Payment Card Industry (PCI) Data Security Standard

Glossary, Abbreviations and Acronyms

Term	Definition
AAA	Authentication, authorization, and accounting protocol
Accounting	Tracking of users' network resources
Access control	Mechanisms that limit availability of information or information processing resources only to authorized persons or applications
Account harvesting	Process of identifying existing user accounts based on trial and error. [Note: Providing excessive information in error messages can disclose enough to make it easier for an attacker to penetrate and 'harvest' or compromise the system.]
Account number	Payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Primary Account Number (PAN)
Acquirer	Bankcard association member that initiates and maintains relationships with merchants that accept payment cards
AES	Advanced encryption standard. Block cipher adopted by NIST in November 2001. Algorithm is specified in FIPS PUB 197
ANSI	American National Standards Institute. Private, non-profit organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system
Anti-Virus Program	Programs capable of detecting, removing, and protecting against various forms of malicious code or malware, including viruses, worms, Trojan horses, spyware, and adware
Application	Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications
Approved Standards	Approved standards are standardized algorithms (like in ISO and ANSI) and well-known commercially available standards (like Blowfish) that meet the intent of strong cryptography. Examples of approved standards are AES (128 bits and higher), TDES (two or three independent keys), RSA (1024 bits) and ElGamal (1024 bits)
Asset	Information or information processing resources of an organization
Audit Log	Chronological record of system activities. Provides a 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. Sometimes specifically referred to as security audit trail
Authentication	Process of verifying identity of a subject or process
Authorization	Granting of access or other rights to a user, program, or process
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss
Cardholder	Customer to whom a card is issued or individual authorized to use the card

Term	Definition
Cardholder data	Full magnetic stripe or the PAN plus any of the following: • Cardholder name • Expiration date • Service Code
Cardholder data environment	Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment
Card Validation Value or Code	Data element on a card's magnetic stripe that uses secure cryptographic process 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) • **CVC** Card Validation Code (MasterCard payment cards) • **CVV** Card Verification Value (Visa and Discover payment cards) • **CSC** Card Security Code (American Express) *Note: The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:* • **CID** Card Identification Number (American Express and Discover payment cards) • **CAV2** Card Authentication Value 2 (JCB payment cards) • **CVC2** Card Validation Code 2 (MasterCard payment cards) • **CVV2** Card Verification Value 2 (Visa payment cards)
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 stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 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
CIS	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
Compromise	Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected

Term	Definition
Console	Screen and keyboard which permits access and control of the server or mainframe computer in a networked environment
Consumer	Individual purchasing goods, services, or both
Cookies	String of data exchanged between a web server and a web browser to maintain a session. Cookies may contain user preferences and personal information
Cryptography	Discipline of mathematics and computer science concerned with information security and related issues, particularly encryption and authentication and such applications as access control. In computer and network security, a tool for access control and information confidentiality
Database	Structured format for organizing and maintaining easily retrieved information. Simple database examples are tables and spreadsheets
Data Base Administrator (DBA)	Database Administrator. Individual responsible for managing and administering databases
DBA (Doing Business As)	Doing business as. Compliance validation levels are based on transaction volume of a DBA or chain of stores (not of a corporation that owns several chains)
Default accounts	System login account predefined in a manufactured system to permit initial access when system is first put into service
Default password	Password on system administration or service accounts when system is shipped from the manufacturer; usually associated with default account. Default accounts and passwords are published and well known
DES	Data Encryption Standard (DES). Block cipher elected as the official Federal Information Processing Standard (FIPS) for the United States in 1976. Successor is the Advanced Encryption Standard (AES)
DMZ	Demilitarized zone. Network added between a private and a public network to provide additional layer of security
DNS	Domain name system or domain name server. System that stores information associated with domain names in a distributed database on networks, such as the Internet
DSS	Data Security Standard
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”
ECC	Elliptic curve cryptography. Approach to public-key cryptography based on elliptic curves over finite fields
Egress	Traffic exiting a network across a communications link and into the customer's 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
FIPS	Federal Information Processing Standard
Firewall	Hardware, software, or both that protect resources of one network from intruders from other networks. Typically, an enterprises with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources
FTP	File transfer protocol
GPRS	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	Global System for Mobile Communications. Popular standard for mobile phones 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
Host	Main computer hardware on which computer software is resident
Hosting Provider	Offer 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
HTTP	Hypertext transfer protocol. Open-internet protocol to transfer or convey information on the World Wide Web
ID	Identity
IDS/IPS	Intrusion Detection System/ Intrusion Prevention System. Used to identify and alert on network or system intrusion attempts. Composed of sensors which 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 security events detected. An IPS takes the additional step of blocking the attempted intrusion.
IETF	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. Open to any interested individual
Information Security	Protection of information to insure confidentiality, integrity, and availability
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information

Term	Definition
Ingress	Traffic entering the network from across a communications link and the customer's network
Intrusion detection Systems	See IDS
IP	Internet protocol. Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite
IP address	Numeric code that uniquely identifies a particular computer on the Internet
IP Spoofing	Technique used by an intruder to gain unauthorized access to computers. Intruder sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host
IPSEC	Internet Protocol Security (IPSEC). Standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSEC provides security at the network layer
ISO	International Organization for Standardization. Non-governmental organization consisting of a network of the national standards institutes of over 150 countries, with one member per country and a central secretariat in Geneva, Switzerland that coordinates the system
ISO 8583	Established standard for communication between financial systems
Key	In cryptography, a key is an algorithmic value applied to unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message
L2TP	Layer 2 tunneling protocol. Protocol used to support virtual private networks (VPNs)
LAN	Local area network. Computer network covering a small area, often a building or group of buildings
LPAR	Logical partition. Section of a disk which is not one of the primary partitions. Defined in a data block pointed to by the extended partition
MAC	Message authentication code
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business
Malware	Malicious software. Designed to infiltrate or damage a computer system, without the owner's knowledge or consent
Monitoring	Use of system that constantly oversees a computer network including for slow or failing systems and that notifies the user in case of outages or other alarms
MPLS	Multi protocol label switching.

Term	Definition
NAT	Network address translation. 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
Network	Two or more computers connected together to share resources
Network Components	Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances
Network Security Scan	Automated tool that remotely checks merchant or service provider systems for vulnerabilities. Non-intrusive test involves probing external-facing systems based on external-facing IP addresses and reporting on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network
NIST	National Institute of Standards and Technology. Non-regulatory federal agency within U.S. Commerce Department's Technology Administration. Mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology to enhance economic security and improve quality of life
Non consumer users	Any individual, excluding consumer customers, that accesses systems, including but not limited to employees, administrators, and third parties
NTP	Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks
OWASP	Open Web Application Security Project (see http://www.owasp.org)
Payment Cardholder Environment	That part of the network that possesses cardholder data or sensitive authentication data
PAN	Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number
Password	A string of characters that serve as an authenticator of the user
Pad	Packet assembler/disassembler. Communication device that formats outgoing data and strips data out of incoming packets. 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 plaintext and used only once. Additionally, if key is truly random, never reused, and, kept secret, the one-time pad is unbreakable
PAT	Port address translation. Feature of a network address translation (NAT) device that translates transmission control protocol (TCP) or user datagram protocol (UDP) connections made to a host and port on an outside network to a host and port on an inside network
Patch	Quick-repair job for piece of programming. During software product beta test or try-out period and after product formal release, problems are found. A patch is provided quickly to users

Term	Definition
PCI	Payment Card Industry
Penetration	Successful act of bypassing security mechanisms and gaining access to computer system
Penetration Test	Security-oriented probing of computer system or network to seek out vulnerabilities that an attacker could exploit. Beyond probing for vulnerabilities, this testing may involve actual penetration attempts. The objective of a penetration test is to detect identify vulnerabilities and suggest security improvements
PIN	Personal identification number
Policy	Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures
POS	Point of sale
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 that describes rules and procedures that computer products should follow to perform activities on a network
Public Network	Network established and operated by a telecommunications provider or recognized private company, for specific purpose of providing data transmission services for the public. Data must be encrypted during transmission over public networks as hackers easily and commonly intercept, modify, and/or divert data while in transit. Examples of public networks in scope of PCI DSS include the Internet, GPRS, and GSM.
PVV	PIN verification value. Encoded in magnetic stripe of payment card
RADIUS	Remote authentication and 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
RFC	Request for comments
Re-keying	Process of changing cryptographic keys to limit amount of data to be encrypted with the same key
Risk Analysis	Process that systematically 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 assessment
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
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

Term	Definition
Sanitization	Process for deleting sensitive data from a file, device, or system; or for modifying data so that it is useless if accessed in an attack
SANS	SysAdmin, Audit, Network, Security Institute (See www.sans.org)
Security Officer	Primary responsible person for security related affairs of an organization
Security policy	Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction
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 providers 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, authentication, DNS, mail, proxy, and NTP
Service Code	Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.
Service Provider	Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members 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. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded
SHA	Secure Hash Algorithm. A family or set of related cryptographic hash functions. SHA-1 is most commonly used function. Use of unique salt value in the hashing function reduces the chances of a hashed value collision
SNMP	Simple Network Management Protocol. Supports monitoring of network-attached devices for any conditions that warrant administrative attention
Split knowledge	Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key
SQL	Structured (English) 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. An attacker executes unauthorized SQL commands by taking advantage of insecure code on 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

Term	Definition
SSH	Secure shell. Protocol suite providing encryption for network services like remote login or remote file transfer
SSID	Service set identifier. Name assigned to wireless WiFi or IEEE 802.11 network
SSL	Secure sockets layer. Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel
Strong Cryptography	General term to indicate cryptography that is extremely resilient to cryptanalysis. That is, given the cryptographic method (algorithm or protocol), the cryptographic key or protected data is not exposed. The strength relies on the cryptographic key used. Effective size of the key should meet the minimum key size of comparable strengths recommendations. One reference for minimum comparable strength notion is NIST Special Publication 800-57, August, 2005 (http://csrc.nist.gov/publications/) or others that meet the following minimum comparable key bit security: • 80 bits for secret key based systems (for example TDES) • 1024 bits modulus for public key algorithms based on the factorization (for example, RSA) • 1024 bits for the discrete logarithm (for example, Diffie-Hellman) with a minimum 160 bits size of a large subgroup (for example, DSA) • 160 bits for elliptic curve cryptography (for example, ECDSA)
System Components	Any network component, server, or application included in or connected to the cardholder data environment
TACACS	Terminal access controller access control system. Remote authentication protocol
Tamper-resistance	System that is difficult to modify or subvert, even for an assailant with physical access to the system
TCP	Transmission control protocol
TDES	Triple Data Encription Standard also known as 3DES. Block cipher formed from the DES cipher by using it three times
TELNET	Telephone network protocol. Typically used to provide user-oriented command line login sessions between hosts on the internet. Program originally designed to emulate a single terminal attached to the other computer
Threat	Condition that may 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	Transport layer security. Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL
Token	Device that performs dynamic authentication
Transaction data	Data related to electronic payment
Truncation	Practice of removing data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits

Term	Definition
Two-factor authentication	Authentication that requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors
UDP	User datagram protocol
UserID	A character string used to uniquely identify each user of a system
Virus	Program or string of code that can replicate itself and cause modification or destruction of software or data
VPN	Virtual private network. Private network established over a public network
Vulnerability	Weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy
Vulnerability Scan	Scans used to identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network
WEP	Wired equivalent privacy. Protocol to prevent accidental eavesdropping and intended to provide comparable confidentiality to traditional wired network. Does not provide adequate security against intentional eavesdropping (for example, cryptanalysis)
WPA	WiFi Protected Access (WPA and WPA2). Security protocol for wireless (WiFi) networks. Created in response to several serious weaknesses in the WEP protocol
XSS	Cross-site scripting. Type of security vulnerability typically found in web applications. Can be used by an attacker to gain elevated privilege to sensitive page content, session cookies, and variety of other objects