Smartex Limited

PO Box 146 Haverhill, CB9 7RL
01440 712610 info@smartex.com www.smartex.com
Registered in England No: 2758219

Glossary

of
terms and expressions used
in the advanced card industry

Updated May 2013

AVAILABLE ONLINE

with acknowledgements to the many sources

Whilst every reasonable effort has been made to make the content of this Glossary as accurate and complete as possible, no responsibility will be accepted for errors and omissions therein.

We are happy to update this Glossary, and to correct inaccurate definitions in later editions.

If you notice errors or omissions, please email these to Richard Poynder (richard@smartex.com).

Expression	Explanation
A	
A3 Algorithm	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 not the same for the entire GSM system.
A5 Algorithm	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	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 not the same for the entire GSM system.
Aadhaar number	An initiative of Unique Identification Authority of India of the Indian government to create a unique ID for every Indian resident. Previously referred to as the UID.
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.
Accounted e-purse	A form of electronic purse in which all transactions are recorded and processed as data records which go through a central acquiring and settlement system.
ACD	Application Carrier Device, usually a smart card.
Acquirer	A member of a payment card scheme (e.g. a bank, but in some countries more likely to be an independent company) which contracts with a merchant (e.g. a retailer) to accept the cards concerned as a means of payment. The acquirer is responsible for checking the data for these card transactions, and for reimbursing the merchant (credit/charge cards) or transmitting the data to a bank or other authorised entity for direct settlement (debit cards and accounted e-purse cards).
Activation	A secure procedure under control of the card/SAM which switches the card/SAM to its active state for normal operation. Alternatively, in the ISO/IEC 7816 standard, specifically the sequence in which electrical power and signals are applied to a card so that the card begins to operate and becomes ready to accept commands.
Advanced electronic signature	A form of **electronic signature** (qv): an electronic signature which meets the following requirements: [a] it is uniquely linked to the signatory; [b] it is capable of identifying the signatory; [c] it is created using means that the signatory can maintain under his sole control; and [d] it is linked to the data to which it relates that any subsequent change of the data is detectable" (Also known as Qualified digital signature and Qualified electronic signature) http://www.symantec.com/connect/articles/digital-signatures-and-european-laws
AES	Advanced Encryption Standard. The USA name for a symmetric encryption standard to replace DES. After a competition, the US Govt based it on the Rijndael (pronounced 'Reindahl') algorithm. See FIPS publication 197 ('FIPS 197') and ISO/IEC 18033-3.
AFC	Automatic Fare Collection, as in public transport. Now expanded to encompass the whole area of journey logging, revenue allocation and subsidy claim, on the basis of accounting for every leg of every journey by making and storing transaction records.
AFNOR	Association Française de Normalisation – the national French standards-making body responsible for the early smart card standards. Historically, when cards were referred to as having chips in the AFNOR position, that meant that the IC (chip) was towards the top left hand corner of the card rather than in the ISO position lower down.

Expression	Explanation
AID	Application Identifier (e.g. in ISO/IEC 7816). 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 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)
Algorithm	A set of rules specifying the procedure to perform a specific computation.
American Express	Amongst other activities, operates the American Express card payment system.
Anonymisation	Modifying person-specific data in such a manner that it is no longer possible to associate the modified data with the original person. (see also **Pseudonymisation**)
ANSI	American National Standards Institute – sets US standards, in particular for IT activities and protocols. Note that there are other US standardisation bodies producing standards and specifications used in the smart card and security industries (IEEE, NIST/NBS), and one company, RSA Labs, produces the PKCS series of security specifications.
ANSI X3	American National Standards Institute X3 – standards committee for smart cards and other machine-readable cards in the USA.
ANSI X9	American National Standards Institute X9 – standards committee for financial services in the USA.
ANSI X12	American National Standards Institute X12 – standards committee for EDI in the USA.
Answer To Reset	See **ATR**
Anti-collision	A method that permits access to multiple contactless cards without interference. 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 recognised.
APACS	Historical term: Association of (UK) Payment Clearing Services. An association of UK banks (the 'clearing banks') which develops and maintains specifications for data exchange and hardware and software products for retail financial services. Particularly involved with UK debit/credit implementation of the EMV smart card and terminal specifications. In 2009, APACS merged into a more general UK bank payments company **UKPA**.
APDU	Application Protocol Data Unit. A message between an IFD (PCD) and an ACD (PICC) (terminal and smart card), as defined in ISO/IEC 7816. The APDU is converted into a transmission protocol data unit (TPDU) by the transmission protocol and then sent by the smart card or terminal via the serial interface.
API	Application Programme Interface. (1) A software interface, specified in detail, that provides access to specific functions of a program. (2) A set of rules (code) and specifications that software programmes can follow to communicate with each other.
App	A smartphone user-facing application
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 smart cards, applets are sometimes called 'cardlets'. In a smart card, an applet usually corresponds to a smart card application.
Application identifier (AID)	Number that uniquely identifies an application in an ISO/IEC 7816 or ISO contactless card. ISO/IEC (SC17) operates a registration scheme for AIDs for microprocessor cards, and there is at least one industry registrar for other card types (for Mifare® family secure memory cards).
Application Programming Interface	See **API**
ASIC	Application Specific Integrated Circuit – an integrated circuit (chip) with special features designed to meet particular requirements. In the smart card context, an ASIC is usually an IC with special cells for functions such as security or communications.
ASK	Amplitude-Shift-Keying is a modulation method in which the amplitude of the carrier wave is switched between two states. Used in contactless smartcards.

Expression	Explanation
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 cryptography	A set of cryptographic techniques in which two different keys (private and public keys) are used for encrypting and decrypting data. The private key is kept secret by its holder while the public key is made available to communicating entities. Also known as public key cryptography and public key infrastructure (PKI).
Asynchronous password generation	A method of generating a unique one-time password for a computer user based on a challenge-response sequence between a host and a device possessed by the user.
ATM	Automated Teller Machine. Colloquially the familiar cash dispensers seen outside (and inside) banks and building societies, and increasingly in other locations. More precisely an electronic device that allows consumers with accounts to perform financial transactions including the withdrawal of cash; generally known as a "hole in the wall" in the UK.
ATM	Asynchronous Transfer Mode – a communications protocol for the transfer of data (any type) across a network.
ATM	Automated Ticket Machine – a vending machine for issuing (usually public transport) tickets. Sometimes encountered as ATVM (Automatic Ticket Vending Machine), as TVM (Ticket vending Machine) or as ETM (Electronic Ticket Machine).
ATOC	Association of Train Operating Companies (ATOC Ltd), to which all UK mainland operators of heavy rail passenger services (but excluding the operators of heritage railways) belong. With its partner **RSP** (Rail Settlement Plan Ltd) makes possible the operation of the UK mainland rail network as a seamless network providing through passenger journeys with one ticket.
ATQA	Answer to request for contactless smart cards of Type A complying with ISO/IEC 14443.
ATQB	Answer to request for contactless smart cards of Type B complying with ISO/IEC 14443.
ATR	Answer To Reset is a sequence of bytes sent by a contact smart card in response to a (hardware) reset. The ATR includes various parameters relating to the transmission protocol for the contact smart card complying with ISO/IEC 7816.
ATS	Counterpart of ATR for contactless smart cards of Type A complying with ISO/IEC 14443.
Audit trail	A sequential record of events that have occurred in a system.
Authentication	The methods used to verify the origin of a message or to verify the identity of a participant connected to a system.
B	
Back office system	Data processing system that processes transactions in the background, i.e. not interacting directly with customers, users or customer service staff.
Barclaycard OnePulse	Combined **Oyster** card, Credit and Cashless payment al in one card. Used in London, UK during 2007, no longer available.
BiBo	Be-In Be-Out, a technology in which the presence of an electronic token is automatically detected when it enters a zone or other enclosure (e.g. a vehicle), is regularly polled after detection, and is assumed to have left the area when it can no longer be detected. In 2007/8 being considered in Switzerland for deployment for public transport ticketing on high density services. Also studied for UK DfT public transport ticketing strategy but not proceeded with. Typically uses HF and UHF technology, but may use 2.5GHz Wi-Fi based technology; the tokens require battery power. The Dresden trial used 6.67MHz at the entry to the vehicle to wake up the token and 868 MHz to detect the continuing presence of the token.
Biometric	A method of authenticating a user by electronically measuring some unique physical characteristic of the user, such as voice pattern, fingerprint, hand geometry, hand blood vessel pattern, signature dynamics or retinal pattern.

Expression	Explanation
Biometric Residence Permit (UK)	A biometric residence permit is a smart card which holds: - your biographic details (your name, and your date and place of birth); - your 'biometric information' (e.g. fingerprints and facial image). For foreign nationals residing in the UK. it also shows your immigration status and your entitlements while you are in the UK.
Bit	A binary digit, either 0 or 1.
Bitcoin	An alternative currency, completely decentralised (no controlling financial institution or central organisation; no fiduciary backing) and internet based.
Bit width of CPU: 8-bit/16-bit/32-bit	An important characteristic with regard to the processing power of a microprocessor (CPU) is the width of the register and data paths for data to be processed in the processing unit. It is expressed in terms of the number of bits.
BlackBerry	Smartphone from RIM (Research In Motion), notable for being bundled with secure network functions for encrypted communication.
Black list	A list in a database identifying all cards or devices that are no longer allowed to be used in a particular scheme or application. By extension, may be applied to any list containing the authorised members of a larger set (e.g. currencies) and to components of a card based system (e.g. AIDs, ticket Products). The term **Hot list** is also used. See also **White list**.
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.
Border Agency (UK)	Until end March 2013, an executive agency of the UK Home Office. Its executive status has been removed, and it is being split into two new organisations, one for the visa system and the other for immigration law enforcement.
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 on a high end SIM and are thus Smartcard WebServers.
Brute-force attack	A method of cryptanalysis in which every possible cryptographic key is tried. Often called ‘Exhaustive Search’.
BSI	British Standards Institution – a body responsible for the development of UK standards, and for UK participation in European and international standards. Smartex is a member of the BSI.
BSI IST/17	BSI committee responsible for ‘Identification Cards and Related Devices’, and representing the UK on ISO/IEC JTC1/SC17 and CEN TC224 and TC278 via delegates and 'experts'.
BSI	Bundesamt for Sicherheit in der Informationstechnik (www.BSI.de) is the German Federal Security agency. 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. It also advises manufacturers, operators and users with regard to IT security, and certifies according to Common Criteria the security of smart card hardware and software.
Buffering	The process of copying card data to an intermediate store and restoring it to the card at some later point in time. Generally, but not exclusively, applied to some forms of (stored value) magnetic stripe card fraud. The most common closed system defence is to track the current value of the card in a central computer. Open systems generally employ some kind of irreversible process - punching holes in the card for example, or switching so-called 'ES' bits on Watermark Magnetics™ cards. Hence closed systems frequently recharge/recycle cards; open systems do so rarely (see also **Skimming**).
Bullet-proof write	See **Persistent write**
Byte	A series of 8 bits, sufficient in length to represent a character set with 256 members.
B2B	Business to Business
B2C	Business to Consumer
C	

Expression	Explanation
CAD	Card Accepting Device – a key component in reader/writer terminals and the mechanism into which a contact smart card is inserted or near or onto which a contactless card is placed.
CAFÉ project	(Historical) Conditional Access for Europe – an EC-funded project to develop an electronic wallet to be used as a Pan-European device for consumer payments, access to information services and, if required, identification. The project concluded with a trial on the payment device in 1995.
Card	General term used to refer to a thin rectangular piece of non-metallic material with rounded corners whose physical dimensions comply with an international standard. A card can have various card components such as magnetic strip, signature strip, laser engraving, surface printing, embossing, etc, but is not considered "smart" unless an Integrated Circuit is present. Normally assumed to conform to one of two of the sizes defined in ISO/IEC 7810: **ID-1** for a credit card size device, or **ID-000** for a SIM card size device.
Card blocking	See **Locking**.
Card Holder	A natural or legal person having use of a card, often the customer, consumer or user of service to which the card holds their entitlement.
CHV	CardHolderValue, a designation for the 3 digit number found on the rear of EMV payment cards, and used for online transactions.
Card Issuer	The entity responsible for personalisation and distribution of cards for a particular application, and, in the case of multi-application card platforms, responsible for loading and deleting third party applications. Also takes legal and managerial responsibility for the card throughout its life. Uses a **CMS**.
Card Management System	System used by a card issuer to hold a database of information about a population of smart cards and other smart devices and optionally execute associated card management transactions.
Card Manufacturer	An entity that produces card bodies in which it embeds modules and may add other card features (aerial coil for contactless interface, surface printing, magnetic stripe, signature panel, possibly keypad, battery and electronic display).
Card Not Present (CNP)	A card payment via mail order, telephone or online where the retailer cannot see the physical card.
Card Personaliser	An entity that adds Personalisation after manufacture of the card.
Card unblocking	The reverse procedure to locking a card. Also known as rehabilitation.
Cartes Bancaires	The French financial payment card association, primarily operating a debit card scheme. Its smart cards for many years famously ran the B0' (B nought prime) application, with the contact area or stamp in the AFNOR position, but (1998) CB declared its intention to migrate to the EMV specification. Allied to Visa, but operates independently, recognising both Eurocard/Mastercard and Visa cards.
CCDA	Common cardholder data application
CEN	Comité Européen de Normalisation: European Committee for Standardisation. The UK is represented by the British Standards Institution (BSI). National standards bodies of Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden and Switzerland are also CEN members. See references to specific EN/ENV standards.
CEPS	Common Electronic Purse Specification; a mainly European accounted purse specification, using public key cryptography, intended to replace many of the pre-existing contact smart card accounted e-purses with an interoperable purse. Existing brands were expected to continue alongside the interoperability CEPS brand, but in practice e-purse cards to the specification were not rolled out and by end 2007 bank-specified contactless accounted payment cards were being rolled out (e.g. Visa Wave and MasterCard PayPass)
Central repository	Government department or agency set up by Government, which acts as a point of contact for interfacing between a Trusted Third Party (TTP) and the appropriate law enforcement agency.
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 recognised as authentic by third parties (see **PKI**). The most widely used and best-known specification for the structure and coding of certificates is the X.509 standard.

Expression	Explanation
Certificate Revocation List (CRL)	A list, held by a directory service, that identifies all certificates within a PKI based system that are blocked and no longer accepted.
Certification	Of equipment and cards: see **Type approval**.
Certification Authority (CA)	An entity entrusted with creating and assigning public key certificates. Sometimes referred to as Certificate Authority.
Challenge-response	A means of authentication in which a device replies in a predetermined way to a challenge from another device, thus proving its authenticity.
Charge card	Similar to a credit card, but (a) without a limit on the amount of credit, and (b) with a commitment by the cardholder to repay on a fixed date (usually monthly) the amounts charged.
Checksum	A control procedure used by applications in verifying the integrity of a string of data. The numeric values represented by the data bytes are summed using a predetermined algorithm to create the Checksum. See also **CRC**, **ECC**.
Chip	A small, usually rectangular, piece of thin semiconductor material (aka a die) – usually silicon – which has been chemically processed to contain a specific set of electronic characteristics such as analogue circuits, storage elements or logic elements. (Sometimes confused with **Chip Module**, qv) The Chip size, measured in millimetres, has a functional relationship to the cost of a chip, and is limited by chip module construction. The physical robustness of the chip is inversely proportional to its size.
Chipper	Electronic purse scheme run by the Dutch Postbank, with other partners. Now discontinued.
Chip card	Also known as an IC (integrated circuit) card (ICC) or Smart Card. A card containing one or more integrated circuits (chips) for identification, data storage or special-purpose processing. May be personalised and used to attest to the identity of natural or legal persons, validate personal identification numbers (PINs), authorise purchases, store electronic money or similar tokens, verify account balances, store personal records, etc.
Chip Knip	Dutch bank-owned e-purse scheme, based on licence to use Proton technology.
Chip Module	A carrier and support for a die. A contact chip module has a set of 6 or 8 electrically isolated contact plates arranged on its surface. A contactless chip module has two contact plates to attach to the antenna of an inlay. When embedded in a smart card, the surface contact plates are visible, the connection to the aerial coil is not visible. A dual interface module has both sets of contact plates. The short form 'module' is frequently used to refer to the chip module.
Chip-on-board	See **COB**
Ciphertext	The encrypted form of data (also known as encrypted text).
CISC	Complex Instruction Set Computer. A synchronous (clocked) CPU in which the instruction set is extended by combining many machine cycles so as to perform complex functions, with each function invoked by one operation code (opcode, machine instruction). See **RISC**.
Clearing	The process of transmitting, reconciling and, in some cases, confirming payment orders prior to settlement, possibly including netting of instructions and the establishment of final positions for settlement. Sometimes the term is used (imprecisely) to include settlement.
Clearing System	A set of procedures whereby financial institutions present and exchange data and/or documents relating to funds or securities transfer to other financial institutions. The procedures often also include a mechanism for the calculation of participants' bilateral and/or multilateral net positions with a view to facilitating the settlement of their obligation on a net basis.
Clip	An e-purse brand owned by Europay. Was expected to be implemented as a CEPS compliant e-purse from Europay (using technology developed by Proton), but not deployed (and Europay has been absorbed into MasterCard).
Clone	A card which has had its data copied from another
Closed e-purse scheme	Strictly, an e-purse scheme in which there is only one issuer of the tokens stored in the e-purse, so that they all have to be redeemed by returning them to that issuer. By extension, frequently also means a scheme in which the tokens are used only under control of the issuer or the issuer's associates (e.g. a transport e-purse used only to purchase tickets and associated goods and services, such as refreshments and newspapers).

Expression	Explanation
Cloud computing	Provision of remote computing services via an outsourced environment. Typically presents the user with the functionality and user interface otherwise implemented in the desktop environment.
CM	(ITSO) **Customer Media** (qv)
CMD	(ITSO) **Customer Media Definition** (qv)
CMOS	Complementary Metal Oxide Silicon – a chip technology giving moderate to high performance with extremely low power consumption.
CMS	See **Card Management System**
CNP	See **Card Not Present**
COB	Chip-on-board, where the silicon chip (die) is mounted directly on a printed circuit substrate (PCB), and the bond wires from the chip contact pads are bonded at their other end directly to contact points on the PCB (instead of the chip being mounted on a lead frame and encapsulated in a plastic or other protective cover). The external contact or 'stamp' area is on one side of a very thin PCB, with the chip bonded to the other side.
Collection	The process of transferring data or transactions either from load devices to the purse provider host or from purchase devices to purse provider hosts via acquirers.
Combi card	Generally used to describe a smart card with one or two chips, associated with the result being a dual-interface card (contact and contactless interface). (Currently most dual interface cards, e.g. bank cards, use only a single chip.)
Combined Authority	Type of English Local Authority formed by the merger of the PTE or ITA and the local highway authority, with devolved responsibility for transport related funds.
Common Criteria	The Common Criteria for Information Technology Security Evaluation. A criteria catalogue for the development and evaluation of information technology systems, which is intended to replace national and international criteria catalogues. The Common Criteria were first published in 1996 by the **NIST** organisation (USA) and have been internationally standardized as ISO 15408. Hence Target of Evaluation (ToE), Protection Profile (PP), Security target (ST), Security Functional Requirements (SFRs), Security Assurance Requirements (SARs), Evaluation Assurance Level (EAL). http://en.wikipedia.org/wiki/Common_Criteria
Compatible	Complies with or implements sufficient of the mandatory features of a standard or specification to be interchangeable and/or inter-operable with standard devices within (stated) limits.
Compiler	A program that translates a program written in a language such as "C" or Python 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 to other code bodies using a linker program.
Compliant (or conforming)	Complies with or implements the mandatory features of a standard or specification. 'Fully compliant' means that all mandatory requirements in the standard or specification are met. Selective compliance may be encountered, where only certain parts of the standard are used, perhaps for ease of manufacture or to achieve a result that is, to some defined degree, compatible with the standard or specification.
Concessions scheme	In ticketing (e.g. for public transport), an agreement under which certain tickets or 'permissions to use' a service are issued at reduced or nil cost to the holder. Hence concessionary ticket and ticket scheme, concessionary travel permit or pass, concessionary entitlement. See **ENCTS** for England; there are equivalent schemes for Scotland and Wales.
Conformance testing	Testing to verify that a device conforms to, or complies with, the requirements of a given standard. For example, testing a Proximity card purporting to conform to the Type A requirements of ISO/IEC 14443. Note that, where there are options in a standard, conformance only requires the implementation of one set of options.
Congestion charging	A road user charging scheme, in which tolls are varied according to the actual or expected degree of congestion of the road system. Expected to use smart cards for vehicle ID and payment (but the London scheme currently uses vehicle number plate recognition via cameras).

Expression	Explanation
Contact card	A smart card with a visible module cover (the 'stamp' or contact plate, usually gold or palladium plated) which has six or eight electrical contact points which are used to transfer power and control signals to the card and transfer information to and from the card. Contact cards may be memory only, ASIC, or microprocessor.
Contactless card	A smart card with no visible module contact area, but which transfers data using RF technology. Such cards are generally used for transport and ID applications. They usually obtain their power from a magnetic field generated by the terminal or CAD, but may be powered by an integral battery. Data is transferred by modulation of the RF field. See **Proximity card** (**ISO/IEC 14443**) and **Vicinity card** (**ISO/IEC 15693**); there is also a Close-coupled card standard (**ISO/IEC 10536**), but no evidence of its use
Contactless News	USA journal, delivering weekly news emails free of charge. http://www.contactlessnews.com/
Coupler	Device between the electronic and logical interface of the card and host computer or intermediate microprocessor. Typically, for a contact card, the slot with electrical contacts into which the card is inserted.
CPU	Central Processing Unit: area of a computer system (and of most IC cards) that performs computations.
CRC	Cyclic Redundancy Check. A particular form of Checksum which, under some circumstances, may be used to correct errors in data transmission as well as detect them. See also **ECC**.
Credit card	A card indicating that the holder has been granted a line of credit. It enables the holder to make purchases and/or withdraw cash up to a prearranged ceiling; the credit granted can be settled in full by the end of a specified period or can be settled in part, with the balance taken as extended credit. Interest is charged on the amount of any extended credit and the holder is sometimes charged an annual fee. In the American jargon: 'Pay Later'.
Credit card company	A company which owns the trademark of a particular credit card brand, and which may also provide a number of marketing, processing or other services to institutions issuing its credit card. The term became somewhat dated with the advent of debit and purse cards.
Credit institution	The definition given to a "bank" in the European Union. The First EC Banking Directive defines it as an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account.
Cryptanalysis	Area of Cryptography dedicated to studying and developing methods by which, without prior knowledge of the cryptographic key, plaintext may be deduced from cipher text.
CRYPTO-GRAM	A free monthly newsletter providing summaries, analyses, insights, and commentaries on security: computer and otherwise, by Bruce Schneier, Chief Security Technology Officer, BT (and author). http://www.schneier.com/crypto-gram.html Also 'Schneier on Security' blog http://www.schneier.com/blog .
Cryptographic algorithm	A mathematical function used in combination with a key that is applied to data to ensure confidentiality, data integrity and/or authentication. Also called a cipher.
Cryptographic key	A parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.
Cryptography	The application of mathematical theory to develop techniques and algorithms that can be applied to data to assure goals such as confidentiality, data integrity and/or authentication.
CSP	Communication Services Provider
Customer Media (CM)	(**ITSO**) The smart device which interacts with payment or ticketing. It is usually a smartcard but could be a smart-enabled mobile phone or key fob or other approved format.
Customer Media Definition (CMD)	(**ITSO**) Customer Media Definition: describes the mapping of the logical Data Elements onto a (defined) physical **CM** platform.
CVC	Card Verification Code. See **CVV**.
CVM	Cardholder Verification Method (CVM) is the process to confirm Card Holder authorisation for a particular transaction. This usually consists of **PIN** testing, or **CVC** or **CVV** verification, but biometric user identification may be used in more sophisticated systems.

Expression	Explanation
CVV	Card Verification Value, a 3 digit number routinely used for cardholder verification during transactions featuring "card not present" at the physical point of sale (e.g. online payment where card data is entered into a web browser, or payment over the phone) in the EMV payment environment. Normally printed at the right hand end of the signature panel on the reverse side of an EMV card.
D	
Danmønt	A Danish originated accounted e-purse scheme, originally using disposable cards but later developed to use rechargeable cards. The parent of several accounted e-purse technologies, including some variants of Visa Cash.
DDOS	See **Distributed Denial of Service**
Deactivation	A secure procedure under control of the card/SAM issuer, switching a card or a SAM from its active life state to permanently disabled state which only allows unprotected data to be read. Alternatively, in the ISO/IEC 7816 standard, specifically the sequence in which electrical power and signals are removed from a card so that the card ceases to operate.
Debit Card	A card enabling the holder to have purchases directly charged against funds on a current banking account. In the American jargon: 'Pay Now'.
Decryption	The use of cryptographic algorithms to decode encrypted data so that it can be read by the recipient.
Depot processor or Depot system	In public transport, the computer system in the transport depot that collects transaction records from a vehicle and updates the vehicle's database. Such transfers may be direct (e.g. by wireless LAN) or indirect (e.g. via a driver's data module or by means of portable equipment temporarily connected to the vehicle). In an ITSO-compliant scheme, a depot processor is transparent to the messages.
Depository Institution	The definition given to a "bank" in the United States. Under the Depository Deregulation and Monetary Control Act all depository institutions, including commercial banks, savings and loan associations, mutual savings banks and credit unions, are authorised to issue demand or time deposits to individuals and non-profit organisations.
Derived Key	A cryptographic key that is obtained by using an arithmetic function in combination with a master key and a unique identification value such as a card serial number. AKA Key diversification, Diversified keys.
DES	Data Encryption Standard – a **symmetric** cryptographic algorithm (ANSI standard X3.92) that is widely used, in particular within the financial sector. EMV refers to ISO 8731-1 (DEA). See also **Triple DES** (3DES**)**. Since 2007 slowly being superseded by the stronger **AES**.
DESFire	A proprietary contactless card family based on ISO 14443 type A and using a security protocol (using 3DES/AES). The brand and IP is owned by NXP and is incorporated into various smart card chips and reader ICs. Several card IC suppliers have licences from NXP to incorporate DESFire in USIMs and other chips. The ITSO Specification includes a format definition for use of the original DESFire product (and the EV1 product used in legacy mode) as CMD 7. http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_desfire/
Designed to	Generally conforming to the design philosophy of a standard or specification, but without any guarantee of compatibility or compliance
DF	Dedicated File, used to define a (permanent) directory within a smart card filing system according to ISO/IEC 7816 Part 4. The **MF** is the root directory and is a special type of DF.
DfT	Department for Transport. UK government department. Now at: https://www.gov.uk/government/organisations/department-for-transport
Digital Fingerprint	A commonly used designation for the hash value of a message (e.g. as generated using the SHA-1 algorithm).
Digital Signature	A string of data generated from the data (usually text) of a message by an asymmetric cryptographic method. The signature is attached to the message to ensure its authenticity as well as to protect the recipient against repudiation by the sender. See **Electronic signature**.
Digital wallet	See **Electronic wallet**

Expression	Explanation
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, or a set of access rights to a service or location as part of the provisioning process during card issuance and usage.
Disintermediation	The voluntary exclusion, in an Electronic Purse System, by a Purse Provider of participation in, or mandatory registration of, value transfers between purse cards. The Mondex and MintChip products are examples of this. Also used more widely to describe the devolving by one party (typically a bank) of functions to another organisation of a different type.
Distributed Denial of Service	An attempt to make a computer resource unavailable to its intended users, normally by overloading its input with messages and/or commands from multiple sources.
Diversified keys	A set of derived cryptographic keys, all generated from a single master key, using the same algorithm. Typically a card's serial number will be used in the algorithm.
Differential Power Analysis (DPA)	Differential Power Analysis (DPA) is a method of attacking smart cards that involves first making repeated measurements of the current consumption of its microcontroller for certain operations using known data. The method requires high time resolution and elimination of random noise by averaging. Following this, the current consumption is measured when the card is using unknown data, and conclusions regarding the unknown data are then drawn by analysing 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.
Domain Name System (DNS)	A hierarchical distributed naming system for computers, services or any resource connected to the internet or a private network
DRAM	Dynamic Random Access Memory – standard computer memory which loses its contents on removal of power or removal of clock signals. Not used in smart cards.
Driver and Vehicle Licensing Agency	UK agency of DfT (DVLA) that issues driving licences, vehicle identity documents, etc. Not currently issuing smart cards, but is fully equipped to do that, and already personalises them for other sections of government.
DSA	Digital Signature Algorithm – a US Government standard.
DSS	Digital Signature System – a type of asymmetric encryption/decryption system used for remote authentication of data.
Dual-distance card	Smart card with both a very short range contactless interface capability (usually compliant with the Proximity standard ISO/IEC 14443) and a longer range contactless interface capability (usually compliant with the Vicinity standard ISO/IEC 15693). Sometimes referred to as a Hybrid Card.
Dual-Interface card	Smart card with both a contact interface (compliant with ISO/IEC 7816 and/or EMV) and a contactless interface (normally compliant with ISO/IEC 14443 and/or Contactless EMV).
DVLA	See **Driver and Vehicle Licensing Agency**
E	
e-Banking	Banking services where a customer of a financial institution can access the service using a phone, television, terminal or personal computer as a telecommunication link to the institution's network.
ECC	Error Correcting Code – a combination of bits resulting from a calculation under a set of given rules used to detect and correct errors.
ECC	European Citizen Card specification, developed by CEN TC 224 as PD CEN/TS 15480 (published 2012, multi-part). Initially defined for use in electronic travel documents within the Schengen group of EU countries, but the scope has expanded to include eID functions for on-line transactions between the citizen and public administrations. Initial deployment is expected to be for **eResident** functions, with full deployment delayed until 2015.
EDI	Electronic Data Interchange.
EDIFACT	EDI for Administration, Commerce and Trade – EDI standard ISO 9375, initially developed by the United Nations, combining UN/GTDI and ANSI X12.

Expression	Explanation
EEPROM (E^2PROM)	Electrically Erasable Programmable Read-Only Memory – similar to battery-backed SRAM, but truly non-volatile with no power needed to retain the data. Write/erase capability is generally rated only for 100,000 cycles, so the need for frequent updates can be a problem. Special memory management techniques can be used to extend this lifetime.
eESC	eEurope Smart Cards Charter (2003), the proposal for the Open Smart Card Infrastructure for Europe (OSCIE) and part of the eEurope initiative. Output from the programme may be found at www.iosis.org.uk .
eEurope	The M Prodi 'Initiative' from the EC, started in late 1999, to harmonise the methods of secure access to electronically provided services across Europe. More colloquially, a drive for interoperability, particularly in the use of smart cards and PKI security services. One of the outputs was **eESC**.
EF	Elementary File; used to define a file within a smart card filing system according to ISO/IEC 7816 Part 4.
EFTPoS	Electronic Funds Transfer at Point of Sale. Usually involves the use of debit or credit cards in the retail environment.
eID	Electronic representation of identity data. Often held in a smart card (thus eID card), more recently held in a chip in a passport (see **ICAO** and **ICAO Document 9303**).
Electronic Money (e-money)	(1) Monetary value measured in currency units stored in electronic form in an electronic device in a consumer's possession (an **e-purse**) or in a computer system. (2) Fiduciary backed virtual currency usable in peer-to-peer transactions over a number of channels. The electronic value can be purchased by the consumer and held in secure storage, and is reduced whenever the consumer uses the device or system to make purchases. This contrasts with traditional electronic payment transactions such as those with debit or credit cards which often require on-line authorisation and involve the debiting of the consumer's account after the transaction. There are two different types of store of value: prepaid secure storage held by the consumer (cards or other secure devices such as mobile devices hosting a secure element) and prepaid software products. With prepaid devices, the electronic value is stored in a chip (integrated circuit) embedded in the device, and value is typically transferred by presenting the device (inserting a card in a card reader or using a mobile phone app). With software products, the electronic value is stored on the hard disk of a computer and is transferred over communication networks such as the Internet when payments are made. See **Accounted e-purse, CEPS, Chip Knip, Clip, Danmønt, Modeus, Mondex, Proton, Visa Cash, MintChip, EMI**. For a scheme without fiduciary backing see **Bitcoin**.
Electronic Money Institution (EMI)	An organisation issuing **Electronic Money** and holding an Electronic Money Institution Licence (EMIL) under EU rules.
Electronic purse (e-purse)	Typically an IC card containing an application that stores a record of funds available to be spent or otherwise used by the holder; the record of funds is updated as transactions are made. Additional funds may be added to the stored balance through a withdrawal from a bank account or by other means. Sometimes referred to also as a stored value card. See **Closed** and **Open e-purse** schemes.

Expression	Explanation
Electronic signature	As defined in EU Directive 93/1999: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. It uses asymmetrical key cryptography. It is used for authentication, to be sure the person who sent the text is the electronic signature's holder, however you can't be sure she is also the key owner. A key holder is an entity that has the practical use of the electronic signature, whereas the key owner is the person who has the explicit right to use it. (http://www.symantec.com/connect/articles/digital-signatures-and-european-laws) See also **Advanced electronic signature**.
Electronic wallet	(1) A computer device used in some electronic money systems, which can contain an IC card or in which IC cards can be inserted and which may perform more functions than an IC card. (2) In the smartphone environment used more generally to describe a function in the smartphone for securely holding a record of funds and/or a token (such as debit or credit card functionality) and/or other secure data such as tickets. Transactions may be possible over the mobile phone network or using other channels (e.g. **NFC**, WiFi). The data being secured is expected to be held in a **Secure Element** in the device. Also referred to as a Digital wallet.
Elliptic curve	A set of algorithms for asymmetric cryptography, based on the properties of mathematical curve functions. More efficient than RSA algorithms (i.e. requires less computing power for the same level of security). Used for securing mobile phone messages (GSM), but not yet accepted for mainstream financial schemes.
EMV	(1) Originally a joint working group set up in December 1993 by Europay International, MasterCard International and Visa International, to develop a common set of technical specifications for the use of IC cards by the payment industry. Responsibility for the specification has now passed to a management company, EMVCo LLC (www.emvco.com), so that EMV is now used to refer to the group of specifications produced by that company. The core EMV specification for contact interface cards is currently (Apr 2013) at V4.3, and the newer contactless interface specification is at V2.3 (Apr 2013). (2) Europay, MasterCard and Visa. A standard for Integrated Circuit Cards and their interaction with POS terminals.
EMVCo	The company, EMVCo LLC (www.emvco.com) jointly set up in 1999 by Europay International, MasterCard International and Visa International to manage the development of the EMV set of smart card and related specifications.
EMV Migration Forum	Formed in 2012 by the **Smart Card Alliance**: “To join the payments ecosystem together as the United States moves to a new way to pay with EMV chip cards”
EN	Prefix to reference number for CEN standards. Standards having this prefix automatically become national standards of CEN Member nations.
EN 726	CEN standard intended to be used to modify ISO/IEC 7816 for the particular technical environment of portable battery operated equipment (e.g. mobile phones), but largely ignored as ETSI provides a complete set of specifications for the mobile phone environment.
EN 1332	A multi-part CEN standard for the user interface to ICT systems and schemes (e.g. EN 1332-4 Coding of User Profiles for people with special needs). See www.tiresias.org, www.rnib.org.uk, and also ISO/IEC 12905 and **SNAPI**.
EN 1545	CEN multi-part standard defining a basic data model for transport telematics and public transport ticketing applications.
EN 1546	CEN standard for Inter-sector Electronic Purse, largely overtaken by the commercial CEPS specification (but CEPS contains much of the EN 1546 design), and by 2007 falling into disuse.
EN 15320	Interoperable Public Transport Application Framework (working title IOPTA). Describes data structures in electronic tickets and the functions used with them.
Encryption	The use of cryptographic algorithms to encode clear text data (plaintext) into ciphertext to prevent unauthorised observation.

Expression	Explanation
Encryption algorithm	A mathematical function used in the process of encryption.
English National Concessionary Travel Scheme (ENCTS)	**DfT** scheme that provides free off-peak travel on local bus services throughout England for elderly and disabled residents. Started April 2008. Enables the issuing of ITSO-compliant smart cards to authorise travel. Provides the framework by which Local Authorities in England issue and record the use of concessionary passes for travel on local bus services, and then use journey data as the basis for payment to bus operators. Similar schemes operate in Scotland and in Wales.
End to end	Typically used to describe a type of transmission protocol that ensures information is transferred directly from the originator to the recipient, and confirmation of transmission is immediately returned to the originator. Used, for example, in Mondex card-to-card value transfer. (The opposite of **Store and forward** transmission.)
Entitlement Card (Scotland)	The National Entitlement Card Programme in Scotland issues smart cards at local govt level, combining travel concessions and entitlement to multiple citizen benefits under one brand with multi-function cards. http://www.entitlementcard.org.uk/
ENV	Prefix to reference number for CEN voluntary standards, by 2007 replaced by **prEN** designation.
ePassport	A travel document with a contactless chip incorporated, compliant with ISO 14443. Defined in ICAO 9303 document.
Electronic Product Code (EPC)	A universal identifier that potentially provides a unique identity for every type of physical object anywhere in the world. Generally used in the retail environment.
EPoS	Electronic Point of Sale. Usually a description of retail store till systems that can process debit/credit and/or e-purse transactions as well as accepting cash, paper cheques and paper vouchers.
EPROM	Electrically Programmable Read-Only Memory: an area of an IC used to store data, in which data may only be written once and cannot be erased selectively. Usually found in a form that can be bulk erased by exposure to ultra-violet light. In the version where the encapsulation of the chip prevents exposure to UV, known as One Time Programmable ROM (OTP-ROM).
eResident Card	Smart card for use as an electronic ID Card by third country nationals resident in EU countries. Uses ICAO 9303 as a basis for its design.
ETM	Electronic Ticket Machine (e.g. used on public transport)
ETSI	European Telecommunications Standards Institute. ETSI card specifications are based on ISO standards where published, but ETSI has taken the liberty of diverging from ISO in detail. Source of GSM (mobile phone), UMTS (next generation mobile phone) and TE9 (operating system) specifications.
eURI	See **Extended User-Related Information**.
Eurosmart	EUROSMART is an international not-for-profit association, located in Brussels, which represents the voice of the Smart Security Industry for multi-sector applications. Created 1995. http://www.eurosmart.com/
Europay	Previous name for MasterCard's European operation. Europay International SA, a payment systems organisation, headquartered in Belgium, worked in association with MasterCard to operate the MasterCard card payment system in Europe, was an association owned by its members, the banks. In 2002 it was absorbed into **MasterCard International**.
EU-IFM Project	Integrated Fare Management for transport http://www.ifm-project.eu/. See **IFM** (standard)
Evaluation Assurance Level	See **Common Criteria**.
Exhaustive search	See Brute-force attack
Exit charging	Process in public transport ticketing by which a passenger is charged the appropriate fare (or refunded the balance where the maximum fare for the route has been charged on entry) when getting off (leaving, exiting) the vehicle or 'paid area' of a terminal.
ExpressCard	Expansion card format, primarily for laptops. Replaced the PC Card and PCMCIA formats.

Expression	Explanation
Extended User-Related Information	CEN/ISSS Workshop Agreement (CWA 13987 multi-part) defining a dataset for holding personal data in a smart card or similar token, along with guidelines for setting up a Smart Card Community. From 2007 being incorporated into the European Citizen Card development (ECC). By 2011 provided the background to ISO/IEC 12905.
F	
Fab	A semiconductor fabrication facility.
False Accept Rate (FAR)	Percentage of occasions an invalid user is incorrectly accepted for a service as in the erroneous acceptance of invalid users by biometric methods. Typically used in card acceptance for EFTPoS or ATM transactions. Also known as Type 2 error.
False Reject Rate (FRR)	Percentage of occasions a valid user is rejected for a service as in the erroneous rejection of valid users by biometric methods. Typically used in card acceptance for EFTPoS or ATM transactions. Also known as Type 1 error.
FASTEST	CEN Workshop Agreement (CWA 14893 multi-part) Facilitating Smart Card Technology for Electronic Ticketing and Seamless Travel. Outcome of **eESC** with respect to Public Transport.
Felica	A proprietary variant of the contactless card communications ISO14443 protocol invented and owned by Sony, used extensively in Japan for payment and transport applications.
File Identifier (FID)	A two-byte attribute of a file in an ISO compliant smart card. Each MF, DF and EF has a FID. The FID of the MF is always '3F00'. Sometimes known as the File Tag.
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.
File Type	Identifies the sort of file for purposes of file management within a smart card: a directory file (MF or DF), or a file for storing user data (EF).
Financial Services Authority (FSA)	Was responsible for the Electronic Money Regulations, but in 2013 replaced by the Financial Conduct Authority (www.fca.org.uk) and the Prudential Regulation Authority (a wholly owned subsidiary of the Bank of England).
FIPPs	Fair Information Practice Principles
FIPS	USA Federal Information Processing Standard, as issued by NIST. FIPS compliance is normally certified only for complete designs, e.g. a card not the chip.
Firewall	A hardware and/or software system which is used between a public network (such as the Internet) and the application execution environment of a computer system or private network thereof, to monitor and filter incoming and outgoing communications.
Flash Card	A card, smart or otherwise, used to authenticate the user by means of a photo printed on the card.
Flash (memory)	A type of memory based on a modified single transistor EPROM cell technology which offers all the usual reliability attributes of EPROM, but is in-system electrically erasable and writeable on a whole chip or sector basis.
Float	The value of funds loaded, but as yet unspent or unclaimed, in Electronic Purse cards and systems. Float values are reflected as a liability in the accounts of the purse provider, but may also be used (with restrictions) by the purse provider to earn interest or, in some cases, to finance the purse provider's own business. Derived from the use of float in traditional retail till systems, where the float is the sum of notes and coins held in the till at the start of a sales session.
Floor Limit	Defines the level at which a purchase, or other transaction, must be authorized by a third party. Authorization is not required below the floor limit, but it must always be obtained above the floor limit, as otherwise the transaction may not be possible or guaranteed.
Fondleslab	Slang term for tablet computer using touchscreen technology.
FRAM	Ferroelectric RAM (patented by Racom): system using memory cells containing a layer of crystals of zirconium/titanium, oxygen, and lead which form a tiny transistor. FRAM is said to be 20,000 times faster than Flash memory and costs 25% less than battery-backed SRAM. A difficult technology to manufacture and make reliable, but some smart card products use it.

Expression	Explanation
G	
Global Platform	(1) A set of specifications for interoperability and security in the use of smart cards and more recently of terminals, particularly in a transaction based environment; also an industry organisation owning those specifications, providing training courses and supporting test and certification services. Largely developed in the USA. (2) From http://www.globalplatform.org/ : A cross industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. Its proven technical specifications are regarded as the international industry standard for building a trusted end-to-end solution which serves multiple actors and supports several business models.
GPS	Nothing to do with smart cards: the Global Positioning System, a network of low orbit satellites run by the US military, by means of which special receivers can determine their position on the surface of the earth. Galileo is the developing EU equivalent, and the Soviets have their own system.
Granularity	A frequently used alternative term for expressing the page size of an EEPROM or flash memory which can be written to or erased at one time. For example an EEPROM with a granularity of 32 has a page size of 32 bytes.
GSM	Global System for Mobile communications (originally Groupe Systemes Mobile); the standard originally adopted by 18 European countries in order to develop compatible digital mobile telecommunications, and now adopted in some 100 countries, with the notable exception of the USA. However, the USA adopted a modified version of GSM, and there are now tri-band phones which can work on the GSM system (900 MHz band), the PCM system (1800 MHz band) and the USA system (1900 MHz band). Sometimes known as 2G. (The designations of the successors to GSM are 3G, 4G and LTE.)
GUI	Graphical User Interface.
Guilloches	Decorative patterns of interwoven lines, usually circular or oval, found on many banknotes and some Identity cards. Due to their fine structures, these patterns can only be reproduced at high quality using printing techniques, so they are difficult to copy.
H	
Hash	A hash function is a procedure for compressing data using a one-way function so that it is not possible to determine the original data. The 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.
Hex	Hexadecimal notation where numbers are represented in base-16 (i.e. 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F).
HLOS	High Level Output Strategy, UK Office of Rail Regulation document defining the govt's requirement for heavy rail services. In August 2012 the 2014-19 requirement was published at http://www.rail-reg.gov.uk/ . (Ticketing technology is not included, but instead is found in tender documents for rail franchises, **DfT** strategy documents, and programmes such as **SEFT**; also see **ITSO**.)
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. Holograms are often impressed on the surface of a smart card, normally by an embossing process which produces reasonably satisfactory three-dimensional images under normal lighting conditions.
Home Banking	A retail customer's version of **e-banking** (qv).

Expression	Explanation
HOPS or IHOPS	ITSO Host Operator or Processing System. That element of the back office system covering among other functions message handling, Shell and Product accounting, and optional Asset Management functions. Accepts ITSO format transaction messages, verifies and archives them, forwards them to business level systems either directly or via another HOPS, and (optionally, through an Asset Management component) manages an estate of terminals: ITSO **POSTs**, typically ticketing equipment for public transport.
Hot list	A list - held by a merchant terminal or other device - of suspicious items, including but not limited to card numbers or ranges of suspicious card numbers. The hot list is used to detect and to block any transactions with such items. By extension, may be applied to any list containing the authorised members of a larger set (e.g. currencies) and to components of a card based system (e.g. AIDs, ticket Products). The term **Black list** is also used. See also **White list**.
Hybrid card	A card containing both a contact smart chip and another machine-readable interface – normally a contactless interface. Sometimes used to describe a smart card that also has a mag stripe data area on its reverse side.
I	
IAAC	See **Information Assurance Advisory Council**
IAID	ISO AID (see **AID**)
ibutton	A proprietary technology, owned by Dallas Semiconductor, in which a contactless card IC and antenna coil are packaged in a button-shaped rugged case.
IC card (ICC)	Integrated Circuit Card – a plastic card in which one or more integrated circuits are embedded. Also known as a chip card or smart card (although the latter expression is sometimes held by purists to refer only to cards containing chips with microprocessors).
ICAO	International Civil Aviation Organisation. Based in Canada.
ICAO Document 9303	Specification dual 'badged' with ISO 7501: technical specification for machine-readable passports. Has been upgraded to include contactless chip technology, compliant with ISO/IEC 14443 but in a passport book format.
ID	Identifier – alphanumeric value which uniquely identifies the card/holder.
ID-000	The typical size and shape of the small card often used as the SIM in a mobile phone. Defined in ENV1375-1 and ETSI specifications; more recently in ISO/IEC 7810. Smaller sizes (micro-SIM) are also defined.
ID-1	The size and shape of the standard credit card. Defined in ISO/IEC 7810.
Identity Assurance	(1) In the context of Federated Identity Management, is the ability for a party to determine, with some level of certainty, that an electronic credential representing an entity - whether a human or a machine, with which it interacts to effect a transaction, can be trusted to actually belong to the entity. (2) In the case where the entity is a person, is the level at which a credential being presented can be trusted to be a proxy for the individual to whom it was issued and not someone else. (3) A UK govt programme (Cabinet Office) to build a UK identity eco-system for the Govt Digital Service.
Identity Ecosystem	Standards and policies for authoritative authentication in cyberspace (USA: see **NSTIC** www.nist.gov). Hence USA Identity Ecosystem Steering Group (IDESG) http://www.idecosystem.org/
IdM	Identity Management (now widely termed Identity Assurance, qv).
IEC	International Electro-technical Commission, an international body responsible jointly with ISO for developing certain classes of technical standards (see ISO/IEC **JTC1**).
IEE	Institution of Electrical Engineers (see IET)
IEEE	Institute of Electrical and Electronic Engineers (USA)
IEP	Intersector Electronic Purse – a smart card application to store and manipulate electronic value according to the proposed CEN standard. It was not expected to be implemented in this form, but the IEP standard influenced the CEPS commercial specification; however, this technology has largely been superseded by contactless EMV technology.

Expression	Explanation
IET	Institution of Engineering and Technology (incorporates IEE)
IFD	Interface device into which a contact IC card is inserted, or near which a contactless IC card is positioned in order to make use of the card. Also known as a Card Accepting Device (CAD).
IFM	Integrated Fare Management: international standard EN ISO 24014-1. Part 2 is under development. http://www.ifm-project.eu/ (EU-IFM Project)
IHOPS	See **HOPS**
IIN	See **Issuer Identification Number**
ILOG	**ITSO** Licensed Operators Group
Information Assurance	An overview concept, which grew out of Information Security to embrace the entire management of risk in the use, processing, storage and transmission of information or data and in associated systems and processes. Analogue and physical formats as well as digital formats are included. Incorporates Identity Assurance.
Information Assurance Advisory Council (IAAC)	"Our mission is to advance Information Assurance to ensure that the UK's Information Society has a robust, resilient and secure foundation. Further, we intend that users of digital products and services should be confident these are safe and secure for them, their families and their businesses." www.iaac.org.uk Operates as a UK 'Community of Interest', runs Workshops (FOC) and an Annual Symposium. Contact info@iaac.org.uk or 01793 417453 to be considered for addition to the Community of Interest distribution list.
Initialisation	The process of loading the fixed, person-independent data of a smart card application into the card's non-volatile memory. A synonym for initialisation is 'pre-personalisation'.
Inlay	(1) A process by which the chip module that includes the contact area ('stamp') is inserted into a smart card body. (2) A plastic foil assembly incorporating a smart card chip and aerial coil which is laminated into a three layer smart card (two outer hard plastic layers and the inlay).
Instruction Set	Set of commands executed by a CPU. By extension, set of commands accepted by an interpreter program in a computer system.
Insult Rate	Percentage of occasions a valid user is rejected for a service as in the erroneous rejection of valid users by biometric methods. Typically used in card acceptance for EFTPoS or ATM transactions. Also known as False Reject Rate (FRR) or Type 1 error.
Integrated Transport Authority (ITA)	A new (2008) type of UK public sector organisation for oversight and partial management of transport services and infrastructure, as an enhanced replacement for **PTAs**, with additional areas of England and Wales being permitted to apply for ITA status. Several non-PTE areas have been considering applying for ITA status, and South Hampshire is believed to have attained it, while Greater Bristol's 4 UAs have failed to reach agreement. See also the later **Combined Authority**.
Internet	An open, world-wide communication infrastructure consisting of interconnected computer networks which allows access to remote information and the exchange of information between computers. Most links use TCP/IP control protocols.
Internet of things	Autonomous devices connected to the internet. Generally used in the context of devices such as electrical power meters that automatically report energy usage across the internet (using wireless or power line transmission methods) and may also receive commands via the same route.
Interoperability	The ability of systems to provide services to, and accept services from, other systems, and to use the services so exchanged to enable them to operate effectively together. When used in relation to ticketing systems in public transport, interoperability means the provision for the passenger of a seamless journey using the same ICC and/or terminals, on all contractually participating operators' routes.
IOPTA	See **EN 15320**
iOS	Operating system used in Apple's iPhones
IPE	ITSO Product Entity. The electronic form of a ticket or other function such as entitlement, i.e. the data structure used within the ITSO Shell to store formatting and other product details.

Expression	Explanation
iPhone	Brand name for Apple's smartphone (related names such as iPad and iOS are also Apple brands).
IPS	The UK Identity and Passport Service (Home Office executive agency), now at https://www.gov.uk/government/organisations/identity-and-passport-service
ISAM	ITSO Secure Application Module, a SIM size secure electronic data processing module installed in all ITSO compliant equipment used in ITSO compliant ticketing schemes for UK mainland public transport. It is used to check the card holder's permissions, authenticate and validate their electronic ticket, and store journey data for further processing.
ISL	(Historic) ITSO Services Ltd, which was funded by DfT to provide start-up back office (HOPS) services to Local Authorities, primarily in conjunction with the **ENCTS** (English National Concessionary Travel Scheme on public transport). The contract ceased in September 2012. Services provided by ISL have been transferred to other HOPS systems, some of which were funded by DfT to be available as regional service providers in England (e.g. South Gloucestershire Unitary Authority operates the HOPS for Greater Bristol and some other South West LAs).
ISMS	**ITSO** Security Management Service. The lead part of the ITSO security sub system which acts as the 'keeper of the keys', managing the provision of data access keys to the secure devices (**ISAM**s) in equipment such as ticketing machines and barriers or gates.
ISO	International Standards Organisation (or International Organisation for Standardisation); an international body, based in Geneva, whose members are national standards bodies and which approves, develops and publishes international standards. The UK is represented by the British Standards Institution (BSI). See JTC1. See also references to specific ISO/IEC standards.
ISO/IEC JTC1	Joint Technical Committee No 1. A committee formed jointly by ISO and IEC to oversee the development and maintenance of IT standards (see subcommittee ISO/IEC JTC1 SC17 for smart cards).
ISO/IEC JTC1/SC17	The subcommittee of ISO/IEC JTC1 that manages the development of international standards for machine readable cards, including smart cards, and has widened its scope to include IFDs or CADs (card terminals)
ISO 7501	Specification dual 'badged' with ICAO Document 9303: technical specification for machine-readable passports. Has been upgraded to include contactless chip technology, compliant with ISO/IEC 14443 but in a passport book format.
ISO/IEC 7816	Main (ISO/IEC) standard, initially for contact smart cards, but sections higher than part 4 also apply to contactless cards and therefore to operation through the contactless interface of dual interface (contact plus contactless) cards.
ISO/IEC 10373	Main (ISO/IEC) standard for test methods for machine readable cards, including magnetic stripe and smart cards, and associated IFDs.
ISO/IEC 10536	Main (ISO/IEC) standard for Close-coupled contactless smart cards (typical operating distance up to about 1 cm from the terminal's antenna). Not currently in common use but close-coupled operation is the subject of increasing interest for financial applications.
ISO/IEC 12905	Integrated circuit cards – Enhanced terminal accessibility using cardholder preference interface. Standardises methods for assisting users with special needs.
ISO/IEC 14443	Main (ISO/IEC) standard for Proximity contactless cards (typical operating distance up to 10 cm from the terminal or PCD's antenna coil) with a carrier frequency of 13.56MHz. Two modulation methods, A and B, are defined (hence Type A and Type B cards, with Type A being by far the most common usage).
ISO/IEC 15693	Main (ISO/IEC) standard for Vicinity contactless cards (typical operating distance up to 30 cm from the terminal's antenna coil).
ISO 24014-1	Part 1 of the Integrated Fare Management (**IFM**) standard, for a set of networked ticketing schemes (e.g. for public transport) within a single security domain. Provides a clear introduction to the concept of multiple but interoperable schemes; the **ITSO** Environment is 24014-1 compliant.
ISO 24014-2	In development as Part 2 of the Integrated Fare Management (**IFM**) standard, for through ticketing and portability of smart media between security domains (e.g. across national boundaries).

Expression	Explanation
ISO/IEC 24727	Interoperability standard for smart cards and related secure tokens.
ISP	Internet Service Provider
Issuer	In a stored-value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it. See also **Card issuer**.
Issuer identification number (IIN)	Number that uniquely identifies the card issuer of an ISO/IEC 7816 or ISO contactless card. ISO (SC17) operates a registration scheme for IINs.
ISTPA	International Security Trust and Privacy Alliance, an industry body dedicated to the development of (among other things) trusted system interfaces and trusted terminals (CADs, IFDs) for use with smart cards.
ITA	Integrated Transport Authority (qv) (UK).
ITSEC	Information Technology SECurity.
ITSO	Now just ITSO, but originally Integrated Transport Smartcard Organisation. A UK membership body comprising public transport operators, public sector transport management organisations (PTEs/ITAs/CAs), local authorities, Department for Transport, Scottish and Welsh devolved governments, and suppliers. Incorporated as a non-profit-distributing company limited by guarantee without shareholders (ITSO Ltd), has developed and maintains interoperability specifications (ITSO Specification and associated material, compliant with **ISO 24014-1**, qv for an introduction to the concept) for open, interoperable public transport ticketing schemes using smart media (currently cards, but in 2013 other forms of smart media, such as smartphones, are being investigated), and provides (with industry partners) a security key and permissions service (ISMS), security modules (ISAMs), and test and certification services. It is controlled by the Members. ITSO compliant schemes operate under a Licence from ITSO Ltd, which in turn operates under a Licence from govt (DfT) to use and further develop the ITSO methodology. For more technical ITSO Definitions see the Specification at http://www.itso.org.uk/wp-content/uploads/2012/09/General-Reference.pdf. See also **ISL** (historic).
ITSO Environment	The entirety of ITSO compliant (and where necessary ITSO certified) hardware and software and communications systems and components implemented and operated within an ITSO security domain. Thus an ITSO **HOPS** and an ITSO certified **POST** are within the security domain, but commercial systems for functions such as financial settlement are outside the security domain.
IVU	In Vehicle Unit – used in road tolling for the electronic car-based unit that communicates with roadside beacons or overhead gantries. Sometimes called On-Board Unit (OBU).
J	
Java	Java is an object-oriented programming language loosely based on C++ and designed primarily for dynamic and changeable hardware. In reduced form, applications written in Java may be run in smart cards. The specification is owned by Sun Microsystems, but others participate in its development.
Java Card	A derivative of original Java, for use in the restricted environment of the smart card.
Java Card Forum	An internationally active organisation founded by several smart card companies in 1997 to promote Java Card technology and develop related specifications.
Java Card virtual machine (JCVM)	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.
JCOP	Java Card Operating System (family thereof), owned by NXP Semiconductors (previously developed and owned by IBM Zurich).
JTOP	Java Card Operating System (family thereof), developed by Trusted Logic SA
JEIDA	Japan Electronics Industry Development Association – the Japanese standards body responsible for setting standards for PCMCIA-style memory cards.
JTC1	See **ISO/IEC JTC1**

Expression	Explanation
K	
K / k	Kilo. In the SI system of units k = 10^3 i.e. 1,000 units. In computer terminology k = 2^{10} i.e. 1,024 units.
Key	A series of digits used in a cryptographic algorithm that is computationally impractical to deduce from the plaintext and ciphertext.
Key diversification	See **Derived key**.
Key length	The number of bits comprising a key.
Key Management	The design of the life cycle of keys and the relationships between keys which are used in a computer system for cryptographic purposes. Alternatively, when referring to a system in operation, the process by which cryptographic keys used in a computer system are generated, stored and updated.
Know Your Customer (KYC)	Requirements in the form of due diligence and banking regulation applicable to companies dealing with financial transactions. The goal is for them to identify their customer correctly in order to help prevent identity theft fraud, money laundering and terrorist financing.
L	
Lamination	The process of gluing together thin sheets of material using heat and pressure. Many smart cards are laminated from several plastic foils.
LASSeO	Local Authority Smartcard Standards e-Organisation, incorporated as a non-profit-distributing company limited by guarantee. Initially promoted the adoption of the output of the UK National Smart Card Project (NSCP) across public sector Local Authorities, now generally promoting the use of smart media for citizen services. Works with ITSO to facilitate sharing of space in smart media. www.lasseo.org.uk
LDS	Logical Data Structure (qv)
Lead frame	The metal carrier used to provide the external contact pins on an encapsulated IC. Usually, the IC die is bonded down onto an area of the lead frame, and thin 'bond wires' connect from the contact areas on the IC to the inner end of the pins. At this stage, all pins are connected together by the outer section of the frame; after the IC is encapsulated (usually in moulded plastic), the outer section of the frame is cut away, leaving the individual pins for soldering down to a printed circuit board. See **COB** (**Chip-on-board**).
Life Cycle	The aggregate of the stages in the life of a smart card, beginning with the production of thechip 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.
Limited-purpose prepaid card	A prepaid card which can be used for a limited number of well-defined purposes. Its use is often restricted to a number of well-identified points of sale within a known location (e.g. a building, corporation or university). In the case of single-purpose prepaid cards, the card issuer and the service provider may be identical (e.g. cards used in public telephones or closed public transit systems).
Linux	An open operating system for use in the PC environment, derived from Unix (which was originally a Bell Labs development of a single user multi-tasking operating system for scientific users in the minicomputer environment).
Load	Process of securely loading an electronic purse with value, or of loading a load module (software and data) into a multi-application card.
Load log	Transaction data held in an electronic purse recording the latest load details.
Load module	Application program and its fixed data, together with a digital certificate to authenticate the module.
Load network	Computer network (LAN or WAN) used to provide the facility to load value or application load modules (software and data) onto a smart card.
Local Authority Smartcards Standards e-Organisation.	**LASSeO** (qv)
Locking	A system for securing a smart card so that unauthorised users cannot gain access. Also known as card blocking when used to disable a card.

Expression	Explanation
Logical Data Structure	Dataset used in electronic passports compliant with ISO 7501 / ICAO Doc 9303. Also applicable to national ID cards.
Loyalty Card	Basic card function for a loyalty program often based on a memory card in a standalone scheme or may be an application in a multi-application card. May hold the user's loyalty points and an identifier for the user's account.
M	
M/m	Mega. In the SI system of units M = 10^6 i.e. 1,000, 000 units. In computer terminology M = 2^{20} i.e. 1,024k or 1,048,576 units.
MAC	Message Authentication Code – an encrypted block checksum appended to messages which may be re-computed by the recipient to ensure data integrity. Normally uses DES symmetric encryption, but AES and asymmetric cryptography may also be used.
Maestro card	International debit card (MasterCard brand).
Man In the Middle Attack	A form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.
Mask	The specification which defines the physical and functional properties of the IC chip, effected during manufacture. Thus 'masked ROM' for the computer code and data permanently inserted into a card IC during manufacture.
MasterCard International (MasterCard Worldwide)	A payment systems organisation, headquartered in Purchase, New York, which operates the MasterCard card payment system. A public company, but in Europe the MasterCard brand continues to be an association owned by its members, the banks, in close association with MasterCard International. MasterCard issues its own specifications M/Chip and requires certification for its members of each card type issued with the MasterCard brand. (In 2002, MasterCard and the former European partner **Europay** merged.)
MasterPass	MasterCard's "digital service that allows consumers to use any payment card or enabled device to discover enhanced shopping experiences that are as simple as a click, tap or touch – online, in-store or anywhere". Being progressively rolled out globally from early 2013 (information from www.mastercard.com).
Memory card	A simple smart card with no application software processing capability, as in prepaid telephone cards and the Mifare® range of cards (Classic, DESFire, UL, etc).
Memory stick	Colloquial term (because of the shape of the device) for a portable USB memory device, usually containing flash memory but may also include security functions implemented in a secure chip.
MF	Master File; used to define the root directory within a smart card filing system according to ISO/IEC 7816 Part 4.
MFC	Multi-Function Card. An IBM-owned specification and design for smart cards, based on the ETSI TE9 specification.
Microcontroller	A microcomputer with all of its micro-processing facilities and enough memory and peripheral device functions in a single chip to permit a fully functional computer system to be implemented within the chip.
Micro-payments	In the electronic purse domain, payment values between, say, a fraction of 1p and £5. Macro-, Pico- and other value-size expressions are also beginning to appear.
Microprocessor	A microcomputer with all of its processing facilities in a single chip.
MIFARE®	Initially a proprietary contactless card security protocol (Crypto-1) based on ISO14443 type A, developed by Mikron AG in Graz, Austria in the 1990's. The brand and IP is now owned by NXP and is incorporated into various smart card chips and reader ICs. Several card and chip suppliers have licences from NXP to include Mifare® in USIMs and other chips. Infineon has compatible IP obtained from Mikron, incorporated into a range of chips. The initial chip product line is now known as Mifare® Classic and is becoming obsolete because of the weakness of the security protocol. The current chip ranges offer a variety of chip capabilities and security protocols.

Expression	Explanation
MintChip	A digital currency backed by the Govt of Canada and denominated in a variety of currencies. Project launched 2012. Managed by the Royal Canadian Mint. http://en.wikipedia.org/wiki/MintChip and http://mintchipchallenge.com/
MIP	Million Instructions per Second.
MNO	Mobile (phone) Network Operator
Modeus	An unaccounted open e-purse. Unlike Mondex (qv), does not permit personal card to personal card value transfers. A French development, initially for deployment in the Paris region.
Mondex	An unaccounted open e-purse, permitting personal card to personal card value transfer as well as personal card to merchant, personal card to/from bank, and merchant to/from bank transfers. Small schemes were introduced in the UK and other countries from 1995, with banking supervision, but no widespread rollout. UK use is believed to have ceased. See also **MXI**.
Moneo (mon€o)	(1) An electronic purse system available on French bank cards to allow small purchases to be made without cash. (2) Scheme management software for local currency schemes using txt2pay for payment by mobile phone.
M-PESA	A mobile phone-based payment scheme in use in Kenya and now a number of other countries
Multi (or general)-purpose prepaid card	A prepaid card that can be used for a wide range of purposes and has the potential to be used on a national or international scale, although it may sometimes be restricted to a certain area. Often referred to as used in an OPEN, as opposed to a CLOSED, scheme.
Multi-application card	A smart card capable of storing data and software for a number of different applications – such as electronic purse, ID and health records. The applications may be provided by different parties or may be controlled by a single scheme developer.
Multi-function card	A smart card capable of storing data from a number of different applications – such as electronic purse, ID and health records. In this case, all of the application software runs in the host computer system(s). The applications may be provided by different parties or be controlled by a single scheme developer.
Multos	Multi-application card operating system, owned by the MAOSCO consortium that is administered by MAOSCO Ltd. MAOSCO includes Dainippon Printing Co. Ltd., Hitachi Ltd., Fujitsu Limited, and MasterCard International Inc.
MUSCLE	Movement for the Use of Smart Cards in a Linux Environment. Runs an internet forum to promote and support an API within the Linux environment on PCs for use when developing applications that access smart cards from Linux. Primarily supports the PC/SC spec, but within Linux rather than Microsoft systems. See http://lists.musclecard.com/mailman/listinfo/muscle_lists.musclecard.com
MXI	Mondex International Ltd, controlled by MasterCard from 1997. Owns the **Mondex** e-purse.
N	
National Identity Scheme	UK government scheme to build a National Identity Register for UK citizens and permanent residents. Operated by the Immigration and Passport Service (**IPS**). Issued a small quantity of ID Cards in 2009/10. Discontinued January 2011.
NBS	National Bureau of Standards (USA), now incorporated into **NIST**)
Near Field Communication	An extension of the Proximity Card (ISO/IEC 14443) contactless technology, allowing both ends of the communication channel to be self-powered and providing enhanced functionality, primarily in mobile telephones. Colloquially also used to describe the incorporation of unpowered 14443 compliant chips into other devices (e.g. stickers applied to mobile phones that do not have inbuilt 14443 compliant functions, touch areas on posters that can be interrogated by NFC enabled mobile phones). Relevant standards are ISO/IEC 18092, 21481, ETSI TS 102190 as well as ISO/IEC 14443.
Negative file	A file that contains zero or more ranges of identifiers for payment systems that are not allowed to perform successful transactions in the payment system.
NFC	See **Near Field Communication**

Expression	Explanation
NFC Steering Board	Industry forum which has membership including banks, mobile network operators, major retailers, the DfT, TfL, ATOC, and ITSO. It has been established to create an open model for the deployment of NFC enabled mobile phones and cards.
NIS	See **National Identity Scheme** (UK). (Discontinued January 2011)
NIST	National Institute for Standards and Technology (USA) (formerly NBS). www.nist.gov Also see **NSTIC**.
Non-bank financial institution	A financial institution that does not come under the definition of a "bank" (e.g. a financial institution other than a credit institution in Europe or a depository institution in the United States).
Non-repudiation	Of a transaction or communication, the making of that transaction or communication in such a way that one of the parties to the transaction or communication cannot deny participation in all or part of the transaction or deny the content of the communication.
Non-volatile memory	A semi-conductor memory that retains its content when the power source is removed. Examples are EEPROM and Flash Memory.
NSTIC	National Strategy for Trusted Identities in Cyberspace (USA). Facilitating the development of an Identity Ecosystem, specifically for securing the online experience. www.nist.gov/nstic/ . In early 2013 considering going global: http://nstic.blogs.govdelivery.com/2013/04/09/nstic-on-the-global-identity-stage-2/
O	
OCF	Open Card Forum, largely of historical interest. Ran an internet forum (www.opencard.org) to support an API within the PC environment, for use when developing application software to access cards. Initially supporting only one card type (the IBM MFC) via a very limited set of card reader/writers, with IBM Germany resources, it later provided support for other card types and card reader/writers (terminals). See also the current, related software environment: **MUSCLE**.
Off-line	A transaction in which no direct connection is made between the device(s) involved in the transaction and a centralised computer system for the purpose of authenticating or otherwise authorising the transaction before it is executed.
On-line	Indicates that a direct connection is made to a centralised computer for authorisation or validation before a transaction can be executed.
OnePulse	See **Barclaycard OnePulse** (but that scheme discontinued).
Open e-purse scheme	Strictly, an e-purse scheme in which there is more than one issuer of the tokens stored in the e-purse, so that the tokens may be redeemed by returning them to any of the issuers. By extension, frequently also means a scheme in which the tokens may be used in a wide variety of retail environments (e.g. throughout the retail environment of shops, service outlets, public transport).
Open network	A telecommunications network to which access is not restricted.
Operating System (OS)	A program which handles the functions available on the processor in which it is executing. And that interfaces them to application programmes through a set of function calls. Normally masked into the ROM of smart cards, but may be designed in such a way that components of the OS are loaded into the same area of memory as the application programs (usually an **EEPROM** or **Flash memory** area).
OSCIE	Proposal for the Open Smart Card Infrastructure for Europe (see **eESC**).
OSPT	Open standard for secure fare collection solutions for transit (public transport), developed and promoted by the OSPT Alliance, an industry body. http://www.osptalliance.org

Expression	Explanation
OTA	Over the Air as in mobile systems such GSM and 3G systems, where it refers to the possibility of establishing an end-to-end link between the background system and the Card or 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. Another example is the use of FTP downloads via the internet connection on a device.
OTPROM	One Time Programmable Read-Only Memory. Often used during personalisation and locked using a hardware fuse or a software one way function "soft fuse".
Oyster	The brand for a proprietary **AFC** smart card scheme operating in London (UK) for Transport for London public transport services and some rail services operated by franchised companies. Cards hold pre-paid transport tokens, tickets and passes. Currently based on **DESFire** EV1 using **AES**. Oyster is expected to remain the brand when by 2015 DESFire cards are largely replaced by account based contactless EMV cards issued by TfL. The original Oyster functionality was included in a 2007 trial of a dual interface card incorporating Oyster (contactless interface) and bank payment (contact interface) functions (**Barclaycard OnePulse**). Oyster is a closed scheme (c.f. **ITSO**, which is an open method for a set of schemes).
P	
Patch	In software development, a small section of 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.
Pay Now, Pay Later	Americanism for the dual, intertwined services of card-based debit and credit facilities. Charge cards fall in between: pay by a fixed date.
Payment	The payer's transfer of a monetary claim on a party acceptable to the payee. Typically, claims take the form of banknote or deposit balances held at a financial institution or at a central bank.
Payment Institution (PI)	A new category of regulated financial institution created by the **PSD**.
Payment Services Directive (PSD)	The legal foundation for the creation of an EU-wide single market for payments (typically using bank cards).
Payment Service Provider (PSP)	An organisation offering merchants online services for accepting electronic payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, real-time bank transfer based on online banking. Other payment methods may also be supported, as well as supporting services such as risk management. Transaction fees are levied. In the EU, PSPs are regulated under the Payment Services Directive.
Payment system	A set of instruments, banking procedures and, typically, interbank funds transfer systems that facilitate the circulation of money. Used by international card schemes, such as Europay, MasterCard and Visa.
PayPal	An online payment service. (1) "PayPal is the faster, safer way to send money, make an online payment, receive money or set up a merchant account." (www.paypal.com) (2) "A global e-commerce business allowing payments and money transfers to be made through the Internet. Online money transfers serve as electronic alternatives to paying with traditional paper methods, such as checks and money orders." (http://en.wikipedia.org/wiki/PayPal)
PayPass	MasterCard accounted contactless bank payment card technology being rolled out in the UK in since 2007. Compatible with Visa **PayWave**.
PayWave	Visa's equivalent to **PayPass** and compatible with it.
PC Card	See PCMCIA

Expression	Explanation
PC/SC	The PC/SC Workgroup began as a joint effort of CP8 (Groupe Bull), Hewlett-Packard, Microsoft, Schlumberger, and Siemens Nixdorf, initiated to develop a specification that can facilitate the interoperability necessary to allow smart cards to be effectively utilised within the PC environment. Sets the standard for integrating smart cards and smart card readers into the mainstream computing environment' (www.pcscworkgroup.com).
PCD	Proximity Coupling Device, the terminal used to provide power to, and communicate with, a Proximity contactless smart card (PICC). Sometimes more strictly used to refer just to the coupling coil (antenna) of the PCD. See also **Proximity** and **PICC**.
PCI-DSS	Payment Card Industry Data Security Standards, mandatory information security standards for organisations handling cardholder information in the payment card environment. Those organisations are required to demonstrate compliance on a periodic basis.
PCI Security Standards Council	The body to which major payment scheme providers belong, setting standards and approving financial payments companies and providers, typically those involved in processing smart card and other smart media payments. See **PCI-DSS**.
PCL	See Prepayment Cards Ltd
PCMCIA	Personal Computer Memory Card International Association – a US-based association with members drawn from leading hardware and software companies world-wide, working to develop international standards for storage and computer application memory cards which are fundamentally different from smart memory cards. PCMCIA Cards are also known as PC Cards. The format was used for expansion card slots for laptops. See also ExpressCard.
Persistent write	An algorithm for storing (writing) data to memory in such a way that interruption of the writing process always produces a known result: either the write operation has successfully and correctly completed, or it has not. If the operation has not successfully completed, it must at least be possible to restore the original data and know that such restoration has taken place. Also known as Bullet-proof write.
Personalisation	The action of loading a smart card (or other smart media) with all of the software and data (including data printed on the surface of the card) that both provides the functionality that a particular card holder requires and installs all data specific to that card holder and to the use that that cardholder is able to make of the card.
Photocard	A card (not necessarily a smart card, but often of ID-1 size) on which is a photograph of the authorised user for ID purposes.
PICC	Proximity Integrated Circuit Card, a smart card in which power is provided to the card, and communication takes place between card and terminal (PCD), via a magnetic field. See also **Proximity** and **PCD**.
PIN	Personal Identification Number – used to authorise transactions. Usually a four digit number chosen by the user for authorization purposes when they try to access their account. The PIN is known only to the user and the system to allow a way for a machine to identify a valid account/card holder. The designation 'CHV' (CardHolderValue) is sometimes used for the PIN, but is more usually used to describe the 3 digit number on the back of payment cards – see **CHV**.
PIN Pad	Originally a data-entry keypad with special mechanical and cryptographic protection for use in a terminal. In general usage, the entire card payment terminal is often called a PIN pad.
Personal Identity Verification (PIV) card	A card conforming to the Personal Identity Verification (PIV) requirements for USA federal employees and contractors. The cards implement the requirements of FIPS 201 (Federal Information Processing Standard Publication 201), a United States federal government standard.
PKCS	Public Key Cryptography System. Usually used to identify the set of security specifications maintained by RSA Labs.
PKCS #11	A specification for an API (e.g. provided within a PC environment) for accessing security services.
PKCS #15	A specification for the storage of security information (e.g. cryptographic keys) within a smart card.
PKI	Public Key Infrastructure. See **Asymmetric cryptography**.

Expression	Explanation
Plaintext	The original, non-encrypted data.
POS	Point-of-sale or Point-of-service – can refer to a variety of definitions including the location of the retail establishment, or the specific counter, however it also could mean the hardware and software of the device used for the money transfer or (most often in the context of this Glossary) the terminal where the transaction occurred.
POST	Point Of Service Terminal (term used by **ITSO**). A terminal where the **Customer Media** is read/written to as appropriate to add products or value, to check the validity of products, or to modify/remove products and or value. A POST contains an **ISAM**.
prEN	Prefix to reference number for **CEN** voluntary standard, replacing **ENV** designation.
Prepaid card	A card in which value is stored, and for which value the holder (or a third party) has paid the issuer in advance. The issuer may require payment transactions to be authorised online. See also **Limited-purpose** and **Multi-purpose prepaid card**, **Stored-value card** and **Electronic Purse**.
Pre-lam	A construction consisting of an antenna, with chip attached, ready for lamination as the centre of a multi-layer laminated card body. Sometimes known as an Inlay.
Pre-personalisation	A synonym for **Initialisation** of a smart card application.
Privacy	In the context of a payment system, the fact that no information that might permit determination of behaviour may be collected or distributed without the consent of the individual to whom it relates.
Private key	The private (secret) part of a cryptographic key pair, knowledge of which should be strictly limited.
Product	ITSO term for the dataset for a ticket, pass, etc, held within the ITSO Shell on the Customer Media.
PROM	Programmable Read Only Memory – solid-state, non-volatile, cheap and reliable, but totally inflexible. Use is limited to applications where the information stored in a chip will never change.
Protection Profile (PP)	In the context of a security evaluation, an implementation-independent set of security requirements (security target) adapted to particular application areas for specific targets of evaluation, such as a smart card. PPs are issued by security agencies. The current one for smart cards (PP035) is believed to originate from BSI in Germany. See **Common Criteria**.
Protocol	Procedures for the interchange of electronic messages between communicating devices.
Proton	An e-purse originally owned by a consortium of Banksys of Belgium, American Express, etc. Developed by Banksys, ownership later passed to PWI, a consortium of Banksys and others, and now owned by ST Microelectronics. The original Proton purse used symmetric cryptography (DES), and this version was expected to continue in use for closed schemes (e.g. public transport ticketing), with a **CEPS** compliant version for wider deployment.
Proximity	For contactless smart cards, Proximity refers to a type of card technology in which the typical maximum distance from the card to the terminal's antenna at which reliable communication may take place is 10 cm. Standardised in ISO/IEC 14443.
PSD	See **Payment Services Directive**
Pseudonymisation	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. (Also see **Anonymisation**)
PSP	See **Payment Service Provider**
PTA	Passenger Transport Authority. The political level organisation for oversight of public transport in a Metropolitan County, now superseded by ITA. See also **ITA** and **PTE**.
PTE	Passenger Transport Executive. A UK public sector entity which partially manages public transport provision in a Metropolitan County, and is responsible to a **PTA**. See also **PTA** and **ITA**.

Expression	Explanation
Public key	In asymmetric cryptography, the public (i.e. non secret) part of a cryptographic key pair which is published by the user (designated recipient) to allow others to send secure messages which may then only be decoded by the designated recipient who possesses the matching private key.
Public key certificate	Public key information supplied by one entity, signed by a trusted entity to certify the integrity of the public key.
Public key cryptography	See **asymmetric cryptography**.
Public key infrastructure (PKI)	(1) Supporting infrastructure, including non technical aspects, for the management of public keys: creating and managing key pairs (private key and associated public key) used in **asymmetric cryptography**. (2) A set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates.
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 the PUK 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.
Purse provider	An organisation responsible for the overall functionality and security of an e-purse system. Also an organisation entitled to receive funds in exchange for load transactions into the e-purse in the card, and which credits the service providers according to the transactions made in their purchase devices or (in the Mondex scheme) according to the deposits of Mondex tokens made with the purse provider.
PWI	Proton World International, the licensor for Proton e-purse schemes worldwide, and technology developer. Ownership later transferred to ST Microelectronics.
P2M	Person-to-Merchant, in the financial context a financial transaction occurring directly between a person and a merchant.
P2P	Person-to-Person, in the financial context a financial transaction occurring directly between two people.
Q	
QR Code	See **2d barcode** (below)
Quantum computing	The deployment of quantum mechanical technology as a possible technique for providing extremely high speed computing devices.
Qualified Electronic Signature	A form of **electronic signature**
R	
Radio Frequency IDentification	(1) A generic term for methods using chip-based devices as ID labels and tags on articles such as items of clothing and many other products. May simply contain the product type code, may also contain a product serial number, batch number, etc. Designed for reading at a distance, and often conforming to international standards such as ISO/IEC 14443, 15693, 18000-6 2013. (2) A family of technologies, which includes **NFC**, for zero-configuration data exchange between devices in proximity.
Random Number Generator (RNG)	A computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. appear random.
RAM	Random Access Memory; the volatile memory area of a chip that is used for transient data and can only store data whilst power is being supplied.
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.
Rehabilitation	See **Card Unblocking**
Remote payment	A payment carried out through the sending of payment orders or payment instruments (e.g. by mail, modem) from a remote location.

Expression	Explanation
Remote Ticket Download (RTD)	Downloading a ticket remotely to a mobile phone or PC. The **ITSO** environment includes a secure method for delivery of ITSO compliant tickets across the internet, etc.
Repudiation	The denial, by one of the parties to a transaction, of participation in all or part of the transaction or of the content of the communication.
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 terminal of the smart card (contact card), or sending a reset message (contactless card), without altering the supply voltage or energising field respectively.
Retail funds transfer system	A funds transfer system which handles a large volume of payments of relatively low value in such forms as cheques, credit transfers, direct debits, withdrawals at automated teller machines and electronic fund transfers at point of sale.
Reverse engineering	The process of analysing software code or hardware designs in order to determine how the software or hardware works.
RF	Radio Frequency.
RFID	**Radio Frequency Identification**
RIM	Research In Motion, the company behind the BlackBerry range of secure smartphones.
RISC	Reduced Instruction Set Computer. A synchronous (clocked) CPU in which the instruction set has been optimised for high-speed execution. In its purist form, each and every machine cycle executes an entire instruction. See **CISC**.
Road user charging	Payment of tolls for travelling along a highway. More recently applied to schemes which use electronic methods of vehicle ID and payment. Expected to use smart cards. The relevant family of standards has been developed in CEN/TC278/WG1.
ROM	Read Only Memory; non-volatile permanent memory which holds the operating system or possibly parts of the operating system, typically in a microprocessor-based smart card. Associated with the word ROM is the work Mask, 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. A smart card application that is not located in the EEPROM, but instead in the mask-programmed ROM of the smart card microcontroller can be said to be ROMed
RSA	Rivest, Shamir and Adleman public key algorithm, so named from the authors of the 1978 paper which described the technique. Because it is asymmetric in operation (i.e. the sender and receiver each have their own key), it is used in secure financial transmissions. It is more secure than DES but also much more difficult to compute. Use in smart cards is normally limited to those processors which have a co-processor dedicated for fast multiplications with large numbers. RSA Labs is the company dedicated to supporting RSA cryptography, and also producing the more general PKCS series of security specifications.
RSP	Rail Settlement Plan Ltd, to which all UK mainland operators of heavy rail passenger services (but excluding the operators of heritage railways) belong. With its partner Association of Train Operating Companies (**ATOC** Ltd) makes possible the operation of the UK mainland rail network as a seamless network providing through passenger journeys with one ticket. RSP handles, in accordance with the 2002 Ticketing and Settlement Agreement, settlement of payment for most of the fares paid for travel on the UK mainland heavy rail network.
S	
SAM	Secure Application Module (e.g. as used in the ITSO Environment) or Secure Access Module; a logical device used to provide security for insecure environments, and must therefore be protected against tampering. Used as a store for secret or critical information and as a secure platform for the execution of security algorithms.

Expression	Explanation
SAM Monitor	A device whereby public information in the SAM may be read.
SC17	See **ISO/IEC JTC1/SC17**
SCIM	The standard developed by the RPA (now NTA) in Dublin as the Republic of Ireland's national security standard for transport smartcard systems
SCNF	See **Smart Card Networking Forum**
SCT	SEPA Credit Transfer – The pan-European standard for "push" payments between bank accounts.
SECG	Standards for Efficient Cryptography Group. Tends to favour elliptic curve cryptography against RSA.
Secret key	The key used in a symmetric cryptographic algorithm, where the same key is used for encryption and decryption. (In asymmetric cryptography, the equivalent term for the key that has to be kept secret is Private key.)
Secure Access Module	See **SAM**
Secure Application Module	See **SAM**
Secure Element (SE)	A Secure Element is a tamper proof Smart Card chip capable of holding smart card-grade applications (e.g., payment, transport …) with the required level of security and features. In the NFC architecture, the Secure Element will hold contactless and NFC-related applications and is connected to the NFC chip acting as the contactless front end. The Secure Element could be integrated in various form factors: SIM Cards, embedded in the handset, or SD Card.
Secure Messaging	All methods, protocols and cryptographic algorithms used to protect smart card data transmissions against manipulation and tapping.
Security Assurance Requirements	See **Common Criteria**.
Security Functional Requirements	See **Common Criteria**.
Security module	A smart card or other protected hardware device in which secret keys are stored, which is resident in a reader/writer terminal. Additionally, in card loading systems, the security module generates keys and other security information to be loaded into the card. See **SAM**, **ISAM**.
Security Target	See **Common Criteria**.
SEFT	South East Flexible Ticketing, a UK DfT funded project to improve rail ticketing and rail journey management across the South East by introducing smart media tickets using ITSO technology and new ticket Products (e.g. managed accounts to automatically calculate discount for off-peak travel by regular travellers). Development started Oct 2011, **ATOC** and **RSP** are handling project management. https://www.gov.uk/government/policies/improving-local-transport/supporting-pages/smart-ticketing
Sequence number	A number attributed sequentially to a message and attached to it in order to prevent duplication or loss of the message.
Server	A computer that provides services through a network to other computers.
Session key	A cryptographic key which is used for a limited time, such as a single communication session or transaction, and then discarded. Usually a Derived key, in that it is generated from keys permanently held by the participants.
SET	Secure Electronic Transaction (SET); a joint specification published by Visa International and MasterCard International, aimed at protecting transactions made using existing payment products, such as credit and debit cards, rather than electronic money products.
Settlement	An act that discharges obligations in respect of funds or securities transfers between two or more parties.
Settlement system	A system used to facilitate the settlement of transfers of funds.
SHA	Secure Hash Algorithm: SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. It produces a 160 bit **hash** and is very popular in smartcard data management
SIM	Subscriber Identity Module, used to identify a GSM mobile phone to the network. Usually a smart card, and now may be combined with WIM and other functions in the same card. The smart card is in the small ID-000 format.

Expression	Explanation
Shell	An ITSO term for the application area held in the Customer Media. The ITSO Shell holds only data.
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 at the logical level. Simulators are generally slower than emulators, which means that they often cannot simulate the target system in real time.
Single European Payment Area (SEPA)	A self-regulatory harmonisation project being introduced across the European payments market by banks with support from the European Commission (EC) and the European Central Bank (ECB). The SEPA initiative will encompass new, standard business and technical frameworks to make cross-border payments with the eurozone the same as domestic payments. The SEPA Credit Transfer went live in January 2008.
Single Wire Protocol (SWP)	A specification for a single-wire connection between the SIM card and a near field communication (NFC) chip in a cell phone. It is currently under final review by the European Telecommunications Standards Institute (ETSI). SWP is an interface between Contactless frontend (CLF) and UICC. It is a contact based protocol which is used for contactless communication. C6 pin of UICC is connected to CLF for SWP support. It is a bit oriented full duplex protocol i.e. at the same time transmission as well as reception is possible. CLF acts as a master and UICC as a slave. CLF provides the UICC with energy, a transmission clock, data and signal for bus management. The data to be transmitted are represented by the binary states of voltage and current on the single wire.
Skimming	The process of electronically copying the data from one card to another. Generally, but not exclusively, applied to magnetic stripe card fraud (see also **Buffering**).
Smart card	Strictly, a card containing an integrated circuit (IC) that is capable of securely performing calculations and storing information. The expression has been widely adopted to refer also to memory-only cards and to cards containing an ASIC. May be accessed and provided with power by means of electrical contacts or an embedded antenna (may feature one or both of those access methods).
Smart Card Alliance (SCA)	USA-based but global not-for-profit multi-industry organisation to stimulate the understanding, adoption, use and widespread application of smart card technology. Has formed the (USA) **EMV Migration Forum**.
Smart Card Club (SCC)	Founded in 1992, a professional association of member companies forming the UK's premier forum for education and networking in the smart card community. An international network of sister associations also exists.
Smart Card Forum	The USA-based equivalent of The Smart Card Club (but not connected with the SCC). May have merged with another organisation.
Smart Card Networking Forum (SCNF)	An organisation of UK Local Authorities for the sharing of experience in the deployment of smart cards for citizen services. http://www.scnf.org.uk/ Grew out of the National Smart Card Project (c2003) sponsored by the then Office of the Deputy Prime Minister (ODPM), now Dept for Communities and Local Govt https://www.gov.uk/government/organisations/department-for-communities-and-local-government
Smartphone	A high-end mobile phone that combines the functions of a personal digital assistant, a web browser and a mobile phone.
SMS	Short Message Service – The mobile telecommunications network service used for text messaging.
SNAPI	The aim of the SNAPI™ project is to implement systems for coding user requirements to enable adaptable user interfaces. http://www.snapi.org.uk/ SNAPI led to the development of EN1332-4 Coding of User Requirements for People with Special Needs.
Solo card	Restricted use debit card (usually in one country only) (MasterCard brand).
SPOM	Self-programmable One-Chip Microcomputer; an electronic component comprising one central unit, one unit of RAM and one of EPROM or E^2PROM. Access depends on the operating system present in the ROM.
SRAM	Static Random Access Memory – Volatile computer memory which may be battery backed to preserve its contents during power failure.

Expression	Explanation
Stamp	Colloquial term for the contact area on an ISO/IEC 7816 contact card.
Store and forward	Typically used to describe a type of transmission protocol which allows information to be temporarily stored at one or more points during transmission from the originator to the recipient. Confirmation of error-free transmission cannot therefore be immediately returned to the originator. Used, for example, in (most) credit card transaction message transfers from retail merchants to acquirers. (The opposite of **End to end** transmission.)
Stored-value card	A prepaid card in which the record of funds can be increased (generally up to a ceiling) as well as reduced. See also **Electronic purse**.
STORK	The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. The first phase is complete, and STORK 2.0 has started: Secure idenTity acrOss boRders linKed 2.0 will contribute to the realisation of a single European electronic identification and authentication area. It does so by building on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities and the facility to mandate. www.eid-stork2.eu
Switch card	A UK debit card issued by the major UK banks, and usually managed through the Europay/MasterCard card system. Now replaced by the Maestro brand.
Symbian	Operating system used in some models of smartphone. Owned by Accenture.
Symmetric cryptography	A set of cryptographic techniques in which devices share the same secret key in combination with algorithms. The key cannot be made public as it is used for encrypting and decrypting. The decrypting algorithm is the reverse function of the encrypting algorithm.
Systemic risk	The risk that the failure of one participant in a transfer system, or in financial markets generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations (including settlement obligations in a transfer system) when due. Such a failure could cause significant liquidity or credit problems and, as a result, might threaten the stability of financial markets (with subsequent effects on the level of economic activity.
T	
T=0	Character oriented asynchronous half-duplex transmission protocol used to communicate with contact IC cards according to ISO/IEC 7816.
T=1	Block oriented asynchronous half-duplex transmission protocol used to communicate with contact IC cards according to ISO/IEC 7816.
Tamper-evident	The capacity of devices to show evidence of physical attack.
Tamper-proof	The proven capacity of devices to resist all attacks. Generally held not to exist in the real world.
Tamper-resistant	The capacity of devices to resist physical attack up to a certain point.
Target of Evaluation (ToE)	A IT system to be evaluated , or in other words, the object under test. For example, a ToE could be a microcontroller smart card with integrated software that must meet certain security targets or catalogue of criteria. (See **Common Criteria**)
TCP	Transmission Control Protocol, used in digital communications link, especially on the internet
TCP/IP	The transmission control and information protocols underpinning the internet, but also used for other data communication applications.
TE9	An operating system specification adopted by IBM in their Multi Function Card. Also the name of an ETSI Committee.
Time-stamp	A value inserted in a message to indicate the time at which the message was created.
TPDU	Transmission Protocol Data Unit. A transport layer message between an **IFD** and an **ACD**, as defined in ISO/IEC 7816
Traceability	In electronic systems, the degree to which value-transfer transactions can be traced to the originator(s) or the recipient(s) of the transfer.
Transaction log	A sequential record of transactions that is stored in a device.
Transferability	In electronic money systems, the degree to which an electronic value can be transferred between devices without interaction with a central authority.

Expression	Explanation
Translink	The public transport service provider for Northern Ireland http://www.translink.co.uk/ . Operates a smart card ticketing scheme using proprietary technology. In spring 2013 procurement for a replacement scheme is starting, with a target in-service date of early 2017.
Transport Scotland	Public sector agency in Scotland responsible for the delivery of major transport infrastructure projects and for overseeing the operation of the Scottish transport networks. Manages the Scottish public transport concessionary travel scheme.
Triple DES	Triple-DES consists of operating the **DES** algorithm three times to ensure greater security. Two keys are used, and the sequence is: first key, second key, first key.
Trusted terminal	For smart card use, a hardware device which is trusted to handle communication between a smart card and an operator (usually the cardholder), in such a manner that communication is not interfered with.
Trusted third party (TTP)	An entity trusted by other entities with respect to security related services and activities.
TVM	Automated Ticket Vending Machine – a vending machine for issuing (usually public transport) tickets. Sometimes encountered as ATVM (Automatic Ticket Vending Machine), as ETM (Electronic Ticket Machine), or as ATM (not to be confused with banking ATM).
Two Factor Authentication (2FA)	Authentication that uses two different mechanisms to verify identity for security purposes. An example of 2FA might require both a password and a smart card thus determining both what the user knows and what the user has.
Type approval	The process by which equipment and cards (with the relevant applications loaded onto them) are tested and certified as compliant with a scheme's rules and specifications. Also known as Certification.
U	
UID	(1) Unique Identifier number (2) Unique Identification Number later renamed as Aadhaar number, an initiative of Unique Identification Authority of India of the Indian government to create a unique ID for every Indian resident.
UKIS	(Historic) The early bank chip debit/credit scheme for the UK. The UKIS specification was for the UK cards and systems, and was initially the national interpretation of EMV V3.0.
UKPA	UK Payments Administration Ltd. From 2009 the successor to **APACS**. Is the umbrella organisation for payment standards and service definition across UK banking.
UMTS	Universal Mobile Telephone System ("3G").
UHF	Ultra High Frequency: carrier frequencies between 300 MHz and 1GHz.
Ultralight-Mifare	A basic memory based proprietary contactless card based on ISO14443 type A. The brand and IP is owned by NXP and is incorporated into various smart card chips and reader ICs from NXP. Infineon has compatible technology incorporated into a range of chips.
USIM	The common name of the smart card application for 3G which resides in a UICC. However, in practice the term 'USIM' is also used to refer to the 3G smart card as well as to 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.
V	
V.me by Visa	**Visa**'s digital wallet service
VCD	Vicinity Coupling Device, the terminal used to provide power to and communicate with a Vicinity contactless smart card (VICC). Sometimes more strictly used to refer just to the coupling coil (antenna) of the VCD. See also **Vicinity** and **VICC**.

Expression	Explanation
VICC	Vicinity Integrated Circuit Card, a smart card in which power is provided to the card, and communication takes place between card and terminal (PCD), via a magnetic field. See also **Vicinity** and **VCD**.
Vicinity	For contactless smart cards, Vicinity refers to a type of card technology in which the typical maximum distance from the card to the terminal's antenna at which reliable communication may take place is 30 cm. ISO/IEC 15693 has standardised this technology.
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	Visa Inc, a payment systems company and organisation, headquartered in California, which operates the Visa card payment system. In 2008 converted from an association owned by its members, the banks, to a public company.
Visa Cash	An e-purse brand owned by Visa. At end 20th century applied to a number of e-purse card types using various technologies. The most advanced version, using public key cryptography, was in 1999/2000 on trial in Leeds, UK, but the original concept was based on disposable cards and Danmønt technology.
Visa Delta card	A debit card operated through the Visa card system.
Visa PayWave	Contactless payment card technology developed by Visa. Compatible with MasterCard PayPass.
VRM	Vendor Relationship Management. A category of business activity made possible by software tools that provide customers with both independence from vendors and better means for engaging with vendors.
VTS	Vulcan To the Sky, supporting keeping the last RAF V-bomber in the air. www.vulcantothesky.org .
W	
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).
Wallet	See **Electronic Wallet**
WAP	Wireless Application Protocol. An information transfer protocol tailored to the special needs of GSM mobile phones, enabling them to connect, via a bridging system, to the internet.
White Card	Refers to non-personalised blank cards, sometimes 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 but for which the manufacturing process is not complete. E.g. credit cards with magnetic stripes and holograms that have not yet been embossed.
White list	In a card based system, a database containing the list of all authorised card numbers. By extension, may be applied to any list containing the authorised members of a larger set (e.g. currencies) and to components of a card based system (e.g. **AIDs**, ticket Products). See also **Hot list** and **Black list**.
White space	Gaps in the UHF broadcast frequency band opened up by transferring TV broadcasts from analogue to digital methods.
WIM	Wireless Identity Module, to authenticate a WAP terminal to the network for internet and related service purposes. May be combined with SIM functions in one smart card.
Windows Phone 7	Smartphone Operating System owned by Microsoft
Wired logic card	Alternative name for a memory card or an ASIC card.
X-Z	
X3, X9, etc	Committees of ANSI
Zero knowledge communication	Method of transferring information across an interface in such a manner that anyone monitoring that communication cannot deduce anything about the operation of the devices at either side of the interface.
Num	

Expression	Explanation
2d barcode	A digital data string represented as shown below:  Otherwise known as a QR code
2FA	See **Two Factor Authentication**
3DES	See **Triple DES**