Security
Standards Council®

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	authenticating a user based on their verifiable identity, authorizing a user 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

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 o 4.3 Key generation ISO 11568-4 Financial services Key management (retail) Part 4: Asymmetric cryptosystems Key management and life cycle o 6.2 Key life cycle stages Generation European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management o 6.1.1 Key generation [for symmetric algorithms] o 6.2.1 Key generation [for asymmetric algorithms]

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	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*

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	A sequence of mathematical instructions used for transforming unencrypted text or data to encrypted text or data, and back again. See

Term	Definition
IDS	- 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	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.

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

Term	Definition
NVD	he U.S. government repository of standards-based vulnerability management data. NVD includes databases of security checklists, security-related software flaws,

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	
PCI DSS	Data Security Standard
PDA	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	

Term	Definition
PIN Block	A block of data used

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	magnetic stripe of payment card.
QIR	Refer to the *QIR Program Guide* on the PCI SSC website for more information.
QSA	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	- 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	

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.

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	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 -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	

Term

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
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	Abbrevi area network that extends beyond a single traditional physical local area network.
VPN	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.