Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)™

Glossary of Terms, Abbreviations, and Acronyms

Version 1.2

February 2013

Term	Definition
Access controls	Controls which ensure that specific objects, functions, or resources can only be accessed by authorized users in authorized ways.
Account data	At a minimum, account data contains the full PAN and (if present) any elements of sensitive authentication data. The following are also considered to be account data if sent in conjunction with the PAN: cardholder name, expiration date, or service code.
Algorithm	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
ANSI	American National Standards Institute. A U.S. standards accreditation organization.
Application Vendor	See *P2PE Application Vendor.*
Asymmetric cryptography (techniques)	See *Public key cryptography*.
ATM	An unattended terminal that has electronic capability, accepts PINs, and disburses currency or checks.
Authentication	The process for establishing unambiguously the identity of an entity, organization, or person at a specific point in time.
Authorization	The right granted to a user to access an object, resource, or function.
Authorize	To permit or give authority to a user to communicate with or make use of an object, resource, or function.
Base (master) derivation key (BDK)	See *Derivation key*.
Cardholder	An individual to whom a card is issued or who is authorized to use the card.
Cardholder data (CHD)	At a minimum, cardholder data contains the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: ▪ Cardholder name ▪ Expiration date ▪ Service Code See *Sensitive authentication data (SAD)* for additional data elements that may be transmitted or processed as part of a payment transaction.
Certificate	The public key and identity of an entity, together with other information, rendered unforgeable by signing the certificate with the private key of the certifying authority that issued that certificate.
Certificate revocation	The process of revoking an otherwise valid certificate by the entity that issued that certificate. Revoked certificates are placed on a Certificate Revocation List (CRL) or the information is conveyed using Online Certificate Status Protocol (OCSP) as specified in the product/service specification.

Term	Definition
Certificate Revocation List (CRL)	A list of revoked certificates. Entities that generate, maintain and distribute CRLs can include the Root or subordinate CAs.
Check value	A computed value that is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation, which takes as input a secret key and an arbitrary string and gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall not be feasible. Also referred to as "key check value."
Cipher text	Data in its encrypted form.
Clear text	Intelligible data that has meaning and can be read or acted upon without the application of decryption.
Clear-text key	An unencrypted cryptographic key, which is used in its current form.
Compromise	In cryptography, the breaching of secrecy and/or security. A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. This includes the unauthorized disclosure, modification, substitution, or use of sensitive data (including clear-text cryptographic keys and other keying material).
Computationally infeasible	The property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it.
Credentials	Identification data for an entity, incorporating at a minimum the entity's distinguished name and public key.
Critical security parameters (CSP)	Security-related information (for example, cryptographic keys, authentication data such as passwords and PINs) appearing in clear text or otherwise unprotected form and whose disclosure or modification can compromise the security of a SCD or the security of the information protected by the device.
Cryptogram	A message or set of data enciphered by a cryptographic key.
Cryptographic boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.
Cryptographic key	A parameter used in conjunction with a cryptographic algorithm that determines: ▪ The transformation of clear-text data into cipher-text data, ▪ The transformation of cipher-text data into clear-text data, ▪ A digital signature computed from data, ▪ The verification of a digital signature computed from data, ▪ An authentication code computed from data, or ▪ An exchange agreement of a shared secret.

Term	Definition
Data Encryption Algorithm (DEA)	A published encryption algorithm used to protect critical information by encrypting data based upon a variable secret key. The Data Encryption Algorithm is defined in *ANSI X3.92: Data Encryption Algorithm* for encrypting and decrypting data. The algorithm is a 64-bit block cipher that uses a 64-bit key, of which 56 bits are used to control the cryptographic process and 8 bits are used for parity checking to ensure that the key is transmitted properly.
Data-encryption (encipherment or exchange) key (DEK)	A cryptographic key that is used for the encryption or decryption of account data.
Decipher	See *Decrypt*.
Decrypt	A process of transforming cipher text (unreadable) into clear text (readable).
Derivation key	A cryptographic key, which is used to cryptographically compute another key. A derivation key is normally associated with the DUKPT key-management method. Derivation keys are normally used in a transaction-receiving (for example, acquirer) SCD in a one-to-many relationship to derive or decrypt the transaction keys (the derived keys) used by a large number of originating SCDs (for example, POIs).
DES	Data Encryption Standard (see Data Encryption Algorithm). The National Institute of Standards and Technology Data Encryption Standard, adopted by the U.S. Government *as Federal Information Processing Standard (FIPS) Publication 46,* which allows only hardware implementations of the data encryption algorithm.
Digital signature	The result of an asymmetric cryptographic transformation of data that allows a recipient of the data to validate the origin and integrity of the data and protects the sender against forgery by third parties or the recipient.
Double-length key	A cryptographic key having a length of 112 active bits plus 16 parity bits, used in conjunction with the TDES cryptographic algorithm.
Dual control	A process of using two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials or functions being protected. Each party is responsible for the protection of mechanisms used to enact dual control (for example, passwords, keys, etc.). No single person must be able to access or use the materials (for example, the password or keys) of the other party. For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. Also see *Split knowledge.*

Term	Definition
DUKPT	Derived Unique Key Per Transaction: a key-management method that uses a unique key for each transaction and prevents the disclosure of any past key used by the transaction-originating POI. The unique transaction keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction.
EEPROM	Electronically erasable programmable read-only memory.
Electronic key entry	The entry of cryptographic keys into a SCD in electronic form using a key-loading device. The user entering the key may have no knowledge of the value of the key being entered.
Encipher	See *Encrypt*.
Encrypt	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data.
Encrypting PIN pad (EPP)	A device for secure PIN entry and encryption in an unattended PIN-acceptance device. An EPP may have a built-in display or card reader, or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an ATM or other unattended device (for example, an unattended kiosk or automated fuel dispenser) for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary, and a tamper-resistant or tamper-evident shell.
EPROM	Erasable programmable read-only memory.
Exclusive-OR	Binary addition without carry, also known as “modulo 2 addition,” symbolized as “XOR,” and defined as: ▪ 0 + 0 = 0 ▪ 0 + 1 = 1 ▪ 1 + 0 = 1 ▪ 1 + 1 = 0
Fail closed	A state where the PCI-approved POI device discontinues operations for PCI payment brand accounts/cards.
FIPS	Federal Information Processing Standard.
Firmware	The programs and data (i.e., software) permanently stored in hardware (for example, in ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Programs and data stored in EEPROM are considered as software.
Hardware/host security module (HSM)	A physically and logically protected hardware device that provides a secure set of cryptographic services, used for cryptographic key-management functions and/or the decryption of account data. For P2PE, these devices must be: a) Approved and configured to FIPS140-2 (level 3 or higher), or b) Approved to the PCI HSM standard. See also *Secure cryptographic device.*

Term	Definition
Hash function	A (mathematical) function that takes any arbitrary-length message as input and produces a fixed-length output. It must have the property that it is computationally infeasible to discover two different messages that produce the same hash result. It may be used to reduce a potentially long message into a "hash value" or "message digest" that is sufficiently compact to be input into a digital-signature algorithm.
Hash value	The value returned by a hash function. Different hash values may be used for different purposes, and are sometimes referred to as hashes, hash codes, checksums, message digests and fingerprints.
Initialization vector	A binary vector used as the input to initialize the algorithm for the encryption of a clear-text block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment. The initialization vector need not be secret.
Integrity	Ensuring consistency of data—in particular, preventing unauthorized and undetected creation, alteration, or destruction of data.
Interface	A logical section of an SCD that defines a set of entry or exit points that provide access to the device, including information flow or physical access.
Irreversible transformation	A non-secret process that transforms an input value to produce an output value such that knowledge of the process and the output value does not feasibly allow the input value to be determined.
ISO	International Organization for Standardization. An international standards accreditation organization.
Issuer	The institution holding the account identified by the primary account number (PAN).
Key	See *Cryptographic key.*
Key agreement	A key-establishment protocol for establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key. That is, the secret key is a function of information contributed by two or more participants.
Key backup	Storage of a protected copy of a key during its operational use.
Key bundle	The three cryptographic keys (K1, K2, K3) used with a TDEA mode. The keys are used in three operations, such that they form the logical equivalent of one key. Keys used in conjunction with a key bundle must never be used separately for any other purpose.
Key component	A parameter used in conjunction with other key components in an approved security function to form a clear-text cryptographic key or perform a cryptographic function. A key component may also be considered a secret share when it is part of a recognized cryptographic secret-sharing scheme.
Key-derivation process	A process that derives one or more session keys from a shared secret and other (possibly) public information.

Term	Definition
Key destruction	Occurs when an instance of a key in one of the permissible key forms no longer exists at a specific location.
Key distribution host (KDH)	A KDH is a processing platform used in conjunction with HSM(s) that generates keys and securely distributes those keys to POIs and the financial-processing platform communicating with those POIs. A KDH shall not be used for certificate issuance, and must not be used for the storage of CA private keys.
Key-encryption (encipherment or exchange) key (KEK)	A cryptographic key that is used for the encryption or decryption of other keys.
Key establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key generation	Creation of a new key for subsequent use.
Key instance	The occurrence of a key in one of its permissible forms, i.e., clear-text key, key components, encrypted key.
Key loading	Process by which a key is manually or electronically transferred into an SCD.
Key-loading device	A self-contained unit that is capable of storing at least one clear-text or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module (such as a POI or HSM).
Key management	The activities involving the handling of cryptographic keys and other related security parameters (for example, initialization vectors, counters) during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction, and archiving.
Key pair	A key pair comprises the two complementary keys for use with an asymmetric encryption algorithm. One key, termed the public key, is expected to be widely distributed; and the other, termed the private key, is expected to be restricted so that it is only known to the appropriate entities.
Key replacement	Substituting one key for another when the original key is known or suspected to be compromised or the end of its operational life is reached.
Key share	Related to a cryptographic key generated such that a specified fraction of the total shares of such parameters can be combined to form the cryptographic key but such that less than a specified fraction does not provide any information about the key. Also referred to as a secret share.
Key storage	Holding of the key in one of the permissible forms.
Key transport	A key-establishment protocol under which the secret key is determined by the initiating party and transferred suitably protected.

Term	Definition
Key usage	Employment of a key for the cryptographic purpose for which it was intended.
Key variant	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Keying material	The data (for example, keys and initialization vectors) necessary to establish and maintain cryptographic-keying relationships.
Manual key loading	The entry of cryptographic keys into an SCD from a printed form, using devices such as buttons, thumb wheels, or a keyboard.
Master derivation key (MDK)	See *Derivation key.*
Master key	In a hierarchy of key-encrypting keys and transaction keys, the highest level of key-encrypting key is known as a master key.
Message	A communication containing one or more transactions or related information.
Node	Any point in a network that does some form of processing of data, such as a terminal, acquirer, or switch.
Non-PCI payment brand accounts/cards	Payment accounts/cards that are not PCI payment brand accounts/cards. Examples of non-PCI payment brand accounts/cards may include certain loyalty cards or non-PCI payment brand store cards. See also *PCI payment brand accounts/cards*.
Non-reversible transformation	See *Irreversible transformation.*
OCSP	See *Online Certificate Status Protocol.*
Online Certificate Status Protocol	The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate in question until the responder provides a response.
Out-of-band notification	Notification using a communication means independent of the primary communications means.
PAN	Primary account number. See also *Cardholder data.*
Password	A string of characters used to authenticate an identity or to verify access authorization.
PCI-approved POI device	Point of interaction (POI) device evaluated and approved via the PCI PTS program, with SRED (secure reading and exchange of data) listed as a "function provided," and with the SRED capabilities enabled and active.

Term	Definition
PCI payment brand accounts/cards	Payment accounts/cards associated with one of the five founding payment card brands of the Payment Card Industry Security Standards Council (PCI SSC). These accounts/cards are issued either by or on behalf of one of the founding payment card brands. The founding payment card brands are: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
Physical protection	The safeguarding of a cryptographic module, cryptographic keys, or other keying materials using physical means.
Physically secure environment	An environment that is equipped with access controls or other mechanisms designed to prevent any unauthorized access that would result in the disclosure of all or part of any key or other secret data stored within the environment. Examples include a safe or purpose-built room with continuous access control, physical security protection, and monitoring.
PIN entry device (PED)	A PED is a device for secure PIN entry and processing. The PED typically consists of a keypad for PIN entry, laid out in a prescribed format, a display for user interaction, a processor, and storage for PIN processing sufficiently secure for the key-management scheme used and firmware. A PED has a clearly defined physical and logical boundary and a tamper-resistant or tamper-evident shell.
Plaintext	See *Clear text.*
Point of interaction (POI)	The initial point where data is read from a card. An electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions." See also *Secure cryptographic device.*
P2PE	Point-to-point encryption.
P2PE Application	A software application that is included in a P2PE Solution, required to be assessed per P2PE Domain 2 Requirements, and is intended for use on a PCI-approved point-of-interaction (POI) device or otherwise by a merchant.
P2PE Application Vendor	A software vendor that develops and then sells, distributes, or licenses any third party any P2PE Application.
P2PE Components	Any application or device that stores, processes, or transmits account data as part of payment authorization or settlement, or that performs cryptographic key management functions, and is incorporated into or a part of any P2PE Solution.
P2PE Solution	A point-to-point encryption solution consists of point-to-point encryption and decryption environments, the configuration and design thereof, and the P2PE Components that are incorporated into, a part of, or interact with such environment.

Term	Definition
P2PE Solution Provider	The P2PE Solution Provider is a third-party entity (for example, a processor, acquirer, or payment gateway) that: a) Designs, implements, and manages a P2PE Solution for merchants (the P2PE Solution Provider may outsource certain aspects of the P2PE Solution—for example, key injection facility, certification authority); and b) Is ultimately responsible for the design, maintenance, and delivery of the overall P2PE solution.
Private key	A cryptographic key, used with a public-key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encryption system, the private key defines the decryption transformation.
PROM	Programmable read-only memory.
Pseudo-random	A value that is statistically random and essentially random and unpredictable although generated by an algorithm.
Public key	A cryptographic key, used with a public-key cryptographic algorithm, uniquely associated with an entity, and that may be made public In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encryption system, the public key defines the encryption transformation. A key that is “publicly known” is not necessarily globally available. The key may only be available to all members of a pre-specified group.

Term	Definition
Public key (asymmetric) cryptography	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is not computationally feasible to derive the private transformation. A system based on asymmetric cryptographic techniques can be any of the following: ▪ An encryption system, ▪ A signature system, ▪ A combined encryption and signature system, or ▪ A key-agreement system. With asymmetric cryptographic techniques, there are four elementary transformations: sign and verify for signature systems, and encrypt and decrypt for encryption systems. The signature and the decryption transformation are kept private by the owning entity, whereas the corresponding verification and encryption transformations are published. There exist asymmetric cryptosystems (for example, RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, this does not conform to the principle of key separation, and where used, the four elementary transformations and the corresponding keys should be kept separate.
Random	The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware-based "noise" mechanisms. This results in a value in a set that has equal probability of being selected from the total population of possibilities, hence unpredictable.
ROM	Read-only memory.
Root Certification Authority (RCA)	The RCA is the top-level Certification Authority in a public-key infrastructure. An RCA is a CA that signs its own public key with the associated private key. RCAs only issue certificates to subordinate CAs. Root CAs do not issue certificates directly to KDHs, EPPs or PEDs. RCAs may also issue certificate status lists for certificates within their hierarchy.
Secret key	A cryptographic key, used with a secret-key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.
Secure card reader (SCR)	A PCI-approved encrypting card reader that is intended for use with a POI device. See also *Point of Interaction (POI).*

Term	Definition
Secure cryptographic device (SCD)	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. An SCD is used either for the acceptance and encryption of account data at the point of sale, or for cryptographic key-management functions and/or the decryption of account data. SCDs used for acceptance or encryption of account data at the point of sale are also referred to at *POIs* or *PCI-approved POI devices*. SCDs used for cryptographic key-management functions and/or the decryption of account data include *HSMs* (host/hardware security modules). See also *Point of Interaction, PCI-approved POI device,* or *Host/hardware security module.*
Sensitive authentication data (SAD)	Security-related information (including but not limited to card-validation codes/values, full-track data from the magnetic stripe, magnetic-stripe image on the chip or elsewhere, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
Sensitive data	Data that must be protected against unauthorized disclosure, alteration, or destruction—especially cardholder data, sensitive authentication data, and cryptographic keys—and includes design characteristics, status information, and so forth.
Session key	A key established by a key-management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys, for example, an encryption key and a MAC key.
Shared secret	The secret information shared between parties after protocol execution. This may consist of one or more session key(s), or it may be a single secret that is input to a key-derivation function to derive session keys.
Single-length key	A cryptographic key having a length of 56 active bits plus 8 parity bits used in conjunction with the DES cryptographic algorithm.
Software	The programs and associated data that can be dynamically written and modified.
Solution Provider	See *P2PE Solution Provider.*
Split knowledge	A condition under which two or more entities separately have key components, which individually convey no knowledge of the resultant cryptographic key.
Subordinate CA and Superior CA	If one CA issues a certificate for another CA, the issuing CA is termed the superior CA, and the certified CA is termed the subordinate CA. Subordinate CAs are typically used to segment risk. Subordinate CAs may issue certificates to KDHs, SCDs. Subordinate CAs may also issue certificates to lower-level CAs and issue certificate status lists regarding certificates the subordinate CA has issued.

Term	Definition
Symmetric key	A cryptographic key that is used in symmetric cryptographic algorithms. The same symmetric key that is used for encryption is also used for decryption.
System software	The special software (for example, operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programs, and data.
Tamper-evident	A characteristic that provides evidence that an attack has been attempted.
Tamper-resistant	A characteristic that provides passive physical protection against an attack.
Tamper-responsive	A characteristic that provides an active response to the detection of an attack, thereby preventing a success.
Tampering	The penetration or modification of internal operations and/or insertion of active or passive tapping mechanisms to determine or record secret data.
TDEA	See *Triple Data Encryption Algorithm.*
Terminal	A device/system that initiates a transaction.
Transaction	A series of messages to perform a predefined function.
Triple Data Encryption Algorithm (TDEA)	The algorithm specified in *ANSI X9.52, Triple Data Encryption Algorithm Modes of Operation.*
Triple Data Encryption Standard (TDES)	See *Triple Data Encryption Algorithm.*
Triple-length key	A cryptographic key having a length of 168 active bits plus 24 parity bits, used in conjunction with the TDES cryptographic algorithm.
Trustworthy system	Computer hardware and software which: ▪ Are reasonably secure from intrusion and misuse; ▪ Provide a reasonable level of availability, reliability, and correct operation; and ▪ Are reasonably suited to performing their intended functions.
Unattended acceptance terminal (UAT)	See *Unattended payment terminal.*
Unattended payment terminal (UPT)	A cardholder-operated device that reads, captures, and transmits card information in an unattended environment, including, but not limited to, the following: ▪ ATM ▪ Automated fuel dispenser ▪ Ticketing machine ▪ Vending machine

Term	Definition
Unprotected memory	Components, devices, and recording media that retain data for some interval of time that reside outside the cryptographic boundary of a SCD.
Variant of a key	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Verification	The process of associating and/or checking a unique characteristic.
Whitelist	A list used by a POI function or application to make processing decisions. For example, a whitelist could be a list and/or range of non-PCI payment brand account/card numbers, approved by the solution provider, that are not required to be encrypted at the POI, or it could be used to make routing decisions that pertain to only a subset of accounts/cards processed. Unless explicitly authorized by the relevant payment brand, PCI payment brand card/account numbers must not be on this list.
Working key	A key used to cryptographically process the transaction. A working key is sometimes referred to as a data key, communications key, session key, or transaction key.
XOR	*See* Exclusive-Or.
Zeroize	The degaussing, erasing, or overwriting of electronically stored data so as to prevent recovery of the data.