Payment Card Industry (PCI)
Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS)

Glossary of Terms, Abbreviations, and Acronyms

Version 3.2

April 2016

Term	Definition
AAA	Acronym for "authentication, authorization, and accounting." Protocol for authenticating a user based on their verifiable identity, authorizing a user based on their user rights, and accounting for a user's consumption of network resources.
Access Control	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.*
Account Number	See *Primary Account Number (PAN).*
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.*
Administrative Access	Elevated or increased privileges granted to an account in order for that account to manage systems, networks and/or applications. Administrative access can be assigned to an individual's account or a built-in system account. Accounts with administrative access are often referred to as "superuser", "root", "administrator", "admin", "sysadmin" or "supervisor-state", depending on the particular operating system and organizational structure.
Adware	Type of malicious software that, when installed, forces a computer to automatically display or download advertisements.
AES	Abbreviation for "Advanced Encryption Standard." 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.*
ANSI	Acronym for "American National Standards Institute." Private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system.
Anti-Virus	Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called "malware") including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.
AOC	Acronym for "attestation of compliance." The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.
AOV	Acronym for "attestation of validation." The AOV is a form for PA-QSAs to attest to the results of a PA-DSS assessment, as documented in the PA-DSS Report on Validation.
Application	Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications.

Term	Definition
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.
Audit Log	Also referred to as "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Audit Trail	See *Audit Log.*
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.
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss.
BAU	An acronym for "business as usual." BAU is an organization's normal daily business operations.
Bluetooth	Wireless protocol using short-range communications technology to facilitate transmission of data over short distances.
Buffer Overflow	Vulnerability that is created from insecure coding methods, where a program overruns the buffer's boundary and writes data to adjacent memory space. Buffer overflows are used by attackers to gain unauthorized access to systems or data.
Card Skimmer	A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.

Term	Definition
Card Verification Code or Value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. (1) Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: ▪ **CAV –** Card Authentication Value (JCB payment cards) ▪ **PAN CVC –** Card Validation Code (MasterCard payment cards) ▪ **CVV –** Card Verification Value (Visa and Discover payment cards) ▪ **CSC –** Card Security Code (American Express) (2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand: ▪ **CID –** Card Identification Number (American Express and Discover payment cards) ▪ **CAV2 –** Card Authentication Value 2 (JCB payment cards) ▪ **PAN CVC2 –** Card Validation Code 2 (MasterCard payment cards) ▪ **CVV2 –** Card Verification Value 2 (Visa payment cards)
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See *Sensitive Authentication Data* for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
CDE	Acronym for “cardholder data environment.” The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
Cellular Technologies	Mobile communications through wireless telephone networks, including but not limited to Global System for Mobile communications (GSM), code division multiple access (CDMA), and General Packet Radio Service (GPRS).
CERT	Acronym for Carnegie Mellon University's “Computer Emergency Response Team.” The CERT Program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services.

Term	Definition
Change Control	Processes and procedures to review, test, and approve changes to systems and software for impact before implementation.
CIS	Acronym for "Center for Internet Security." Non-profit enterprise with mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls.
Column-Level Database Encryption	Technique or technology (either software or hardware) for encrypting contents of a specific column in a database versus the full contents of the entire database. Alternatively, see *Disk Encryption* or *File-Level Encryption.*
Compensating Controls	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: (1) Meet the intent and rigor of the original PCI DSS requirement; (2) Provide a similar level of defense as the original PCI DSS requirement; (3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and (4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. See "Compensating Controls" Appendices B and C in *PCI DSS Requirements and Security Assessment Procedures* for guidance on the use of compensating controls.
Compromise	Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Console	Screen and keyboard which permits access and control of a server, mainframe computer or other system type in a networked environment.
Consumer	Individual purchasing goods, services, or both.
Critical systems / critical technologies	A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. Examples of critical systems often include security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data. Considerations for determining which specific systems and technologies are critical will depend on an organization's environment and risk-assessment strategy.
Cross-Site Request Forgery (CSRF)	Vulnerability that is created from insecure coding methods that allows for the execution of unwanted actions through an authenticated session. Often used in conjunction with XSS and/or SQL injection.
Cross-Site Scripting (XSS)	Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection.

Term	Definition
Cryptographic Key	A value that determines the output of an encryption algorithm when transforming plain text to ciphertext. The length of the key generally determines how difficult it will be to decrypt the ciphertext in a given message. See *Strong Cryptography.*

Cryptographic Key Generation	Key generation is one of the functions within key management. The following documents provide recognized guidance on proper key generation:
	• NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation
	• ISO 11568-2 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle
	  ○ 4.3 Key generation
	• ISO 11568-4 Financial services — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle
	  ○ 6.2 Key life cycle stages — Generation
	• European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management
	  ○ 6.1.1 Key generation [for symmetric algorithms]
	  ○ 6.2.1 Key generation [for asymmetric algorithms]

Cryptographic Key Management	The set of processes and mechanisms which support cryptographic key establishment and maintenance, including replacing older keys with new keys as necessary.
Cryptography	Discipline of mathematics and computer science concerned with information security, particularly encryption and authentication. In applications and network security, it is a tool for access control, information confidentiality, and integrity.
Cryptoperiod	The time span during which a specific cryptographic key can be used for its defined purpose based on, for example, a defined period of time and/or the amount of cipher-text that has been produced, and according to industry best practices and guidelines (for example, *NIST Special Publication 800-57*).
CVSS	Acronym for "Common Vulnerability Scoring System." A vendor agnostic, industry open standard designed to convey the severity of computer system security vulnerabilities and help determine urgency and priority of response. Refer to *ASV Program Guide* for more information.
Data-Flow Diagram	A diagram showing how data flows through an application, system, or network.
Database	Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.
Database Administrator	Also referred to as "DBA." Individual responsible for managing and administering databases.

Term	Definition
Default Accounts	Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.
Default Password	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed.
Degaussing	Also called "disk degaussing." Process or technique that demagnetizes the disk such that all data stored on the disk is permanently destroyed.
Dependency	In the context of PA-DSS, a dependency is a specific software or hardware component (such as a hardware terminal, database, operating system, API, code library, etc.) that is necessary for the payment application to meet PA-DSS requirements.
Disk Encryption	Technique or technology (either software or hardware) for encrypting all stored data on a device (for example, a hard disk or flash drive). Alternatively, *File-Level Encryption* or *Column-Level Database Encryption* is used to encrypt contents of specific files or columns.
DMZ	Abbreviation for "demilitarized zone." Physical or logical sub-network that provides an additional layer of security to an organization's internal private network. The DMZ adds an additional layer of network security between the Internet and an organization's internal network so that external parties only have direct connections to devices in the DMZ rather than the entire internal network.
DNS	Acronym for "domain name system" or "domain name server." A system that stores information associated with domain names in a distributed database to provide name-resolution services to users on networks such as the Internet.
DSS	Acronym for "Data Security Standard." See *PA-DSS* and *PCI DSS.*
Dual Control	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 is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also *Split Knowledge.*)
Dynamic Packet Filtering	See *Stateful Inspection.*
ECC	Acronym for "Elliptic Curve Cryptography." Approach to public-key cryptography based on elliptic curves over finite fields. See *Strong Cryptography.*
Egress Filtering	Method of filtering outbound network traffic such that only explicitly allowed traffic is permitted to leave the network.

Term	Definition
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure. See *Strong Cryptography.*
Encryption Algorithm	Also called "cryptographic algorithm." A sequence of mathematical instructions used for transforming unencrypted text or data to encrypted text or data, and back again. See *Strong Cryptography.*
Entity	Term used to represent the corporation, organization or business which is undergoing a PCI DSS review.
File Integrity Monitoring	Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel.
File-Level Encryption	Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see *Disk Encryption* or *Column-Level Database Encryption.*
FIPS	Acronym for "Federal Information Processing Standards." Standards that are publicly recognized by the U.S. Federal Government; also for use by non-government agencies and contractors.
Firewall	Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
Forensics	Also referred to as "computer forensics." As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.
FTP	Acronym for "File Transfer Protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology. See *S-FTP*.
GPRS	Acronym for "General Packet Radio Service." Mobile data service available to users of GSM mobile phones. Recognized for efficient use of limited bandwidth. Particularly suited for sending and receiving small bursts of data, such as e-mail and web browsing.
GSM	Acronym for "Global System for Mobile Communications." Popular standard for mobile phones and networks. Ubiquity of GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world.

Term	Definition
Hashing	Process of rendering cardholder data unreadable by converting data into a fixed-length message digest. 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. In the context of PCI DSS, 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 *Input Variable*). For further guidance, refer to industry standards, such as current versions of NIST Special Publications 800-107 and 800-106, Federal Information Processing Standard (FIPS) 180-4 Secure Hash Standard (SHS), and FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.
Host	Main computer hardware on which computer software is resident.
Hosting Provider	Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.
HSM	Acronym for "hardware security module" or "host security module." 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.
HTTP	Acronym for "hypertext transfer protocol." Open internet protocol to transfer or convey information on the World Wide Web.
HTTPS	Acronym for "hypertext transfer protocol over secure socket layer." Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins.
Hypervisor	Software or firmware responsible for hosting and managing virtual machines. For the purposes of PCI DSS, the hypervisor system component also includes the virtual machine monitor (VMM).
ID	Identifier for a particular user or application.

Term	Definition
IDS	Acronym for "intrusion-detection system." Software or hardware used to identify and alert on network or system anomalies or intrusion attempts. Composed of: sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to detected security events. See *IPS*
IETF	Acronym for "Internet Engineering Task Force." Large, open international community of network designers, operators, vendors, and researchers concerned with evolution of Internet architecture and smooth operation of Internet. The IETF has no formal membership and is open to any interested individual.
IMAP	Acronym for "Internet Message Access Protocol." An application-layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server.
Index Token	A cryptographic token that replaces the PAN, based on a given index for an unpredictable value.
Information Security	Protection of information to ensure confidentiality, integrity, and availability.
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Ingress Filtering	Method of filtering inbound network traffic such that only explicitly allowed traffic is permitted to enter the network.
Injection Flaws	Vulnerability that is created from insecure coding techniques resulting in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and XPath injection.
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 Tables.*
Insecure Protocol/Service/Port	A protocol, service, or port that introduces security concerns due to the lack of controls over confidentiality and/or integrity. These security concerns include services, protocols, or ports that transmit data or authentication credentials (for example, password/passphrase) in clear-text over the Internet, or that easily allow for exploitation by default or if misconfigured. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.
IP	Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed and delivered from the source host to the destination host. IP is the primary network-layer protocol in the Internet protocol suite. See *TCP*.
IP Address	Also referred to as "internet protocol address." Numeric code that uniquely identifies a particular computer (host) on the Internet.

Term	Definition
IP Address Spoofing	Attack technique used to gain unauthorized access to networks or computers. The malicious individual sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host.
IPS	Acronym for "intrusion prevention system." Beyond an IDS, an IPS takes the additional step of blocking the attempted intrusion.
IPSEC	Abbreviation for "Internet Protocol Security." Standard for securing IP communications at the network layer by encrypting and/or authenticating all IP packets in a communication session.
ISO	In the context of industry standards and best practices, ISO, better known as "International Organization for Standardization" is a non-governmental organization consisting of a network of the national standards institutes.
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."
Issuing services	Examples of issuing services may include but are not limited to authorization and card personalization.
LAN	Acronym for "local area network." A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.
LDAP	Acronym for "Lightweight Directory Access Protocol." Authentication and authorization data repository utilized for querying and modifying user permissions and granting access to protected resources.
Least Privilege	Having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function.
Log	See *Audit Log.*
LPAR	Abbreviation for "logical partition." A system of subdividing, or partitioning, a computer's total resources—processors, memory and storage—into smaller units that can run with their own, distinct copy of the operating system and applications. Logical partitioning is typically used to allow the use of different operating systems and applications on a single device. The partitions may or may not be configured to communicate with each other or share some resources of the server, such as network interfaces.
MAC	In cryptography, an acronym for "message authentication code." A small piece of information used to authenticate a message. See *Strong Cryptography.*
MAC Address	Abbreviation for "media access control address." Unique identifying value assigned by manufacturers to network adapters and network interface cards.
Magnetic-Stripe Data	See *Track Data.*

Term	Definition
Mainframe	Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design.
Malicious Software / Malware	Software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See *Truncation* for protection of PAN when stored in files, databases, etc.
Memory-Scraping Attacks	Malware activity that examines and extracts data that resides in memory as it is being processed or which has not been properly flushed or overwritten.
Merchant	For the purposes of the PCI DSS, a merchant is defined as 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. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
MO/TO	Acronym for "Mail-Order/Telephone-Order."
Monitoring	Use of systems or processes that constantly oversee computer or network resources for the purpose of alerting personnel in case of outages, alarms, or other predefined events.
MPLS	Acronym for "multi-protocol label switching." Network or telecommunications mechanism designed for connecting a group of packet-switched networks.
Multi-Factor Authentication	Method of authenticating a user whereby at least two 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, etc.).
NAC	Acronym for "network access control" or "network admission control." A method of implementing security at the network layer by restricting the availability of network resources to endpoint devices according to a defined security policy.

Term	Definition
NAT	Acronym for "network address translation." Also known as network masquerading or IP masquerading. Change of an IP address used within one network to a different IP address known within another network, allowing an organization to have internal addresses that are visible internally, and external addresses that are only visible externally.
Network	Two or more computers connected together via physical or wireless means.
Network Administrator	Personnel responsible for managing the network within an entity. Responsibilities typically include but are not limited to network security, installations, upgrades, maintenance and activity monitoring.
Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
Network Diagram	A diagram showing system components and connections within a networked environment.
Network Security Scan	Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.
Network Segmentation	Also referred to as "segmentation" or "isolation." Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment. See the Network Segmentation section in the *PCI DSS Requirements and Security Assessment Procedures* for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement.
Network Sniffing	Also referred to as "packet sniffing" or "sniffing." A technique that passively monitors or collects network communications, decodes protocols, and examines contents for information of interest.
NIST	Acronym for "National Institute of Standards and Technology." Non-regulatory federal agency within U.S. Commerce Department's Technology Administration.
NMAP	Security-scanning software that maps networks and identifies open ports in network resources.
Non-Console Access	Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks.
Non-Consumer Users	Individuals, excluding cardholders, who access system components, including but not limited to employees, administrators, and third parties.
NTP	Acronym for "Network Time Protocol." Protocol for synchronizing the clocks of computer systems, network devices and other system components.

Term	Definition
NVD	Acronym for "National Vulnerability Database." The U.S. government repository of standards-based vulnerability management data. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.
OCTAVE®	Acronym for "Operationally Critical Threat, Asset, and Vulnerability Evaluation." A suite of tools, techniques, and methods for risk-based information security strategic assessment and planning.
Off-the-Shelf	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Operating System / OS	Software of a computer system that is responsible for the management and coordination of all activities and the sharing of computer resources. Examples of operating systems include Microsoft Windows, Mac OS, Linux and Unix.
Organizational Independence	An organizational structure that ensures there is no conflict of interest between the person or department performing the activity and the person or department assessing the activity. For example, individuals performing assessments are organizationally separate from the management of the environment being assessed.
OWASP	Acronym for "Open Web Application Security Project." A non-profit organization focused on improving the security of application software. OWASP maintains a list of critical vulnerabilities for web applications. (See http://www.owasp.org).
PA-DSS	Acronym for "Payment Application Data Security Standard."
PA-QSA	Acronym for "Payment Application Qualified Security Assessor." PA-QSAs are qualified by PCI SSC to assess payment applications against the PA-DSS. Refer to the *PA-DSS Program Guide* and *PA-QSA Qualification Requirements* for details about requirements for PA-QSA Companies and Employees.
Pad	In cryptography, the one-time pad is an encryption algorithm with text combined with a random key or "pad" that is as long as the plain-text and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable
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.
Parameterized Queries	A means of structuring SQL queries to limit escaping and thus prevent injection attacks.
Password / Passphrase	A string of characters that serve as an authenticator of the user.
PAT	Acronym for "port address translation" and also referred to as "network address port translation." Type of *NAT* that also translates the port numbers.
Patch	Update to existing software to add functionality or to correct a defect.

Term	Definition
Payment Application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties. Refer to *PA-DSS Program Guide* for details.
Payment Cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.
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	Acronym for "Payment Card Industry."
PCI DSS	Acronym for "Payment Card Industry Data Security Standard."
PDA	Acronym for "personal data assistant" or "personal digital assistant." Handheld mobile devices with capabilities such as mobile phones, e-mail, or web browser.
PED	PIN entry device.
Penetration Test	Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.
Personal Firewall Software	A software firewall product installed on a single computer.
Personally Identifiable Information	Information that can be utilized to identify or trace an individual's identity including but not limited to name, address, social security number, biometric data, date of birth, etc.
Personnel	Full-time and part-time employees, temporary employees, contractors, and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.
PIN	Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.

Term	Definition
PIN Block	A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.
POI	Acronym for "Point of Interaction," 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.
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures
POP3	Acronym for "Post Office Protocol v3." Application-layer protocol used by e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
Port	Logical (virtual) connection points associated with a particular communication protocol to facilitate communications across networks.
POS	Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.
Private Network	Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers. See also *Public Network*.
Privileged User	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use.
Procedure	Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.
Protocol	Agreed-upon method of communication used within networks. Specification describing rules and procedures that computer products should follow to perform activities on a network.
Proxy Server	A server that acts as an intermediary between an internal network and the Internet. For example, one function of a proxy server is to terminate or negotiate connections between internal and external connections such that each only communicates with the proxy server.
PTS	Acronym for "PIN Transaction Security," PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals. Please refer to www.pcisecuritystandards.org.

Term	Definition
Public Network	Network established and operated by a third party telecommunications provider for specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks include, but are not limited to, the Internet, wireless, and mobile technologies. See also *Private Network*.
PVV	Acronym for "PIN verification value." Discretionary value encoded in magnetic stripe of payment card.
QIR	Acronym for "Qualified Integrator or Reseller." Refer to the *QIR Program Guide* on the PCI SSC website for more information.
QSA	Acronym for "Qualified Security Assessor." QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the *QSA Qualification Requirements* for details about requirements for QSA Companies and Employees.
RADIUS	Abbreviation for "Remote Authentication Dial-In User Service." Authentication and accounting system. Checks if information such as username and password that is passed to the RADIUS server is correct, and then authorizes access to the system. This authentication method may be used with a token, smart card, etc., to provide multi-factor authentication.
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.
Re-keying	Process of changing cryptographic keys. Periodic re-keying limits the amount of data encrypted by a single key.
Remote Access	Access to computer networks from a location outside of that network. Remote access connections can originate either from inside the company's own network or from a remote location outside the company's network. An example of technology for remote access is *VPN*.
Remote Lab Environment	A lab that is not maintained by the PA-QSA.
Removable Electronic Media	Media that store digitized data and which can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and external/portable hard drives.
Reseller / Integrator	An entity that sells and/or integrates payment applications but does not develop them.
RFC 1918	The standard identified by the Internet Engineering Task Force (IETF) that defines the usage and appropriate address ranges for private (non-internet routable) networks.

Term	Definition
Risk Analysis / Risk Assessment	Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
Risk Ranking	A defined criterion of measurement based upon the risk assessment and risk analysis performed on a given entity.
ROC	Acronym for "Report on Compliance." Report documenting detailed results from an entity's PCI DSS assessment.
Rootkit	Type of malicious software that when installed without authorization, is able to conceal its presence and gain administrative control of a computer system.
Router	Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.
ROV	Acronym for "Report on Validation." Report documenting detailed results from a PA-DSS assessment for purposes of the PA-DSS program.
RSA	Algorithm for public-key encryption described in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at Massachusetts Institute of Technology (MIT); letters RSA are the initials of their surnames.
S-FTP	Acronym for Secure-FTP. S-FTP has the ability to encrypt authentication information and data files in transit. See *FTP.*
Sampling	The process of selecting a cross-section of a group that is representative of the entire group. Sampling may be used by assessors to reduce overall testing efforts, when it is validated that an entity has standard, centralized PCI DSS security and operational processes and controls in place. Sampling is not a PCI DSS requirement.
SANS	Acronym for "SysAdmin, Audit, Networking and Security," an institute that provides computer security training and professional certification. (See www.sans.org.)
SAQ	Acronym for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS assessment.
Schema	Formal description of how a database is constructed including the organization of data elements.
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.
SDLC	Acronym for "system development life cycle" or "software development lifecycle." Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation.

Term	Definition
Secure Coding	The process of creating and implementing applications that are resistant to tampering and/or compromise.
Secure Cryptographic Device	A set of hardware, software and firmware that implements cryptographic processes (including cryptographic algorithms and key generation) and is contained within a defined cryptographic boundary. Examples of secure cryptographic devices include host/hardware security modules (HSMs) and point-of-interaction devices (POIs) that have been validated to PCI PTS.
Secure Wipe	Also called "secure delete," a method of overwriting data residing on a hard disk drive or other digital media, rendering the data irretrievable.
Security Event	An occurrence considered by an organization to have potential security implications to a system or its environment. In the context of PCI DSS, security events identify suspicious or anomalous activity.
Security Officer	Primary person responsible for an entity's security-related matters.
Security Policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information
Security Protocols	Network communications protocols designed to secure the transmission of data. Examples of security protocols include, but are not limited to TLS, IPSEC, SSH, HTTPS, etc.
Sensitive Area	Any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.
Sensitive Authentication Data	Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
Separation of Duties	Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.
Server	Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP.
Service Code	Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

Term	Definition
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves *only* the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
Session Token	In the context of web session management, a session token (also referred to as a "session identifier" or "session ID"), is a unique identifier (such as a "cookie") used to track a particular session between a web browser and a webserver.
SHA-1/SHA-2	Acronym for "Secure Hash Algorithm." A family or set of related cryptographic hash functions including SHA-1 and SHA-2. See *Strong Cryptography.*
Smart Card	Also referred to as "chip card" or "IC card (integrated circuit card)." A type of payment card that has integrated circuits embedded within. The circuits, also referred to as the "chip," contain payment card data including but not limited to data equivalent to the magnetic-stripe data.
SNMP	Acronym for "Simple Network Management Protocol." Supports monitoring of network attached devices for any conditions that warrant administrative attention.
Split Knowledge	A method by which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.
Spyware	Type of malicious software that when installed, intercepts or takes partial control of the user's computer without the user's consent.
SQL	Acronym for "Structured Query Language." Computer language used to create, modify, and retrieve data from relational database management systems.
SQL Injection	Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database.
SSH	Abbreviation for "Secure Shell." Protocol suite providing encryption for network services like remote login or remote file transfer.
SSL	Acronym for "Secure Sockets Layer." Industry standard that encrypts the channel between a web browser and web server. Now superseded by TLS. See *TLS.*

Term	Definition
Stateful Inspection	Also called "dynamic packet filtering." Firewall capability that provides enhanced security by keeping track of the state of network connections. Programmed to distinguish legitimate packets for various connections, only packets matching an established connection will be permitted by the firewall; all others will be rejected.
Strong Cryptography	Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is "one way"; that is, not reversible). See *Hashing.* At the time of publication, examples of industry-tested and accepted standards and algorithms include AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher). See the current version of NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) for more guidance on cryptographic key strengths and algorithms. ***Note:*** *The above examples are appropriate for persistent storage of cardholder data. The minimum cryptography requirements for transaction-based operations, as defined in PCI PIN and PTS, are more flexible as there are additional controls in place to reduce the level of exposure.* *It is recommended that all new implementations use a minimum of 128-bits of effective key strength.*
SysAdmin	Abbreviation for "system administrator." Individual with elevated privileges who is responsible for managing a computer system or network.
System Components	Any network devices, servers, computing devices, or applications included in or connected to the cardholder data environment.
System-level object	Anything on a system component that is required for its operation, including but not limited to database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components.
TACACS	Acronym for "Terminal Access Controller Access Control System." Remote authentication protocol commonly used in networks that communicates between a remote access server and an authentication server to determine user access rights to the network. This authentication method may be used with a token, smart card, etc., to provide multi-factor authentication.
TCP	Acronym for "Transmission Control Protocol." One of the core transport-layer protocols of the Internet Protocol (IP) suite, and the basic communication language or protocol of the Internet. See *IP*.
TDES	Acronym for "Triple Data Encryption Standard" and also known as "3DES" or "Triple DES." Block cipher formed from the DES cipher by using it three times. See *Strong Cryptography.*

Term	Definition
TELNET	Abbreviation for "telephone network protocol." Typically used to provide user-oriented command line login sessions to devices on a network. User credentials are transmitted in clear text.
Threat	Condition or activity that has the potential to cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization
TLS	Acronym for "Transport Layer Security." Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
Token	In the context of authentication and access control, a token is a value provided by hardware or software that works with an authentication server or VPN to perform dynamic or multi-factor authentication. See *RADIUS, TACACS,* and *VPN.* See also *Session Token*.
Track Data	Also referred to as "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.
Transaction Data	Data related to electronic payment card transaction.
Trojan	Also referred to as "Trojan horse." A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user's knowledge.
Truncation	Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when *stored* in files, databases, etc. See *Masking* for protection of PAN when *displayed* on screens, paper receipts, etc.
Trusted Network	Network of an organization that is within the organization's ability to control or manage.
Untrusted Network	Network that is external to the networks belonging to an organization and which is out of the organization's ability to control or manage.
URL	Acronym for "Uniform Resource Locator." A formatted text string used by Web browsers, e-mail clients, and other software to identify a network resource on the Internet.
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.

Term	Definition
Virtual Appliance (VA)	A VA takes the concept of a pre-configured device for performing a specific set of functions and run this device as a workload. Often, an existing network device is virtualized to run as a virtual appliance, such as a router, switch, or firewall.
Virtual Hypervisor	See *Hypervisor*.
Virtual Machine	A self-contained operating environment that behaves like a separate computer. It is also known as the "Guest," and runs on top of a hypervisor.
Virtual Machine Monitor (VMM)	The VMM is included with the hypervisor and is software that implements virtual machine hardware abstraction. It manages the system's processor, memory, and other resources to allocate what each guest operating system requires.
Virtual Payment Terminal	A virtual payment terminal is web-browser-based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Virtual Switch or Router	A virtual switch or router is a logical entity that presents network infrastructure level data routing and switching functionality. A virtual switch is an integral part of a virtualized server platform such as a hypervisor driver, module, or plug-in.
Virtualization	Virtualization refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including applications, desktops, networks, and storage.
VLAN	Abbreviation for "virtual LAN" or "virtual local area network." Logical local area network that extends beyond a single traditional physical local area network.
VPN	Acronym for "virtual private network." A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.
Vulnerability	Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.

Term	Definition
WAN	Acronym for "wide area network." Computer network covering a large area, often a regional or company-wide computer system.
Web Application	An application that is generally accessed via a web browser or through web services. Web applications may be available via the Internet or a private, internal network.
Web Server	Computer that contains a program that accepts HTTP requests from web clients and serves the HTTP responses (usually web pages).
WEP	Acronym for "Wired Equivalent Privacy." Weak algorithm used to encrypt wireless networks. Several serious weaknesses have been identified by industry experts such that a WEP connection can be cracked with readily available software within minutes. See *WPA.*
Wildcard	A character that may be substituted for a defined subset of possible characters in an application version scheme. In the context of PA-DSS, wildcards can optionally be used to represent a non-security impacting change. A wildcard is the only variable element of the vendor's version scheme, and is used to indicate there are only minor, non-security-impacting changes between each version represented by the wildcard element.
Wireless Access Point	Also referred to as "AP." Device that allows wireless communication devices to connect to a wireless network. Usually connected to a wired network, it can relay data between wireless devices and wired devices on the network.
Wireless Networks	Network that connects computers without a physical connection to wires.
WLAN	Acronym for "wireless local area network." Local area network that links two or more computers or devices without wires.
WPA/WPA2	Acronym for "WiFi Protected Access." Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA.