Payment Card Industry (PCI)

Point-to-Point Encryption

Glossary of Terms, Abbreviations, and Acronyms

Version 2.0

June 2015

Term	Definition
Access controls	Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.
Account data	Account data consists of cardholder data and/or sensitive authentication data. See *Cardholder Data and Sensitive Authentication Data.*
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution." Entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See also *Payment Processor.*
Advanced Encryption Standard (AES)	A block cipher used in symmetric-key cryptography adopted by NIST in November 2001 as U.S. FIPS PUB 197 (or "FIPS 197"). See *Strong Cryptography*.
Algorithm	A clearly specified mathematical process for computation; a set of rules, which, if followed, will give a prescribed result.
American National Standards Institute (ANSI)	A U.S. standards accreditation organization.
Application Vendor	See *P2PE Application Vendor.*
Asymmetric cryptography (techniques)	See *Public key cryptography*.
Authentication	Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as: ▪ Something you know, such as a password or passphrase ▪ Something you have, such as a token device or smart card ▪ Something you are, such as a biometric
Authentication credentials	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process.
Authorization	**In the context of access control,** authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. **In the context of a payment card transaction,** authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

Term	Definition
Base (master) derivation key (BDK)	See *Derivation key*.
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.
Cardholder data environment (CDE)	The people, processes and technology that store, process, or transmit cardholder data and/or sensitive authentication data.
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.
Certificate Revocation List (CRL)	A list of revoked certificates. Entities that generate, maintain, and distribute CRLs can include the Root or subordinate CAs.
Certification Authority (CA)	May also be called *Certificate Authority.* Any entity signing public keys, whether in X.509 certificate-based schemes or other designs for use in connection with the remote distribution of symmetric keys using asymmetric techniques. See also *Registration Authority*
Certification Authority/ Registration Authority (CA/RA) service	A service that can be offered by a third-party P2PE component provider. Such services are offered on behalf of P2PE solution providers, by entities operating CA/RA platforms in connection with remote-key distribution implementations, assessed per Domain 6 and Annex A, part A1 (as applicable) and part A2 See also *P2PE component provider.*
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.

Term	Definition
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	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.
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.
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.

Term	Definition
Data Encryption Standard (DES)	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. See *Data Encryption Algorithm*.
Decryption	A process of transforming cipher text (unreadable) into clear text (readable).
Decryption environment	The P2PE solution provider's or component provider's environment that contains the HSMs—or HSMs and Host System(s) for hybrid decryption solutions—used to decrypt the incoming encrypted account data originating from merchant encryption environments. For purposes of merchant-managed solutions, the *merchant decryption environment* is a restricted zone within the merchant's CDE that contains the HSMs used to decrypt the incoming encrypted account data originating from the merchant's encryption environment.
Decryption-management service	A service that can be offered by a third-party P2PE component provider, on behalf of P2PE solution providers. These entities manage the environment that receives and decrypts encrypted account data, as covered in Domains 5 and 6 (and Annex A as applicable). See also *P2PE component provider.*
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 (e.g., 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).
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.

Term	Definition
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 involved in vulnerable transactions. No single person must be able to access or use the materials (for example, the cryptographic key) of the other party. For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities. No single person can gain control of a protected item or process. Also see *Split knowledge.*
DUKPT	Acronym for "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.
Encipher	See *Encryption*.
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.
Encryption	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text— i.e., hiding the information content of the data.
Encryption environment	A merchant's physical location(s) containing the PCI-approved POI devices used for account-data acceptance and subsequent encryption. Merchant P2PE encryption environments include those for brick-and-mortar and or mail-order/telephone-order (MOTO) merchants, but do NOT include e-commerce environments.
Encryption-management service	A service that can be offered by a third-party P2PE component provider on behalf of P2PE solution providers. These entities manage and deploy POI devices and any resident P2PE applications and/or P2PE non-payment software, as covered in Domains 1 and 6 (and Annex A as applicable). See also *P2PE component provider.*

Term	Definition
Exclusive-OR (XOR)	Binary addition without carry, also known as "modulo 2 addition" and defined as: ▪ 0 + 0 = 0 ▪ 0 + 1 = 1 ▪ 1 + 0 = 1 ▪ 1 + 1 = 0
FIPS	Acronym for "Federal Information Processing Standard."
Firmware	Firmware is considered to be any code within the POI device that provides security protections needed to comply with PTS device security requirements or can impact compliance to these security requirements. Firmware may be further segmented by code necessary to meet PTS Core, OP, or SRED. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware. P2PE applications and P2PE non-payment software are also not considered firmware.
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: 1) Approved and configured to FIPS140-2 (level 3 or higher), or 2) Approved to the PCI HSM standard. See also *Secure cryptographic device.*
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.

Term	Definition
Hashing	Process of rendering cardholder data unreadable by converting data into a fixed-length message digest via *strong cryptography*. Hashing is a one-way (mathematical) function in which a non-secret algorithm takes any arbitrary length message as input and produces a fixed length output (usually called a "hash code" or "message digest"). A hash function should have the following properties: (1) It is computationally infeasible to determine the original input given only the hash code, (2) It is computationally infeasible to find two inputs that give the same hash code. Hashing must be applied to the entire PAN for the hash code to be considered rendered unreadable. It is recommended that hashed cardholder data include an input variable (for example, a "salt") to the hashing function to reduce or defeat the effectiveness of pre-computed rainbow table attacks. See also *Input variable*.
Host System	For hybrid decryption environments only. A combination of software and hardware components used for the purpose of decrypting account data, may also be used for transaction processing, and which is not considered an SCD.
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.
Input variable	Random data string that is concatenated with source data before a one-way hash function is applied. Input variables can help reduce the effectiveness of rainbow table attacks. See also *Hashing* and *Rainbow table attack.*
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.
International Organization for Standardization (ISO)	An international standards accreditation organization.

Term	Definition
Issuer	Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as "issuing bank" or "issuing financial institution."
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 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.
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-encrypting (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-injection facility (KIF)	Entities that perform cryptographic key injection.
Key-injection facility service	A service that can be offered by a third-party P2PE component provider on behalf of P2PE solution providers. KIF services entities perform cryptographic key injection as a stand-alone service, including for POI devices and HSMs used in P2PE solutions, as covered in Annex B and Annex A (as applicable). See also *P2PE component provider.*
Key instance	The occurrence of a key in one of its permissible forms, i.e., clear-text key, key components, encrypted key.

Term	Definition
Key loading	Process by which a key is manually or electronically transferred into an SCD.
Key-loading device (KLD)	An SCD that may be used to perform cryptographic key injection/loading or code signing.
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.
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.

Term	Definition
Message	A communication containing one or more transactions or related information.
Merchant	Any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.
Merchant decryption environment	See *Decryption environment.*
Merchant as a solution provider	A merchant who is acting as its own P2PE solution provider, responsible for role of solution provider in meeting, either directly or through use of outsourced P2PE components, all P2PE Domain requirements.
Merchant-managed solution (MMS)	A P2PE solution managed by a merchant rather than by a third-party solution provider. These merchant solutions are typically for large retail organizations who centrally manage the solution on behalf of their own encryption environments. In a merchant-managed solution, part of the merchant business plays the role of a P2PE solution provider (managing POIs, decryption environment, etc.) and part of the business plays the role of a "merchant" that has no access to clear-text account data, etc. Merchant-managed solutions are not eligible for PCI listing.
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.*
Open Protocols	Optional PTS POI module for POI devices using any communication method that uses a wireless, local, wide-area network, or a public domain protocol or security protocol to transport data. This would include but is not limited to: Bluetooth, Wi-Fi, cellular (GPRS, CDMA), or Ethernet, and a serial point-to-point connection that is wireless or through a hub, switch, or other multiport device.
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account. See also *Cardholder data.*
Password/passphrase	A string of characters that serves as an authenticator of the user.

Term	Definition
Payment processor	Sometimes referred to as “payment gateway” or “payment service provider (PSP)”. Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand. See also *Acquirer.*
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.
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* and *PCI-approved POI device.*
POI device type	Unique instance (combination) of a model name, hardware and firmware number.

Term	Definition
P2PE	Acronym for "point-to-point encryption"
P2PE application	All software or other files, *with access to clear-text account data,* that are intended for use in a P2PE solution and loaded onto a PCI-approved POI device, and that do not meet the PTS definition of "firmware." P2PE payment applications are assessed per all P2PE Domain 2 Requirements. PTS firmware is not considered a P2PE payment application and as such is not reassessed during a P2PE assessment. See also *Account data, Firmware,* and *P2PE non-payment software*
P2PE application vendor	A vendor that develops and then sells, distributes, or licenses any P2PE application for use in a P2PE solution. A P2PE solution provider may also be a P2PE application vendor.
P2PE component	A P2PE service (such as encryption management, decryption management, or key injection) that is accepted on a standalone basis as part of the P2PE Program and may be incorporated into and/or referenced as part of a P2PE solution. A P2PE service is assessed to a specific set of P2PE requirements and results in a PCI P2PE component provider listing. P2PE component providers' services are performed on behalf of other P2PE solution providers for use in P2PE solutions.
P2PE component provider	An entity that provides a service that is assessed to a specific set of P2PE requirements and that results in a P2PE component provider listing on the PCI SSC website. Component providers offer their services on behalf of other P2PE solution providers, intended for use in P2PE solutions. The following P2PE component providers can be separately assessed and PCI-listed: ▪ Encryption-management entity – See *Encryption-management service* ▪ Decryption-management entity – See *Decryption-management service* ▪ Key-injection facilities (KIF) – See *Key-injection facility service* ▪ Certification Authorities/Registration Authorities (CA/RA) – See *Certification Authority/Registration Authority service*.

Term	Definition
P2PE non-payment software	Any software or other files, *with no access to clear-text account data,* that are intended for use in a P2PE solution and loaded onto a PCI-approved POI device, and that do not meet the PTS definition of "firmware." P2PE non-payment software is assessed per designated P2PE Domain 1 Requirements. Note that this software is not subject to P2PE Domain 2 Requirements. PTS firmware is not considered P2PE non-payment software and as such is not reassessed during a P2PE assessment. See also *Account data* and *Firmware*
P2PE solution	A combination of secure devices, applications, and processes that encrypt cardholder data from a PCI-approved point-of-interaction (POI) device through to decryption, assessed in accordance with PCI's P2PE standard and included on PCI's list of Validated P2PE Solutions.
P2PE solution provider	An entity that: a) Designs, implements, and manages a P2PE solution for merchants (the P2PE solution provider may include outsourced P2PE components that cover 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. A P2PE solution provider may be a third-party entity such as a processor, acquirer, or payment gateway. A merchant can also be a solution provider (see also *Merchant as a solution provider* and *Merchant-managed 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.
Pseudo-random value	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.
Rainbow table attack	A method of data attack using a pre-computed table of hash strings (fixed-length message digest) to identify the original data source, usually for cracking password or cardholder data hashes.
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.
Registration Authority (RA)	An entity that performs registration services on behalf of a certification authority (CA). Registration authorities (RAs) work with a particular certification authority (CA) to vet requests for certificates that will then be issued by the certification authority. See also *Certification Authority* and *Certification Authority/Registration Authority service.*

Term	Definition
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).*
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.*
Secure Reading and Exchange of Data (SRED)	A set of PTS POI requirements that provide a standardized approach to protecting account data in POI devices. SRED requirements cover all methods of account-data entry supported by the POI device, and include physically and logically protecting account data within the device, protecting any associated sensitive data or functions, and providing for the encryption of account data before transmission outside the device.
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.

Term	Definition
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.
Solution provider	See *P2PE solution provider.*
Split knowledge	A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key. Also see *Dual control.*
Strong cryptography	Cryptography based on industry-tested and accepted algorithms, along with industry-tested and accepted key lengths and key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is "not reversible, or "one way"). See also *Hashing*. See *NIST Special Publication 800-57,* Part 1 (http://csrc.nist.gov/publications/) for more guidance on cryptographic key strengths and algorithms. See *P2PE Domain 6 Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms* for reference to specifics related to the P2PE standard.
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.
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.
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.

Term	Definition
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.
Terminal	A device/system that initiates a transaction.
Terminal master key (TMK)	A symmetric key used to encrypt other cryptographic keys at the point of interaction.
Test platform	In the context of Domain 2, special test functionality that is separate or absent from production-level code. This platform is expected to be provided by the application vendor to the P2PE assessor, as needed to provide a framework that allows for testing of the application's functionality outside of a production-deployment environment.
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.
Two-factor authentication	Method of authenticating a user whereby two or more factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN), or something the user is or does (such as fingerprints, other forms of biometrics, parametrics, etc.)
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
Unprotected memory	Components, devices, and recording media that retain data for some interval of time that reside outside the cryptographic boundary of an SCD.

Term	Definition
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.
Versioning methodology	A process of assigning version schemes to uniquely identify a particular state of an application or software. These schemes follow a version-number format, version-number usage, and any wildcard element as defined by the software vendor. Version numbers are generally assigned in increasing order and correspond to a particular change in the software.
Whitelist	A list of approved items used 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 a whitelist.
Whitelisting functionality	Functionality that utilizes an authorized and cryptographically authenticated whitelist to output permitted non-PCI payment brand account/card numbers. See *Whitelist*.
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.