclusive exploitation of his or her invention for a limited amount of time and in one or more countries. The maximum term of a patent is usually 20 years.

Pay before

The expression ‘pay before’ refers to the money flow for cards that are used for payment transactions. The ‘real’ money flows out of the card owner’s account before the goods or services are actually purchased. Typical representatives of ‘pay before’ cards are electronic purse cards, which the user must load with electronic money prior to making a purchase.

Pay later

The expression ‘pay later’ refers to the money flow for cards that are used for payment transactions. The ‘real’ money flows out of the card owner’s account only some time after the goods or services are actually purchased. Typical representatives of ‘pay later’ cards are credit cards, with which it may take up to several weeks after the purchase before the money is transferred from the account of the payer to the account of the merchant.

Pay now

The expression ‘pay later’ refers to the money flow for cards that are used for payment transactions. The ‘real’ money flows out of the card owner’s account at the same time as the goods or services are purchased. Typical representatives of ‘pay now’ cards are debit cards, such as the Eurocheque card, which allow the money to be transferred from the account of the payer to the account of the merchant at the time that the purchase occurs.

Personalizer

An entity that carries out personalization.

Personalization

The process in which a card is assigned to a person. This can take place by means of physical personalization (e.g. embossing or laser engraving) as well as by means of electronic personalization (loading personal data in the memory of the Smart Card).

PIN pad

In its original sense, a PIN pad is a terminal data-entry keypad that has special mechanical and cryptographic protection. In general usage, the entire terminal is often referred to as a PIN pad.

PKCS#1...11

The Public Key Cryptographic Standards (PKCS) are computation rules published by RSA Inc that relate to the use of asymmetric cryptographic algorithms, such as the RSA algorithm.

Plug-in

A Smart Card with a very small format, which is primarily used in GSM phones (length \approx 25 mm, width \approx 15 mm, thickness \approx 0.76 mm).

Polling

Polling is the regular querying or sampling of an input channel under software control in order to detect the content of an incoming message. Depending on the repetition rate of the queries, polling can require a considerable amount of processing power. Normally, interrupt-driven sampling that is supported by the processor hardware is preferred to pure software polling.

POS

POS (point of sale) refers to any location at which a particular item or service is sold.

Positive result

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

Pre-personalization

This is another name for initialization (*qv*).

Processor

The most important subassembly of a microcontroller. It executes the machine instructions in the order defined by the program and performs memory accesses. The term CPU (central processing unit) is often used as a synonym for 'processor'.

Processor card

This is a short form of 'microprocessor card' (*qv*).

Purse holder

A person who possesses a Smart Card containing an electronic purse.

Purse provider

The organization that is 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 the intervention of a third, higher-level system. Normally, this functionality means that the purse system must operate anonymously and that the electronic purses must use a single common key for this function.

RAM (random-access memory)

A type of volatile memory that is used in Smart Cards as working storage. RAM loses its contents in the absence of power. SRAM and DRAM are types of RAM with special technical properties.

Record

A record or set of data is a certain quantity of data that is similar to a string.

Red list

See Hot list.

Reset

A reset means that the computer (in this context, a Smart Card) is restored to a clearly defined initial state. A ‘cold reset’ or ‘power-on reset’ means that the reset is initiated by switching the power off and then on again. A ‘warm reset’ is initiated by a signal on the reset lead of the Smart Card, without affecting the supply voltage.

Response APDU

The Smart Card sends a response APDU as its answer to a command APDU received from a terminal. The response APDU consists of optional response data and a mandatory 2-byte portion containing the status words SW1 and SW2. It is described in detail in Section 6.5, ‘Message Structure: APDUs’.

Retry counter

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

ROM (read-only memory)

A type of non-volatile memory that is used in Smart Cards. It is mainly used to store programs and static data, since the contents of a ROM cannot be altered.

ROM mask

An exposure mask used to produce the ROM in the semiconductor fabrication process. This expression is also used to refer to the data contents of the ROM in a Smart Card microcontroller.

Sandbox

See Virtual machine.

Scrambling

An intentionally confusing layout of the address, data and control busses on a microcontroller chip, so that it is not possible to recognize the functions of individual bus lines without inside information. 'Static' scrambling means that the busses of a given series of chips are all scrambled in the same way. 'Dynamic' scrambling means that the busses are scrambled differently for each different chip.

Secure messaging

A method for protecting data transferred via an interface against manipulation (by means of a MAC, i.e. 'authentic mode') or eavesdropping (by means of encryption, i.e. 'combined mode').

Security module

An assembly that is secured both mechanically and computationally and is used for the storage of secret data. It is also called a secure application module (SAM) or a hardware security module (HSM).

Service provider

A service provider in a Smart Card system is an entity that offers services that are utilized and paid for by a card user. In the case of payment system with electronic purses, a service provider is the entity that receives money from the purse system owner in exchange for his electronic money.

Session

The interval between when the activation and deactivation sequences of a Smart Card, during which both the complete data exchange and the necessary computational mechanisms take place.

SET

The Secure Electronic Transaction (SET) standard is a protocol for payment transactions for carrying out secure credit card payments via the Internet, as defined by Visa and Mastercard. It does not necessarily require the payer to have a Smart Card, since it can be implemented fully in software on a PC. An extension of the SET, called C-SET (Chip-SET), is up to now only relevant inside France and is not yet internationally standardized.

Short FID

A Sort FID is a 5-bit identifier for an EF that can have a value from 1 through 31. It is used within a write or read command (such as READ BINARY) for the implicit selection of an EF.

Shutter

A shutter is a mechanical assembly in a terminal that cuts off any wires leading from the card. This is intended to prevent manipulation of the communications. If it is not possible to cut through any such wires, the inserted circuit card will not be electrically activated.

Signaturgesetz (SigG)

This refers to the German signature law (*Signaturgesetz*), or in full Article 3 of the *Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG)* of 13 June 1997. This legislation prescribes the general conditions for the use of digital signatures in Germany.

Signaturverordnung (SigV)

The German *Signaturverordnung* (signature regulation) of 8 October 1997 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 the generation of 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.

SIM

Subscriber Identity Module (SIM) is another name for a GSM-specific Smart Card. This can be the same size as a standard credit card (ID-1 format), or it can be a small plug-in card in the ID-000 format. The SIM carries the secret authentication data for the network operator and also contains user-specific data, such as the telephone number of the mobile phone (see also Section 13.5, ‘The GXM Network’). The successor to the SIM in the UMTS is the USIM (*qv*).

SIMEG

The Subscriber Identification Module Expert Group (SIMEG) was a group of experts working within the framework of ETSI who defined the specifications for the interface between Smart Cards and mobile telephones (GSM 11.11). The name ‘SIMEG’ was replaced in 1994 by ‘SMG9’.

Smart Card

Strictly speaking, the expression ‘Smart Card’ is an alternative 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 chip cards.

Smartcard

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

SMG9

The Special Mobile Group 9 (SMG9) is a group of experts working within the framework of ETSI who define the specifications of the interface between Smart Cards and mobile telephones (GSM 11.11). It is composed of representatives of card manufacturers, mobile phone manufacturers and network operators. The SMG9 was formerly called the SIMEG.

Soft mask

The term ‘soft mask’ means that part of the program code based on the Smart Card operating system in ROM is located in the EEPROM. Programs in the 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 a program stored in EEPROM. Soft masks are typically used for small numbers of cards (e.g. for field trials) in rapid prototyping. The opposite of a soft mask is a hard mask, with which the essential functions are in the ROM.

Specification

In this book, the work *specification* is used to refer to any document that resembles a standard (*qv*) but which is generated or issued by (for example) a company or an industrial group, rather than by a national or international standardization authority. The terms ‘specification’ and ‘standard’ are sometimes used interchangeably, but this is not actually correct.

SRAM (static random-access memory)

A static RAM needs only a constant supply of power to retain its contents; it does not need to be periodically refreshed. The access time of a SRAM is less than that of a DRAM, but SRAM takes up more space on the chip and is thus more expensive.

Stack

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

Standard

A standard is a document that contains technical descriptions and/or precise criteria that are 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 always used in connection with a national or international standardization authority (such as ISO, CEN, ANSI or ETSI). A standard is not the same as a specification (*qv*).

State machine

A part of a program that determines the course of a process 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 no longer can be recognized 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 that the changes to the image are practically unobservable.

Super Smart Card

The term ‘Super Smart Card’ refers to a Smart Card with integrated complex card elements such as a display and keypad.

TCSEC

The Information Technique System Evaluation Criteria (TCSEC) were published in 1985 by the NCSC. They are a catalog of criteria for the evaluation and certification of the security of information technology systems in the United States. The national TCSEC were followed by the internationally valid Common Criteria.

TDES

See Triple-DES.

Terminal

A terminal is the complement to a Smart Card. It is the device that allows the Smart Card to receive electrical power and exchange data. Some terminals have displays and keypads.

Testing

Testing means checking whether an already debugged program is in good working order. The primary objective of testing is not to look for errors in the program, but rather to check out the expected functions. Testing is thus not the same thing as debugging.

Thread

See Multithreading.

TLV format

A data format conforming to ASN.1, which uses a prefix label (*tag*) and a length code (*length*) to uniquely describe a particular data object (*value*). The TLV format also allows chained data objects.

TPDU

See APDU.

Transaction number

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

Transfer card

A transfer card is a Smart Card that is used as a transport medium to carry data between two entities. It contains a large data memory for this purpose, and it normally contains keys for authenticating whether the data to be transferred are allowed to be read or written by the entity in question.

Transmission protocol

In the Smart Card world, the term ‘transmission protocol’ refers to the mechanisms used to send and receive data between a terminal and a Smart Card. A transmission protocol describes in detail the OSI protocol layers that are used

Transport protocol

An alternate name for transmission protocol (*qv*).

Trap door

A trap door is a mechanism in software or an algorithm that is intentionally included in order to allow security functions or protective mechanisms to be circumvented.

Triple-DES

The Triple-DES algorithm, which is also referred to as TDES and 3 DES, is a modified DES encryption. It consists of calling the DES algorithm three times in succession, with alternating encryption and decryption. If the same key is used for all three DES calls, the Triple-DES encryption corresponds to a normal DES encryption. However, if two or three different keys are used, the Triple-DES encryption is significantly stronger than a single DES encryption. See also Section 4.6.1, 'Symmetric cryptographic algorithms'.

Trojan horse

Historically, this refers to the wooden horse that enabled Odysseus to gain entry into the heavily fortified city of Troy. In modern usage, it refers to a program that performs a specific 'foreground' function but also can execute additional functions unbeknownst 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.

UIM (user identification module)

An outdated term for USIM (*qv*).

Unicode

Unicode is a further refinement of the well known ASCII code for characters. 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. The WWW site of the Unicode consortium is [Unicode].

Upload

'Upload' means to transfer data from a lower-level system (such as a terminal) to a higher-level system (such as a background or host system). It is the opposite of 'download'.

Useful data

Data that are directly needed by an application.

User

A person who uses a Smart Card. This need not necessarily be the cardholder.

USIM

Universal Subscriber Identity Module (USIM) is another name for a UMTS-specific Smart Card. This can be the same size as a standard credit card (ID-1 format), or it can be a small plug-in card in the ID-000 format. The USIM carries the secret authentication data for the

network operator and also contains user-specific data, such as the telephone number of the mobile phone.

Virgin card

A virgin card is one that has not been implanted with a chip and has not yet been optically or electronically personalized. It is essentially a printed, undistinguished card body, such as is made in the mass production of cards.

Virtual machine (VM)

A virtual machine is a microprocessor that is simulated in software. Among other things, it has its own opcodes for machine instructions and a (also simulated) address space. This makes it possible to generate software that is independent of the particular features of specific hardware. For example, the virtual address space of a VM can be many times larger than the actual address space that provided by the hardware. The term 'sandbox' is often used in the Java milieu to refer to the closed environment of the VM.

Visa Easy Entry (VEE)

Visa Easy Entry is a method for simple migration from magnetic-strip credit cards to credit cards with microcontroller chips. It is accomplished by storing the name of the cardholder and all the data from the magnetic strip 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 that are needed for the transaction from the chip instead of from the magnetic strip. The advantage of this approach is that only the POS terminals have to be upgraded to include a Smart Card contact unit, 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.

Warm reset

See Reset.

White list

A database list that notes all Smart Cards that are allowed to be used in a particular application.

Whitebox test

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

Work-around

In software development, a work-around is something that circumvents a known problem by 'programming around' it. A work-around does not eliminate the actual error, but only eliminates its negative effects on the rest of the program. Work-arounds are typically made in the EEPROM portion of mask-programmed Smart Card operating systems, since the program code in the ROM cannot be changed after the chip has been manufactured.

WWW (W3)

The World Wide Web (WWW) is a part of the international Internet. It is best known for its ability to link any desired documents by means of hyperlinks and the integration of multimedia objects in documents.

X.509

The X.509 standard defines the structure and coding of certificates. It is internationally the most commonly used standard for certificate structures.

ZKA

The *Zentraler Kreditausschuß* (ZKA) in Germany is a committee that coordinates the electronic payment procedures 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 chairman of the ZKA is chosen from each of the four member associations in yearly rotation.