Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms

Term	Definition
Account	Also referred to as "user ID," "account ID," or "application ID." Used to identify an individual or process on a computer system. See *Authentication Credentials* and *Authentication Factor*.
Account Data	Account data consists of cardholder data and/or sensitive authentication data. See *Cardholder Data* and *Sensitive Authentication Data*.
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution." Entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See *Payment Processor*.
Administrative Access	Elevated or increased privileges granted to an account 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.
AES	Acronym for "Advanced Encryption Standard." See *Strong Cryptography.*
ANSI	Acronym for "American National Standards Institute."
Anti-Malware	Software that is designed to detect, and remove, block, or contain various forms of malicious software.
AOC	Acronym for "Attestation of Compliance." The AOC is the official PCI SSC form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in a Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC).
Application	Includes all purchased, custom, and bespoke software programs or groups of programs, including both internal and external (for example, web) applications.
Application and System Accounts	Also referred to as "service accounts." Accounts that execute processes or perform tasks on a computer system or in an application. These accounts usually have elevated privileges that are required to perform specialized tasks or functions and are not typically accounts used by an individual.
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.

Term	Definition
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.
Authentication	Process of verifying identity of an individual, device, or process. Authentication typically occurs with one or more authentication factors. See *Account, Authentication Credential,* and *Authentication Factor.*
Authentication Credential	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process. See *Account* and *Authentication Factor.*
Authentication Factor	The element used to prove or verify the identity of an individual or process on a computer system. Authentication typically occurs with one or more of the following authentication factors: • 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 element. The ID (or account) and authentication factor together are considered authentication credentials. See *Account* and *Authentication Credential.*
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 refers to the authorization process, which completes when a merchant receives a transaction response (for example, an approval or decline).
BAU	Acronym for “Business as Usual.”
Bespoke and Custom Software	*Bespoke software* is developed for the entity by a third party on the entity’s behalf and per the entity’s specifications. *Custom software* is developed by the entity for its own use.
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.
Card Verification Code	Also referred to as Card Validation Code or Value, or Card Security Code. For PCI DSS purposes, it is the three- or four-digit value printed on the front or back of a payment card. May be referred to as CAV2, CVC2, CVN2, CVV2, or CID according to the individual Participating Payment Brands. For more information, contact the Participating Payment Brands.

Term	Definition
Cardholder	Customer to which a payment card is issued, or any individual authorized to use the payment card. See *Visitor.*
Cardholder Data (CHD)	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 might be transmitted or processed (but not stored) as part of a payment transaction.
CDE	Acronym for "Cardholder Data Environment." The CDE is comprised of: • The system components, people, and processes that store, process, or transmit cardholder data and/or sensitive authentication data, and, • System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.
CERT	Acronym for "Computer Emergency Response Team."
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."
Cleartext Data	Unencrypted data.
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* and *File-Level Encryption*.
Commercial Off-the-Shelf (COTS)	Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Compensating Controls	See PCI DSS Appendices B and C.
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	Directly connected screen and/or keyboard which permits access and control of a server, mainframe computer, or other system type. See *Non-Console Access*.

Term	Definition
Consumer	Individual cardholder purchasing goods, services, or both.
Critical systems	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.
Cryptographic Algorithm	Also referred to as “encryption algorithm.” A clearly specified reversible mathematical process used for transforming cleartext data to encrypted data, and vice versa. See *Strong Cryptography.*
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that is used for operations such as: • Transforming cleartext data into ciphertext data, • Transforming ciphertext data into cleartext data, • A digital signature computed from data, • Verifying a digital signature computed from data, • An authentication code computed from data, or • An exchange agreement of a shared secret. 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* – 4.1.1 Key generation [for symmetric algorithms] – 4.2.1 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.

Term	Definition
Cryptoperiod	The time span during which a cryptographic key can be used for its defined purpose. Often defined in terms of the period for which the key is active and/or the amount of ciphertext that has been produced by the key, and according to industry best practices and guidelines (for example, *NIST Special Publication 800-57*).
Customized Approach	See PCI DSS section: *8 Approaches for Implementing and Validating PCI DSS.*
CVSS	Acronym for “Common Vulnerability Scoring System.” Refer to *ASV Program Guide* for more information.
Data-Flow Diagram	A diagram showing how and where data flows through an entity’s applications, systems, networks, and to/from external parties.
Default Account	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.
Defined Approach	See PCI DSS section: *8 Approaches for Implementing and Validating PCI DSS.*
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.
DNS	Acronym for “Domain Name System.”
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 *Split Knowledge*.
ECC	Acronym for “Elliptic Curve Cryptography.” See *Strong Cryptography*.
E-commerce (web) Redirection Server	A server that redirects a customer browser from a merchant’s website to a different location for payment processing during an ecommerce transaction.

Term	Definition
Encryption	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text, i.e., to hide the information content of the data. See *Strong Cryptography*.
Encryption Algorithm	See *Cryptographic Algorithm*.
Entity	In the context of a PCI DSS assessment, a term used to represent the corporation, organization, or business which is undergoing an assessment.
File Integrity Monitoring (FIM)	A change-detection solution that checks for changes, additions, and deletions to critical files, and notifies when such changes are detected.
File-Level Encryption	Technique or technology (either software or hardware) for encrypting the full contents of specific files. Alternatively, see *Disk Encryption* and *Column-Level Database Encryption*.
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. Investigations into compromises of payment data are typically conducted by a PCI Forensic Investigator (PFI).
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 cleartext. FTP can be implemented securely via SSH or other technology.
Hashing	A method to protect data that converts 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"). Hash functions are required to have the following properties: • It is computationally infeasible to determine the original input given only the hash code, • It is computationally infeasible to find two inputs that give the same hash code.
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.
IDS	Acronym for "intrusion-detection system."

Term	Definition
Index Token	A random value from a table of random values that corresponds to a given PAN.
Interactive Login	The process of an individual providing authentication credentials to directly log into an application or system account. Using interactive login means there is no accountability or traceability of actions taken by that individual.
IPS	Acronym for "intrusion prevention system."
ISO	Acronym for "International Organization for Standardization."
Issuer	Also referred to as "issuing bank" or "issuing financial institution." Entity that issues payment cards or performs, facilitates, or supports issuing services, including but not limited to issuing banks and issuing processors.
Issuing services	Examples of issuing services include but are not limited to authorization and card personalization.
Keyed Cryptographic Hash	A hashing function that incorporates a randomly generated secret key to provide brute force attack resistance and secret authentication integrity. Appropriate keyed cryptographic hashing algorithms include but are not limited to: HMAC, CMAC, and GMAC, with an effective cryptographic strength of at least 128-bits (*NIST SP 800-131Ar2).* Refer to the following for more information about HMAC, CMAC, and GMAC, respectively: *NIST SP 800-107r1, NIST SP 800-38B, and NIST SP 800-38D).* See *NIST SP 800-107 (Revision 1): Recommendation for Applications Using Approved Hash Algorithms* §5.3.
Key Custodian	A role where a person(s) is entrusted with, and responsible for, performing key management duties involving secret and/or private keys, key shares, or key components on behalf of an entity.
Key Management System	A combination of hardware and software that provides an integrated approach for generating, distributing, and/or managing cryptographic keys for devices and applications.
LAN	Acronym for "local area network."
LDAP	Acronym for "Lightweight Directory Access Protocol."
Least Privileges	The minimum level of privileges necessary to perform the roles and responsibilities of the job function.

Term	Definition
Legal Exception	A legal restriction due to a local or regional law, regulation, or regulatory requirement, where meeting a PCI DSS requirement would violate that law, regulation, or regulatory requirement. Contractual obligations or legal advice are **not** legal restrictions. See the following PCI DSS v4.x documents for information on reporting legal exceptions: • *The Report on Compliance (ROC) Template* and related *Attestations of Compliance*. • *The Self-Assessment Questionnaires (SAQs)* and related *Attestations of Compliance*. *Note: Where an entity operates in multiple locations, a legal exception may only be claimed for the locations governed by the law, regulation, or regulatory requirement, and may not be claimed for locations in which such law, regulation, or regulatory requirement is inapplicable.*
Log	See *Audit Log*.
Logical Access Control	Mechanisms that limit the availability of information or information-processing resources only to authorized persons or applications. See *Physical Access Control*.
MAC	In cryptography, an acronym for “message authentication code.” See *Strong Cryptography*.
Magnetic-Stripe Data	See *Track Data*.
Masking	Method of concealing a segment of PAN when displayed or printed. Masking is used when there is no business need to view the entire PAN. Masking relates to protection of PAN when displayed on screens, paper receipts, printouts, etc. See *Truncation* for protection of PAN when electronically stored, processed, or transmitted.
Media	Physical material, including but not limited to, electronic storage devices, removable electronic media, and paper reports.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand as payment for goods and/or services. 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.”
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 and other biometric elements).

Term	Definition
Multi-Tenant Service Provider	A type of Third-Party Service Provider that offers various shared services to merchants and other service providers, where customers share system resources (such as physical or virtual servers), infrastructure, applications (including Software as a Service (SaaS)), and/or databases. Services may include, but are not limited to, hosting multiple entities on a single shared server, providing e-commerce and/or "shopping cart" services, web-based hosting services, payment applications, various cloud applications and services, and connections to payment gateways and processors. See *Service Provider* and *Third-Party Service Provider*.
NAC	Acronym for "Network Access Control."
NAT	Acronym for "Network Address Translation."
Network Connection	A logical, physical, or virtual communication path between devices that allows the transmission and reception of network layer packets.
Network Diagram	A diagram showing system components and connections within a networked environment.
Network Security Controls (NSC)	Firewalls and other network security technologies that act as network policy enforcement points. NSCs typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules.
NIST	Acronym for "National Institute of Standards and Technology." Non-regulatory federal agency within U.S. Commerce Department's Technology Administration.
Non-Console Access	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.
NTP	Acronym for "Network Time Protocol."
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."
PAN	Acronym for "primary account number." Unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the issuer and the cardholder account.

Term	Definition
Password / Passphrase	A string of characters that serve as an authentication factor for a user or account.
Patch	Update to existing software to add function or to correct a defect.
Participating Payment Brand	Also referred to as “payment brand.” A payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. At the time of writing, Participating Payment Brands include PCI SSC Founding Members and Strategic Members.
Payment Brand	An organization with branded payment cards or other payment card form factors. Payment brands regulate where and how the payment cards or other form factors carrying its brand or logo are used. A payment brand may be a PCI SSC Participating Payment Brand or other global or regional payment brand, scheme, or network.
Payment Card Form Factor	Includes physical payment cards as well as devices with functionality that emulates a payment card to initiate a payment transaction. Examples of such devices include, but are not limited to, smartphones, smartwatches, fitness bands, key tags, and wearables such as jewelry.
Payment Cards	For purposes of PCI DSS, any payment card form factor that bears the logo of any PCI SSC Participating Payment Brand.
Payment Channel	Methods used by merchants to accept payments from customers. Common payment channels include card present (in person) and card not present (e-commerce and MO/TO).
Payment Page	A web-based user interface containing one or more form elements intended to capture account data from a consumer or submit captured account data, for purposes of processing and authorizing payment transactions. The payment page can be rendered as any one of: • A single document or instance, • A document or component displayed in an inline frame within a non-payment page, • Multiple documents or components each containing one or more form elements contained in multiple inline frames within a non-payment page.
Payment Page Scripts	Any programming language commands or instructions on a payment page that are processed and/or interpreted by a consumer’s browser, including commands or instructions that interact with a page’s document object model. Examples of programming languages are JavaScript and VB script; neither markup-languages (for example, HTML) or style-rules (for example, CSS) are programming languages.

Term	Definition
Payment Processor	Sometimes referred to as “payment gateway” or “payment service provider (PSP).” Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. See *Acquirers.*
PCI DSS	Acronym for “Payment Card Industry Data Security Standard.”
Personnel	Full-time and part-time employees, temporary employees, contractors, and consultants with security responsibilities for protecting account data or that can impact the security of cardholder data and/or sensitive authentication data. See *Visitor.*
Phishing Resistant Authentication	Authentication designed to prevent the disclosure and use of authentication secrets to any party that is not the legitimate system to which the user is attempting to authenticate (for example, through in-the-middle (ITM) or impersonation attacks). Phishing-resistant systems often implement asymmetric cryptography as a core security control. Systems that rely solely on knowledge-based or time-limited factors such as passwords or one-time-passwords (OTPs) are not considered phishing resistant, nor are SMS or magic links. Examples of phishing-resistant authentication includes FIDO2.
Physical Access Control	Mechanisms that limit the access to a physical space or environment to only authorized persons. See *Logical Access Control*.
PIN	Acronym for “personal identification number.”
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 the PAN (or a truncation thereof) depending on the approved ISO PIN Block Format used.
POI	Acronym for “Point of Interaction,” the initial point where data is read from a card.
Point of Sale System (POS)	Hardware and software used by merchants to accept payments from customers. May include POI devices, PIN pads, electronic cash registers, etc.
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.
QIR	Acronym for “Qualified Integrator or Reseller.” Refer to the *QIR Program Guide* on the PCI SSC website for more information.

Term	Definition
QSA	Acronym for “Qualified Security Assessor.” QSA companies are qualified by PCI SSC to validate an entity’s adherence to PCI DSS requirements. Refer to the *QSA Qualification Requirements* for details about requirements for QSA Companies and Employees.
Remote Access	Access to an entity’s network from a location outside of that network. An example of technology for remote access is a VPN.
Removable Electronic Media	Media that stores digitized data that 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. In this context, removable electronic media does not include hot-swappable drives, tape drives used for bulk back-ups, or other media not typically used to transport data from one location for use in another.
Risk Assessment	Enterprise-wide 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 to minimize total exposure. See *Targeted Risk Analysis*.
Risk Ranking	Process of classifying risks to identify, prioritize, and address items in the order of importance.
ROC	Acronym for “Report on Compliance.” Reporting tool used to document detailed results from an entity’s PCI DSS assessment.
RSA	Algorithm for public-key encryption. See *Strong Cryptography*.
SAQ	Acronym for “Self-Assessment Questionnaire.” Reporting tool used to document self-assessment results from an entity’s PCI DSS assessment.
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. See PCI DSS section: *4 Scope of PCI DSS Requirements*.
Secure Coding	The process of creating and implementing applications that are resistant to tampering and/or compromise.
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.
Segmentation	Also referred to as “network segmentation” or “isolation.” Segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. See “Segmentation” in PCI DSS section: *4 Scope of PCI DSS Requirements*.

Term	Definition
Sensitive Area	A sensitive area is typically a subset of the CDE and is any area that houses systems considered critical to the CDE. This includes data centers, server rooms, back-office rooms at retail locations, and any area that concentrates or aggregates cardholder data storage, processing, or transmission. Sensitive areas also include areas housing systems that manage or maintain the security of the CDE (for example, those providing network security controls or that manage physical or logical security). This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store or call centers where agents are taking payments.
Sensitive Authentication Data (SAD)	Security-related information used to authenticate cardholders and/or authorize payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.
Separation of Duties	Practice of dividing steps in a function among multiple individuals, to prevent a single individual from subverting the process.
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.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data (CHD) and/or sensitive authentication data (SAD) on behalf of another entity. This includes payment gateways, payment service providers (PSPs), and independent sales organizations (ISOs). This also includes companies that provide services that control or could impact the security of CHD and/or SAD. 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). See *Multi-Tenant Service Provider* and *Third-Party Service Provider.*
SNMP	Acronym for “Simple Network Management Protocol.”.
Split Knowledge	A method by which two or more entities separately have key components or key shares that individually convey no knowledge of the resultant cryptographic key.
SQL	Acronym for “Structured Query Language.”
SSH	Abbreviation for “Secure Shell.”
SSL	Acronym for “Secure Sockets Layer.”

Term	Definition
Strong Cryptography	Cryptography is a method to protect data through a reversible encryption process, and is a foundational primitive used in many security protocols and services. Strong cryptography is 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. Effective key strength can be shorter than the actual 'bit' length of the key, which can lead to algorithms with larger keys providing lesser protection than algorithms with smaller actual, but larger effective, key sizes. *It is recommended that all new implementations use a minimum of 128-bits of effective key strength.* Examples of industry references on cryptographic algorithms and key lengths include: • *NIST Special Publication 800-57 Part 1,* • *BSI TR-02102-1,* • *ECRYPT-CSA D5.4 Algorithms, Key Size and Protocols Report (2018), and* • *ISO/IEC 18033 Encryption algorithms, and* • *ISO/IEC 14888-3:2-81 IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*.
System Components	Any network devices, servers, computing devices, virtual components, or software included in or connected to the CDE, or that could impact the security of cardholder data and/or sensitive authentication data.
System-level object	Anything on a system component that is required for its operation, including but not limited to 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.
Targeted Risk Analysis	For PCI DSS purposes, a risk analysis that focuses on a specific PCI DSS requirement(s) of interest, either because the requirement allows flexibility (for example, as to frequency) or, for the Customized Approach, to explain how the entity assessed the risk and determined the customized control meets the objective of a PCI DSS requirement.
TDES	Acronym for "Triple Data Encryption Standard." Also referred to as "3DES" or "Triple DES."
Telnet	Abbreviation for "telephone network protocol."
Third-Party Service Provider (TPSP)	Any third party acting as a service provider on behalf of an entity. See *Multi-Tenant Service Provider* and *Service Provider*.
Third-Party Software	Software that is acquired by, but not developed expressly for, an entity. It may be open source, freeware, shareware, or purchased.
TLS	Acronym for "Transport Layer Security."

Term	Definition
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.
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 track data on the magnetic stripe.
Truncation	Method of rendering a full PAN unreadable by removing a segment of PAN data. Truncation relates to protection of PAN when electronically stored, processed, or transmitted. See *Masking* for protection of PAN when displayed on screens, paper receipts, etc.
Trusted Network	Network of an entity that is within the entity’s ability to control or manage and that meets applicable PCI DSS requirements.
Untrusted Network	Any network that does not meet the definition of a “trusted network.”
Virtual Payment Terminal	In the context of Self-Assessment Questionnaire (SAQ) C-VT, 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 through a 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.
Virtualization	The logical abstraction of computing resources from physical and/or logical 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. Other common abstractions include, but are not limited to, containers, serverless computing, or microservices.
Visitor	A vendor, guest of any personnel, service worker, or personnel that normally do not have access to the subject area. Cardholders present in a retail location to purchase goods or services are not considered “visitors.” See *Cardholder* and *Personnel.*
VPN	Acronym for “virtual private network.”
Vulnerability	Flaw or weakness which, if exploited, may result in an intentional or unintentional compromise of a system.
Web Application	An application that is generally accessed through a web browser or through web services. Web applications may be available through the Internet or a private, internal network.