支付卡行业（PCI）
数据安全标准（DSS）
和支付应用程序
数据安全标准（PA-DSS）

术语、缩写词和首字母缩略词词汇表

3.2 版

2016 年 4 月

术语	定义
AAA	“验证、授权和计帐”的缩写。该协议用于根据用户可验证身份对用户进行验证，基于用户权限进行授权，以及记录用户对网络资源的占用量。
访问控制	限制信息或信息处理资源可用性使其仅供授权人员或应用程序使用的机制。
帐户数据	帐户数据包括持卡人数据和/或敏感验证数据。请参见*持卡人数据*和*敏感验证数据*。
帐户	请参见*主帐户 (PAN)*。
收单机构	也称为“商业银行”、“收单银行”或“收单金融机构”。收单机构是为商户处理支付卡交易的实体，通常为金融机构，由支付品牌定义。收单机构须遵从有关商户合规性的支付品牌规则和程序。另请参见*支付处理商*。
管理访问	为使某帐户能够管理系统、网络和/或应用程序而赋予的升级或更高权限。 管理访问可以分配给个人帐户或内置系统帐户。拥有管理访问权限的帐户通常被称为“超级用户”、“根用户”、“管理员”、“系统管理员”或“主管状态”，根据具体的操作系统和组织结构而定。
广告软件	一种恶意软件，安装后会迫使计算机自动显示或下载广告。
AES	“高级加密标准”的缩写。对称密钥加密中使用的分组密码，由 NIST 于 2001 年 11 月采用其作为美国 FIPS PUB 197 标准（或称“FIPS 197”）。请参见*强效加密法*。
ANSI	“美国国家标准学会”的缩写。管理和协调美国自愿性标准和符合性评定系统的私有非盈利组织。
杀毒	可检测、移除和防范各种形式的恶意软件（包括病毒、蠕虫、特洛伊或特洛伊木马、间谍软件、广告软件和 rootkit 内核型病毒）的程序或软件。
AOC	“遵从性证明书”的缩写。AOC 是商户和服务提供商用于证明 PCI DSS 评估结果的表格，记录于自我评估调查问卷或遵从性报告。
AOV	“认证证明”的缩写。AOV 是 PA-QSA 用于证明 PA-DSS 评估结果的表格，记录于 PA-DSS 认证报告。
应用程序	包括所有购买和定制的软件程序或程序组，包括内部和外部（例如 web）应用程序。
ASV	“授权扫描服务商”的缩写。由 PCI SSC 授权可执行外部漏洞扫描服务的公司。
检查日志	也称为“检查记录”。系统活动的序时记录。提供独立可验证的记录，可用于重建、审核和检查从交易启动到获得最终结果过程中的一系列围绕或导致操作、程序或事件的环境和活动。
检查记录	请参见*检查日志*。
验证	确认个人、设备或流程身份的流程。通常通过使用一个或多个验证因素进行验证，例如： ▪ 所知，如密码或口令等 ▪ 所有，如令牌设备或智能卡等 ▪ 个人特征，如生物特征等
验证凭证	用户 ID 或帐户 ID 以及用于验证个人、设备或流程身份的验证因素相结合。

术语	定义
授权	就访问控制而言，授权是将访问权限或其他权限授予用户、程序或流程。授权定义了个人或程序在成功验证后可进行的操作。 就支付卡交易而言，在收单机构与发卡机构/处理机构验证交易后，商户获得交易许可时，则发生授权。
备份	复制数据副本以用于存档或以防损坏或丢失。
BAU	“常规业务”的缩写。BAU 是组织常规的日常业务操作。
蓝牙	采用短范围通信技术的无线协议，便于短距离的数据传输。
缓冲区溢出	非安全编码方法所引起的漏洞，这种情况下程序超出了缓存区的限制，并将数据写入相邻的内存空间。攻击者会利用缓存区溢出在未授权的情况下访问系统或数据。
读卡器	一种物理设备，通常连接到合法的读卡设备，用于非法捕获和/或存储支付卡中的信息。
卡验证代码或值	也称为卡认证代码或值，或者卡安全码。指以下两种中的某一种：(1) 磁条数据或 (2) 印上的安全特征。 (1) 卡片磁条上的数据元素，利用安全的加密流程来保护磁条上的数据完整性，并显示所有改动和伪造。根据支付卡品牌称为 CAV、CVC、CVV 或 CSC。下面列出了各支付卡品牌的术语： ▪ **CAV** - 卡验证值（JCB 支付卡） ▪ **PAN CVC** - 卡认证代码（MasterCard 支付卡） ▪ **CVV** - 卡验证值（Visa 和 Discover 支付卡） ▪ **CSC** - 卡安全代码 (American Express) (2) 对于 Discover、JCB、MasterCard 和 Visa 支付卡，第二类卡验证值或代码是印在卡背面签名栏区域中最右边的三位值。对于 American Express 支付卡，安全代码是印在支付卡正面 PAN 上方未突出显示的四位号码。该代码是唯一的，与每张个人信用卡相关联，并将 PAN 与信用卡相关联。下面列出了各支付卡品牌的术语： ▪ **CID** - 卡识别码（American Express 和 Discover 支付卡） ▪ **CAV2** - 卡验证值 2（JCB 支付卡） ▪ **PAN CVC2** - 卡认证代码 2（MasterCard 支付卡） ▪ **CVV2** - 卡验证值 2（Visa 支付卡）
持卡人	支付卡发给的非消费者或消费者客户或者任何被授权使用支付卡的个人。
持卡人数据	持卡人数据至少包含完整 PAN。持卡人数据还可能以完整 PAN 加上以下任何信息的形式显示：持卡人姓名、失效日和/或业务码 关于可能在支付交易中传输或处理（但不存储）的其他数据元素，请参见*敏感验证数据*。
CDE	“持卡人数据环境”的缩写。存储、处理或传输持卡人数据或敏感验证数据的人员、流程和技术。
蜂窝技术	通过无线电话网络进行的移动通信，包括但不限于全球移动通信系统 (GSM)、码分多址 (CDMA) 和通用分组无线业务 (GPRS)。

术语	定义
CERT	卡内基梅隆大学的“计算机紧急响应小组”的缩写。CERT 计划发展并推广采用适用技术和系统管理方法，以抵抗联网系统上的攻击、限制损害以及确保关键服务的连续性。
变更控制	审核、测试和批准系统和软件变更以便在实施前施加影响的流程和程序。
CIS	“互联网安全中心”的缩写。非盈利企业，其任务为帮助组织降低因技术安全控制不足导致的业务和电子商务中断的风险。
列级数据库加密	用于加密的技巧或技术（软件或硬件），加密内容为数据库中的特定列内容，而不是整个数据库的全部内容。或者，请参见*磁盘加密*或*文件级加密*。
补偿性控制	当实体因合理的技术限制或书面业务限制无法满足明确指定的要求，但已通过实施其他控制充分降低与该要求相关的风险时，可能需要考虑引入补偿性控制。补偿性控制必须： (1) 符合最初 PCI DSS 要求的目的和严格程度； (2) 提供与最初 PCI DSS 要求级别类似的防线； (3) “超越”其他 PCI DSS 要求（不仅仅是符合其他 PCI DSS 要求）；以及 (4) 与不遵守 PCI DSS 要求导致的其他风险相称。 关于补偿性控制使用的相关指南，请参见*《PCI DSS 要求和安全评估程序》*中的“补偿性控制”附录 B 和 C。
威胁	也称为“数据威胁”或“数据漏洞”。对计算机系统的入侵，其中涉嫌持卡人数据的非授权披露/盗窃、修改或销毁。
控制台	允许访问和控制联网环境中的服务器、大型机或其他系统类型的屏幕和键盘。
消费者	购买商品、服务或商品和服务的个人。
关键系统 / 关键技术	被实体视为特别重要的系统或技术。例如，关键系统可能对于企业经营的业绩或安全功能的维护至关紧要。关键系统往往包括安全系统、面向公众的设备和系统、数据库以及存储、处理或传输持卡人数据的系统。确定具体关键系统和关键技术的考虑因素取决于组织的环境和风险评估策略。
跨站请求伪造 (CSRF)	非安全编码方法所引起的漏洞，该漏洞通过验证会话允许执行不需要的操作。通常与 XSS 和/或 SQL 注入一起使用。
跨站脚本 (XSS)	非安全编码技术所引起的漏洞，该漏洞会导致不正确的输入认证。通常与 CSRF 和/或 SQL 注入一起使用。
密钥	在将纯文本转换为密文时决定加密算法输出的值。通常，密钥的长度决定特定消息中密文的解密难度。请参见*强效加密法*。

术语	定义

密钥生成	密钥的生成是密钥管理中的职能之一。下列文件提供了关于适当密钥生成的公认指导：
	• NIST 特别出版物 800-133：对密钥生成的建议（Recommendation for Cryptographic Key Generation）
	• ISO 11568-2 Financial services — 密钥管理（零售）— 第 2 部分：对称加密算法，其密钥管理和生命周期
	  o 4.3 密钥生成
	• ISO 11568-4 Financial services — 密钥管理（零售）— 第 4 部分：非对称密码系统 - 密钥管理和生命周期
	  o 6.2 密钥寿命周期阶段 — 生成
	• 欧洲支付委员会 EPC 342-08 关于算法使用和密钥管理的指导
	  o 6.1.1 密钥生成［对称算法］
	  o 6.2.1 密钥生成［非对称算法］

密钥管理	支持密钥建立和维护（包括在必要时使用新密钥替换旧密钥）的流程和机制集合。
加密法	与信息安全（尤其是加密和验证）相关的数学和计算机科学规章制度。在应用程序和网络安全中，它是用于访问控制、信息机密性和完整性的工具。
密钥周期	特定密钥可用于指定目的的时间段，基于指定期限和/或密文生成的数量等，且符合行业最优方法和指南（例如 *《NIST 特别出版物 800-57》*）。
CVSS	“通用漏洞评分系统”的缩写。供应商无关的行业开放标准，旨在传达计算机系统安全漏洞的严重程度以及帮助确定响应的紧急程度和优先级。更多信息，请参见 *《ASV 计划指南》*。
数据流程图	显示数据在应用程序、系统或网络间的流动方式的图表。
数据库	便于整理和维护可检索信息的结构化格式。简单的数据库包括表格和电子表格等。
数据库管理员	也称为“DBA”。负责管理数据库的个人。
默认帐户	系统、应用程序或设备中预定义的登录帐户，允许系统首次交付使用后的初次访问。系统也可能在安装流程中生成其他默认帐户。
默认密码	系统、应用程序或设备中预定义的关于系统管理员、用户或服务帐户的密码；通常与默认帐户相关。默认帐户和密码会对外发布，因此很容易猜出。
消磁	也称为“磁盘消磁”。对磁盘消磁以致存储在磁盘上的所有数据永久销毁的流程或技术。
依赖条件	就 PA-DSS 而言，依赖条件是支付应用程序满足 PA-DSS 要求所必须的特定软件或硬件组件（例如软件终端、数据库、操作系统、API、代码库等）。
磁盘加密	用于加密所有存储在设备（例如硬盘或闪存驱动器）上的数据的技巧或技术（软件或硬件）。或者，使用 *文件级加密*或 *列级数据库加密*加密特定文件或列的内容。

术语	定义
DMZ	“非军事区”的缩写。为组织的内部专用网络提供其他安全层的物理或逻辑子网络。DMZ 在互联网和组织的内部网络之间添加了额外的网络安全层，以确保外部各方仅能直接连接到 DMZ 中的设备，而不能连接到整个内部网络。
DNS	“域名系统”或“域名服务器”的缩写。在分布式数据库中存储域名的相关信息以便向各网络（如互联网）上的用户提供名称解析服务的系统。
DSS	“数据安全标准”的缩写。请参见 *PA-DSS* 和 *PCI DSS*。
双重控制	需要两个或更多的单独实体（通常是个人）共同操作以便保护敏感功能或信息的流程。两个实体共同负责存在漏洞的交易中相关材料的物理保护。不允许单独的个人访问或使用材料（例如密钥）。对于手动密钥生成、转易、加载、存储和恢复，双重控制需要在实体之间分割密钥知识 （另请参见*分割知识*）。
动态数据包过滤	请参见*状态检查*。
ECC	“椭圆曲线加密法”的缩写。基于有限域上椭圆曲线的公开密钥加密方法。请参见*强效加密法*。
出口过滤	过滤输出网络流量以致只有明确允许的流量才能离开网络的方法。
加密	将信息转化为只有特定密钥持有者才能理解的形式的过程。利用加密保护加密流程和解密流程（加密的逆过程）之间的信息防止非授权的泄漏。请参见*强效加密法*。
加密算法	也称为“加密的算法”。用于将未加密的文本或数据转换为加密的文本或数据并复原的数学指令的序列。请参见*强效加密法*。
实体	用于表示正在接受 PCI DSS 审查的公司、组织或企业的术语。
文件完整性监控	监控特定文件或日志以检测它们是否被修改的技巧或技术。当重要文件或日志被修改时，应向相关的安全人员发出警报。
文件级加密	用于加密特定文件的全部内容的技巧或技术（软件或硬件）。或者，请参见*磁盘加密*或*列级数据库加密*。
FIPS	“联邦信息处理标准”的缩写。美国联邦政府公开认可的标准；也为非政府机构和承包商所用。
防火墙	阻止非授权访问网络资源的硬件和/或软件技术。防火墙会根据规则和其他标准的集合允许或阻止不同安全级别的网络间的计算机流量。
取证	也称为“计算机取证”。它涉及信息安全，包括应用调查工具和分析技术从计算机资源中收集证据以确定数据遭受威胁的原因。
FTP	“文件传输协议”的缩写。用于将数据通过公共网络（例如互联网）从一台计算机传输到另一台计算机的网络协议。一般认为 FTP 是非安全协议，因为密码和文件内容是在无保护的情况下以明文形式发送的。FTP 可通过 SSH 或其他技术安全实施。请参见 *S-FTP*。

术语	定义
GPRS	“通用分组无线业务”的缩写。提供给 GSM 手机用户的移动数据业务。因可有效利用有限的带宽而得到认可。尤其适合发送和接受小型数据突发（如电子邮件和网络浏览）。
GSM	“全球移动通信系统”的缩写。手机和网络的流行标准。GSM 标准的普遍性使得手机运营商之间的国际漫游很常见，让订阅者能够在世界上的很多地方使用自己的手机。
散列	通过将数据转化为固定长度的消息摘要实现持卡人数据不可读的流程。散列是单向（数学）函数，其中非秘密算法会将任一任意长度的消息作为输入，生成固定长度的输出（通常称为“散列代码”或“消息摘要”）。散列函数应具备以下特性： (1) 只知道散列代码，通过计算不可能确定原始输入， (2) 通过计算不可能找到散列代码相同的两个输入。 就 PCI DSS 而言，散列必须应用于整个 PAN，因为散列代码被视为不可读。建议散列持卡人数据在散列函数中添加输入变量（例如“salt”）以使预先计算的彩虹表攻击降低或失去有效性（请参见*输入变量*）。 如需获得更多指导，请参见行业标准，例如《NIST 特别出版物 800-107》和《NIST 特别出版物 800-106》的最新版本、《联邦信息处理标准 (FIPS) 180-4 安全散列标准》、以及《FIPS 202 SHA-3 标准》：基于排列的散列和可延长的输出功能。
主机	安装计算机软件的主要计算机硬件。
托管服务提供商	向商户和其他服务提供商提供各类服务。服务多种多样，有简单有复杂；包括服务器上的共享空间和所有“购物车”选项；也包括支付应用程序和连接到支付网关和处理器的连接；还包括专用托管服务和每台服务器托管一个客户的服务。托管服务提供商可能是在单台服务器上托管多个实体的共享托管服务提供商。
HSM	“硬件安全模块”或“主机安全模块”的缩写。物理和逻辑上受保护的硬件设备，会提供加密服务的安全集合以用于密钥管理函数和/或帐户数据的解密。
HTTP	“超文本传输协议”的缩写。传输和传递万维网上的信息的开放互联网协议。
HTTPS	“安全套接层上超文本传输协议”的缩写。万维网上提供验证和加密通信的安全 HTTP，针对安全敏感性通信（如基于网络的登录）设计。
监控程序	负责托管和管理虚拟机的软件或固件。就 PCI DSS 而言，监控程序系统组件还包括虚拟机监控 (VMM)。
ID	特定用户或应用程序的标识符。
IDS	“入侵检测系统”的缩写。用于识别和警报网络或系统异常或入侵尝试的软件或硬件。包含：生成安全事件的传感器；监控事件和警报以及控制传感器的控制台；记录数据库中传感器记录事件的中心引擎。使用规则系统来生成警报以响应检测到的安全事件。请参见 *IPS*
IETF	“互联网工程任务组”的缩写。与互联网架构的演变以及互联网的稳定运转相关的互联网设计人员、操作人员、供应商和研究人员组成的大型开放国际社区。IETF 没有正式的成员，对任何感兴趣的个人开放。

术语	定义
IMAP	“互联网消息访问协议”的缩写。允许电子邮件客户访问远程邮件服务器上的电子邮件的应用层互联网协议。
索引令牌	根据特定索引用一个不可预测的值替代 PAN 的加密令牌。
信息安全	保护信息以确保其保密性、完整性和可用性。
信息系统	整理的结构化数据资源的离散集，用于收集、处理、维护、使用、共享、传播或清除信息。
入口过滤	过滤输入网络流量以致只有明确允许的流量才能进入网络的方法。
注入攻击	非安全编码技术所引起的漏洞，会导致不正确的输入认证，从而让攻击者能够通过网络应用程序将恶意代码中继到底层系统。这类漏洞包括 SQL 注入、LDAP 注入和 XPath 注入。
输入变量	在应用单向散列函数之前与源数据组合的随机数据字符串。输入字符串可帮助降低彩虹表攻击的有效性。另请参见*散列*和*彩虹表*。
非安全协议/服务/端口	由于缺乏对保密性和/或完整性的控制而引入安全问题的协议、服务或端口。这些安全问题包括以明文形式通过互联网传输数据或验证凭证（例如密码/口令）的服务、协议或端口，或者默认情况下或错误配置的情况下很容易被利用的服务、协议或端口。非安全服务、协议或端口包括但不限于 FTP、Telnet、POP3、IMAP 以及 SNMP 1 版和 2 版。
IP	“互联网协议”的缩写。包含地址信息和某些控制信息的网络层协议，使数据包能够路由至以及通过源主机传输至目标主机。IP 是互联网协议套件中的主要互联网层协议。请参见*TCP*。
IP 地址	也称为“互联网协议地址”。识别互联网上特定计算机（主机）的唯一数字代码。
IP 地址欺骗	非授权访问网络或计算机的攻击技术。恶意个人会利用表明消息来源于受信任主机的 IP 地址发送欺骗消息。
IPS	“入侵防御系统”的缩写。超越 IDS，IPS 会执行额外的步骤阻止入侵企图。
IPSEC	“互联网协议安全”的缩写。通过加密和/或验证通信会话中所有 IP 数据包以保护网络层中 IP 通信安全的标准。
ISO	在行业标准和最佳实践背景下，ISO，即“国际标准化组织”是一个由国家标准学会网络组成的非政府组织。 Issuer
发卡机构	发行支付卡或者提供、促进或支持发卡服务的实体，包括但不限于发卡银行和发卡处理机构。也称为“发卡银行”或“发卡金融机构”。
发卡服务	发卡服务可能包括但不限于授权和卡片个性化等。
LAN	“局域网”的缩写。共享公用通信线的一组计算机和/或其他设备，通常在同一建筑或建筑群中。
LDAP	“轻量级目录访问协议”的缩写。用于查询和修改用户权限以及对受保护的资源授予访问权限的验证和授权数据存放。
最小权限	拥有行使工作职能的角色和责任所需的最小访问权限和/或权限。

术语	定义
日志	请参见*检查日志*。
LPAR	“逻辑分区”的缩写。将计算机总资源（处理器、内存和存储）细分或分割为可独立运行的较小单元、操作系统和应用程序的不同副本的系统。逻辑分区通常用于允许在单一设备上使用不同的操作系统和应用程序。分区可针对是否互相通信或共享服务器的某些资源（如互联网接口）进行配置。
MAC	在加密法中，“消息验证代码”的缩写。用于验证消息的小块信息。请参见*强效加密法*。
MAC 地址	“媒介访问控制地址”的缩写。制造商分配给网络适配器和网络接口卡的唯一识别值。
磁条数据	请参见*磁道数据*。
大型机	用处理海量数据输入和输出以及专门针对吞吐量计算的计算机。大型机能够运行多个操作系统，像是作为多个计算机运行一样。许多遗留系统采用大型机设计。
恶意的软件/恶意软件	在所有者不知情或未经所有者同意的情况下潜入或破坏计算机系统，意图破坏所有者数据、应用程序或操作系统的保密性、完整性或可用性的软件或固件。这类软件一般在很多业务许可活动中进入网络，从而利用系统漏洞。示例包括病毒、蠕虫病毒、特洛伊（或特洛伊木马）、间谍软件、广告软件和 rootkit 内核型病毒。
掩盖	就 PCI DSS 而言，显示或打印时隐藏数据分段的方法。查看完整的 PAN 没有业务要求时使用掩盖。掩盖与显示或打印时的 PAN 保护有关。关于存储在文件、数据库等时 PAN 的保护，请参见*截词*。
内存刮擦攻击	检查或提取内存中正在处理的数据或未正确刷新或覆盖的数据的恶意软件活动。
商户	就 PCI DSS 而言，商户定义为接受使用 PCI SSC 支付卡（带有 American Express、Discover、JCB、MasterCard 或 Visa 五名成员的徽标）支付商品和/或服务的所有实体。请注意接受使用相关支付卡支付商品和/或服务的商户也可能是服务提供商，前提是销售的服务会导致代表其他商户或服务提供商存储、处理或传输持卡人数据。例如，ISP 是接受按月使用支付卡结算的商户，但是如果其客户为商户，那么它也是服务提供商。
MO/TO	“邮件订单/电话订单”的缩写。
监控	使用系统或流程不断监督计算机或网络资源以便在发生运转中断、告警或其他预定义事件时警报相关工作人员。
MPLS	“多协议标签交换”的缩写。用于连接一组数据包交换网络的网络或电信机制。
多因素验证	通过认证至少两个因素验证用户身份的方法。这些因素包括用户所有（例如智能卡或加密狗），用户所知（例如密码、口令或 PIN）或者用户特征或用户所为（例如指纹或其他类型的生物特征）。
NAC	“网络访问控制”或“网络管理控制”的缩写。依据定义的安全政策将网络资源的可用性限制在终端设备，从而在网络层实施安全性的方法。

术语	定义
NAT	“网络地址转换”的缩写。也称为网络伪装或 IP 伪装。将某个网络内使用的 IP 地址更改为另一个网络内已知的不同 IP 地址，使组织能够同时拥有内部可见的内部地址和仅外部可见的外部地址。
网络	通过物理或无线方式连在一起的两台或更多的计算机。
网络管理员	负责管理实体内网络的工作人员。职责一般包括但不限于网络安全、安装、升级、维护和活动监控。
网络组件	包括但不限于防火墙、交换机、路由器、无线接入点、网络设备和其他安全设备。
网络图	显示联网环境内系统组件和连接的图表。
网络安全扫描	通过使用手动或自动工具远程检查实体的系统是否有漏洞的流程。安全扫描包括探测内部和外部系统以及报告暴露于网络的服务。扫描可识别操作系统、服务和设备中可能被恶意个人所利用的漏洞。
网络分段	也称为“分段”或“隔离”。网络分段可将存储、处理或传输持卡人数据的系统组件与其他无法执行此类操作的系统隔离开来。充足的网络分段可缩小持卡人数据环境的范围，从而缩小 PCI DSS 评估的范围。关于使用网络分段的相关指南，请参见 *《PCI DSS 要求和安全评估程序》* 中的“网络分段”部分。网络分段并不属于 PCI DSS 要求。
网络嗅探	也称为“数据包嗅探”或“嗅探”。被动监控或收集网络通信、解码协议和检查感兴趣的信息的内容的技术。
NIST	“国家标准与技术研究所”的缩写。美国商务部技术管理内部的无管理联邦机构。
NMAP	映射网络以及识别网络资源中的开放端口的安全扫描软件。
非控制台访问	指的是对系统组件的逻辑访问，通过网络接口（而不是通过直接的物理连接）连接到系统组件上。非控制台访问包括通过本地/内部网络进行的访问，也包括通过外部或远程网络进行的访问。
非消费者用户	除持卡人以外访问系统组件的个人，包括但不限于员工、管理员和第三方。
NTP	“网络时间协议”的缩写。用于同步计算机系统、网络设备和其他系统组件的时钟的协议。
NVD	“国家漏洞数据库”的缩写。美国政府用于存放基于标准的漏洞管理数据。NVD 包括安全核对表数据库、安全相关软件攻击数据库、错误配置数据库、产品名称数据库和影响指标数据库。
OCTAVE®	“操作性关键威胁、资产和漏洞评估”的缩写。用于风险信息安全性战略评估和规划的一套工具、技术和方法。
现货供应	产品描述，即非针对特定客户或用户特别定制或设计且现成的库存商品。
操作系统/OS	负责所有活动的管理和协调以及计算机资源共享的计算机系统中的软件。操作系统包括 Microsoft Windows、Mac OS、Linux 和 Unix 等。

术语	定义
组织独立性	确保执行活动的个人或部门与评估活动的个人或部门之间没有利益冲突的组织结构。例如，执行评估的个人有组织地与正在评估环境的管理工作分离。
OWASP	“开放式网络应用程序安全项目”的缩写。专注于提高应用程序软件安全性的非盈利组织。OWASP 负责维持网络应用程序的关键漏洞列表。（请参见 http://www.owasp.org）。
PA-DSS	“支付应用程序数据安全标准”的缩写。
PA-QSA	“支付应用程序合格安全性评估商”的缩写。PA-QSA 由 PCI SSC 授予按照 PA-DSS 评估支付应用程序的资格。关于 PA-QSA 公司和员工要求的详情，请参见*《PA-DSS 计划指南》*和*《PA-QSA 资格要求》*。
索引簿	在加密法中，一次性索引簿是将文本和与纯文本长度相同的随机密钥或“索引簿”相结合的加密算法，仅可使用一次。此外，如果密钥是真正随机的、从不重用的且保密的，那么一次性索引簿就是牢不可破的
PAN	“主帐户号”的缩写，也称为“帐号”。识别发卡机构和特定持卡人帐户的唯一支付卡号（一般是信用卡和借记卡）。
参数化查询	限制转义从而防止注入攻击的结构化 SQL 查询方式。
密码/口令	作为用户的验证器的字符串。
PAT	“端口地址转换”的缩写，也称为“网络地址端口转换”。也转换为端口号的 *NAT* 类型。
补丁	更新为现有软件以添加功能或修正缺陷。
支付应用程序	就 PA-DSS 而言，支付应用程序是指销售、发布或授权给第三方用于存储、处理或者传输持卡人的授权或结算数据的软件应用程序。更多详情，请参见*《PA-DSS 计划指南》*。
支付卡	就 PCI DSS 而言，任何带有 PCI SSC 创办成员（American Express、Discover Financial Services、JCB International、MasterCard Worldwide 或 Visa, Inc）徽标的支付卡/设备。
支付处理商	有时被称为“支付网关”或“支付服务提供商（PSP）”。 商户雇佣的实体或其他代表商户处理支付卡交易的实体。虽然支付处理商一般提供收单服务，但除非由支付卡品牌定义，否则支付处理商不被视为收单机构。另请参见*收单机构*。
PCI	“支付卡行业”的缩写。
PCI DSS	“支付卡行业数据安全标准”的缩写。
PDA	“个人数据助理”或“个人数字助理”的缩写。带有手机、电子邮件或网络浏览器功能的手持式移动设备。
PED	PIN 输入设备。
穿透测试	穿透测试会尝试识别利用漏洞绕过或攻克系统组件安全功能的方式。穿透测试包括网络和应用程序测试以及围绕网络和应用程序的控制和流程，并且包括从环境外部尝试进行（外部测试）以及从环境内部进行。

术语	定义
个人防火墙软件	安装在单台计算机上的软件防火墙产品。
个人可识别信息	用于识别或跟踪个人身份（包括但不限于姓名、地址、社会保险号码、生物特征数据、出生日期等）的信息。
工作人员	“常驻”实体经营场所或以其他方式可访问持卡人数据环境的全职和兼职员工、临时工、承包商和顾问。
PIN	“个人识别码”的缩写。只有用户以及验证用户的系统知道的秘密数字密码。只有用户提供的 PIN 与系统中的 PIN 相匹配时，用户才能访问系统。一般的 PIN 用于预借现金交易的现金自动取款机。另一类 PIN 用于 EMV 芯片，可代替持卡人的签名。
PIN 数据块	处理过程中用于压缩 PIN 的数据块。PIN 数据块格式定义了 PIN 数据块的内容以及用于恢复 PIN 的处理方式。PIN 数据块包括 PIN 和 PIN 长度，还可能包含 PAN 的子集。
POI	“交互点”的缩写，从卡中读取数据的起点。电子交易认可产品，POI 由硬件和软件组成且托管在认可设备中，可让持卡人执行支付卡交易。POI 可能有人看管，也可能无人看管。POI 交易一般是集成电路（芯片）和/或磁条卡支付交易。
政策	支配可接受的计算资源使用和安全实践以及指导操作程序发展的组织级规则。
POP3	“邮局协议版本 3”的缩写。电子邮件客户用来在远程服务器中通过 TCP/IP 连接检索电子邮件的应用层协议。
端口	与特定通信协议相关的逻辑（虚拟）连接点，便于整个网络的通信。
POS	“销售点”的缩写。商户所在地点用于处理支付卡交易的硬件和/或软件。
专用网络	使用私人 IP 地址空间的组织所建立的网络。专用网络通常设计为局域网。从公共网络进行的专用网络访问应使用防火墙和路由器进行适当的保护。另请参见*公共网络*。
特权用户	拥有的权限超出基本访问权限的所有用户帐户。一般而言，这些帐户享有较高和较多的特权，比标准用户帐户拥有更多权利。但是不同特权帐户的特权范围差异很大，具体取决于组织、工作职能或角色以及使用的技术。
程序	政策的描述性叙述。程序是政策的“执行方式”，描述了政策的实施方式。
协议	网络内部使用的协定通信方法。描述计算机产品在网络上执行活动时应遵循的规则和程序的规范。
代理服务器	作为内部网络和互联网之间的中介的服务器。例如代理服务器的一项功能是终止或商谈内部和外部连接之间的连接，以便这两个连接分别仅与代理服务器通信。
PTS	“PIN 交易安全”的缩写，PTS 受 PCI 安全标准委员会管理，是 PIN 认可 POI 终端的模块化评估要求集合。请参见 www.pcisecuritystandards.org。

术语	定义
公共网络	第三方电信提供商建立或运营的网络，专用于为公众提供数据传输服务。公共网络上的数据可能在传输时被拦截、修改和/或转移。公共网络包括但不限于互联网、无线和移动技术等。另请参见 *专用网络*。
PVV	“PIN 验证值”的缩写。编译在支付卡磁条中的任意值。
QIR	“合格的集成商或经销商”的缩写。更多信息，请参见 PCI SSC 网站上的 *《QIR 计划指南》*。
QSA	“合格的安全评估商”的缩写。QSA 经由 PCI SSC 授予执行 PCI DSS 现场评估的资格。关于 QSA 公司和员工要求的详情，请参见 *《QSA 资格要求》*。
RADIUS	“远程验证拨号用户服务”的缩写。验证和计帐系统。检查用户名和密码等传递到 RADIUS 服务器的信息是否正确，然后授予访问系统的权限。此验证方法可与令牌、智能卡等结合使用，提供多因素验证。
彩虹表攻击	使用散列字符串的预计算表格（固定长度的消息摘要）识别原始数据源的数据攻击方法，通常用于破解密码或持卡人数据散列。
密钥更换	更换密钥的流程。定期的密钥更换限制了单密钥加密的数据数量。
远程访问	从网络外部位置访问电脑网络。远程访问连接可自公司自己网络的内部发起，也可自公司网络外部的远程位置发起。*VPN* 就是一种远程访问技术。
远程实验室环境	并非 PA-QSA 维护的实验室。
可移动电子媒介	存储数字化数据的媒介，可轻松从一个计算机系统移动和/或传输到另一个。可移动电子媒介包括 CD-ROM、DVD-ROM、USB 闪存驱动器和外部/便携式硬盘等。
经销商/集成商	销售和/或集成（但不研发）支付应用程序的实体。
RFC 1918	互联网工程任务组 (IETF) 确定的标准，定义了专用（非互联网可路由的）网络的使用情况和适当的地址范围。
风险分析/风险评估	识别有价值的系统资源和威胁的流程；根据估算的频率和产生的成本量化损失暴露风险（即可能导致的损失）；以及（可选）建议如何分配用于应对的资源以最大限度地降低总暴露风险。
风险等级	测量的定义标准，基于针对指定实体所执行的风险评估和风险分析。
ROC	“遵从性报告”的缩写。报告某实体的 PCI DSS 评估中详细记录的结果。
Rootkit 内核型病毒	恶意软件类型，未经授权安装后能够隐藏自身的存在，管理控制计算机系统。
路由器	连接两个或更多网络的硬件或软件。着眼于地址，并将零散信息传递到正确的目的地，从而发挥分类器和解释器的作用。软件路由器有时称为网关。
ROV	“认证报告”的缩写。报告用于 PA-DSS 计划的 PA-DSS 评估中详细记录的结果。

术语	定义
RSA	1977 年麻省理工学院 (MIT) 的 Ron Rivest、Adi Shamir 和 Len Adleman 所描述的公钥加密算法；字母 RSA 是他们姓氏的首字母。
S-FTP	安全 FTP 的缩写。S-FTP 能够加密传输中的验证信息和数据文件。请参见 *FTP*。
抽样	选择某个组中代表整个组的典型的流程。评估商可使用抽样减少整体测试工作，实体要拥有标准的中央 PCI DSS 安全和操作流程和控制才能进行验证。抽样不属于 PCI DSS 要求。
SANS	“美国系统网络安全协会”的缩写，提供计算机安全培训和专业认证的协会 （请参见 www.sans.org）。
SAQ	“自我评估调查问卷”的缩写。用于记录某实体的 PCI DSS 评估中自我评估结果的报告工具。
架构	数据库（包括整理数据元素）构造方法的正式描述。
范围界定	要包含在 PCI DSS 评估中的所有系统组件、人员和流程的识别流程。PCI DSS 评估的第一步是准确确定审核范围。
SDLC	“系统开发生命周期”或“软件开发生命周期”的缩写。软件或计算机系统的开发阶段，包括规划、分析、设计、测试和实施。
安全编码	创建和实施应用程序以防止被篡改和/或遭受威胁的流程。
安全加密设备	实施加密流程（包括加密算法和密钥生成）的硬件、软件和固件集合，属于定义的加密界限内。安全加密设备包括已通过 PCI PTS 认证的主机/硬件安全模块 (HSM) 和交互点设备 (POI) 等。
安全擦除	也称为“安全删除”，覆盖硬盘或其他数字媒体上的数据使数据不可检索的方法。
安全事件	组织认为对于系统或其环境而言存在潜在安全隐患的事件。就 PCI DSS 而言，安全事件会识别可疑或异常活动。
安全人员	负责实体的安全相关问题的主要人员。
安全政策	法律、规则和实践的集合，可监管组织如何管理、保护和分配敏感信息。
安全协议	用于保护数据传输安全的网络通信协议。安全协议包括但不限于 TLS、IPSEC、SSH、HTTPS 等。
敏感区域	任何数据中心、服务器室或任何存储、处理或传输持卡人数据的系统所在区域。这不包括仅有销售点终端的区域，例如零售店的收银区。
敏感验证数据	用于验证持卡人身份和/或授权支付卡交易的安全相关信息（包括但不限于卡认证代码/值、全磁道数据（磁条数据或芯片上的等效数据）、PIN 和 PIN 数据块）。
职责分离	为不同的个人划分职能，以确保单独的个人无法破坏流程的方法。
服务器	向其他计算机提供服务（如处理通信、文件存储或访问打印设备）的计算机。服务器包括但不限于网络、数据库、应用程序、验证、DNS、邮件、代理器和 NTP。

术语	定义
业务码	磁条中的三位或四位值，位于磁道数据上的支付卡失效日之后。业务码用途多样，可用于定义服务属性、区分国际和国内交换或识别使用限制等。
服务提供商	并非支付品牌的企业实体，代表其他实体直接参与持卡人数据的处理、存储或传输。服务提供商也提供控制或可能影响持卡人数据安全的服务。示例包括提供托管防火墙、IDS 和其他服务的托管服务提供商，以及托管提供商和其他实体。如果某实体提供*仅*涉及公共网络访问提供的服务（例如仅提供通信链接的电信公司），则不认为该实体是相关服务的服务提供商（不过可认为该实体是其他服务的服务提供商）。
会话令牌	在网络会话管理背景下，会话令牌（也被称为“会话标识符”或“会话ID”），是用于跟踪网络浏览器与网站服务器之间个别会话的唯一标识符（例如“网络跟踪器”(cookie)）。
SHA-1/SHA-2	“安全散列算法”的缩写。相关加密散列函数（包括 SHA-1 和 SHA-2）系列或集合。请参见*强效加密法*。
智能卡	也称为“芯片卡”或“IC 卡（集成电路卡）”。内嵌集成电路的支付卡类型。电路也称为“芯片”，包含的支付卡数据包括但不限于磁条数据的等效数据。
SNMP	“简单网络管理协议”的缩写。支持对联网设备进行监控，保证管理人员注意到任何情况。
分割知识	两个或更多的实体分别掌握部分密钥且根据密钥的单个部分无法得知整个密钥的方法。
间谍软件	恶意软件类型，安装后会在用户不知情的情况下拦截或部分控制用户计算机。
SQL	“结构化查询语言”的缩写。用于创建、修改和检索关系数据库管理系统中的数据的计算机语言。
SQL 注入	攻击数据库驱动网站的形式。恶意个人在连接到互联网的系统上利用非安全代码执行非授权的 SQL 命令。SQL 注入攻击用于从数据正常情况下不可用的数据库中盗取信息和/或通过托管数据库的计算机获取组织主机的访问权限。
SSH	“安全外壳”的缩写。为远程登录或远程文件传输等网络服务提供加密的协议套件。
SSL	“安全套接层”的缩写。加密网络浏览器和网络服务器间通道的行业标准。现在已被 TLS 取代。请参见 *TLS*。
状态检查	也称为“动态数据包过滤”。通过跟踪网络连接的状态提高安全性的防火墙功能。旨在区分各类连接的合法数据包，防火墙只允许与已建立的连接相匹配的数据包；所有其他数据包将遭到拒绝。

术语	定义
强效加密法	以经过行业测试和认可的算法为基础的加密法，以及提供至少 112 位的有效密钥长度及合适的密钥管理方法的密钥长度。加密法是一种保护数据的方法，包括加密（可逆的）和散列（单向的，即不可逆的）。另请参见*散列*。 本文发表时，经过行业测试和认可的标准和算法包括 AES（128 位和更高）、TDES/TDEA（最少三倍长的密钥）、RSA（2048 位和更高）、ECC（224 位和更高）以及 DSA/D-H（2048/224 位和更高）。关于密钥强度和算法的更多指南，请参见《NIST 特别出版物 800-57》第 1 部分的最新版本（http://csrc.nist.gov/publications/）。 ***注：****以上示例适用于持卡人数据的永久储存。如 PCI PIN 和 PTS 中所定义，交易操作的最低加密要求更加灵活，因为设有附加控制以减少暴露风险。* *我们建议所有新实施的内容使用至少 128 位的有效密码长度。*
SysAdmin	“系统管理员”的缩写。享有较高特权的个人，负责管理计算机系统或网络。
系统组件	包含在或连接到持卡人数据环境的任何网络设备、服务器、计算设备或应用程序。
系统级对象	系统组件上所需的任何对象，包括但不限于数据库表、存储的程序、应用程序执行表和配置文件、系统配置文件、静态和共享库与 DLL、系统执行表、设备驱动程序和设备配置文件以及第三方组件。
TACACS	“终端访问控制器访问控制系统”的缩写。常用于网络中的远程验证协议，在远程访问服务器和验证服务器间通信以决定用户对网络的访问权限。此验证方法可与令牌、智能卡等结合使用，提供多因素验证。
TCP	“传输控制协议”的缩写。互联网协议（IP）套件的核心传输层协议之一，也是互联网的基本通信语言或协议。请参见 *IP*。
TDES	“三重数据加密标准”的缩写，也称为“3DES”或“三重 DES”。使用三次 DES 密码形成的数据块密码。请参见*强效加密法*。
TELNET	“电话网络协议”的缩写。一般用于向网络中的设备提供面向用户的命令行登录会话。用户凭证以明文形式传输。
威胁	可能有意或无意导致信息或信息处理资源丢失、变动、暴露、不可访问或以其他方式损害组织的条件或活动
TLS	“传输层安全”的缩写。用于确保两个通信应用程序间的数据安全性和数据完整性。TLS 是 SSL 的继承者。
令牌	就验证和访问控制而言，令牌是由硬件或软件提供的值，可与验证服务器或 VPN 一起执行动态或多因素验证。请参见 *RADIUS*、*TACACS* 和 *VPN*。另请参见*会话令牌*。
磁道数据	也称为“全磁道数据”或“磁条数据”。编译在磁条或芯片中的数据，用于支付交易中的验证和/或授权。可以是芯片上的磁条图片，也可以是磁条的磁道 1 和/或磁道 2 部分上的数据。
交易数据	与电子支付卡交易相关的数据。

术语	定义
特洛伊	也称为“特洛伊木马”。恶意软件类型，安装后允许用户执行正常功能，但是特洛伊在用户不知情的情况下会对计算机系统执行恶意功能。
截词	通过永久移除 PAN 数据的某分段，使完整 PAN 不可读的方法。截词*存储*在文件、数据库中时，与 PAN 的保护相关。关于 PAN *显示在屏幕、纸质收据上时的保护，请参见*掩盖。
可信网络	组织能够控制或管理的组织网络。
不可信网络	组织所拥有的网络外部的网络，组织不能掌握或管理的网络。
网址	“统一资源定位符”的缩写。网络浏览器、电子邮件客户和其他软件用来识别互联网上的网络资源的格式化文本字符串。
版本控制方法	分配版本方案以识别应用程序或软件唯一特定状态的流程。这些方案遵循软件供应商定义的版本号格式、版本号使用情况和任何通配符元素。版本号通常以递增顺序分配，且与软件的特定变更相对应。
虚拟设备 (VA)	VA 将预配置的设备设想为执行特定功能集合，并将相应设备作为负载运行。通常，现有的网络设备会经过虚拟化作为虚拟设备运行，例如路由器、交换机或防火墙。
虚拟监控程序	请参见*监控程序*。
虚拟机	像独立的计算机一样自给自足的操作环境。也称为“客户”，在监控程序之上运行。
虚拟机监控 (VMM)	VMM 包含在监控程序中，是实施虚拟机硬件抽象的软件。VMM 管理着系统的处理器、存储器和其他资源以分配各个客户操作系统所需的资源。
虚拟支付终端	虚拟支付终端会通过网络浏览器访问收单机构、处理机构或第三方服务提供商网站以授权支付卡交易，其中商户通过安全连接的网络浏览器手动输入支付卡数据。与物理终端不同，虚拟支付终端不会直接从支付卡中读取数据。由于支付卡交易信息是手动输入的，因此虚拟支付终端一般用于替代商户环境中交易量较小的物理终端。
虚拟交换机或路由器	虚拟交换机或路由器是描述网络基础架构级数据路由和交换功能的逻辑实体。虚拟交换机是虚拟服务器平台（监控程序驱动程序、模块或插件）的组成部分。
虚拟化	虚拟化是将计算资源从物理约束中进行逻辑抽象。常见的一种抽象为虚拟机或 VM，VM 会获取物理机的内容，允许这些内容在不同的物理硬件上和/或与相同物理硬件上的其他虚拟机一起进行操作。除 VM 外，虚拟化还可针对许多其他计算资源执行，包括应用程序、桌面、网络和存储。
VLAN	“虚拟 LAN”或“虚拟局域网”的缩写。延伸到单一的传统物理局域网之外的逻辑局域网。

术语	定义
VPN	“虚拟专用网络”的缩写。计算机网络中的某些连接是某些较大网络（如互联网）内的虚拟电路，而不是通过物理线缆直接连接。在这种情况下，虚拟网络的端点被认为是经过较大网络连通的。虽然常见应用程序由通过公共互联网的安全通信构成，但是 VPN 是否拥有强大的安全功能（如验证或内容加密）并不确定。 VPN 可与令牌、智能卡等结合使用，提供双因素验证。
漏洞	一旦被利用可能有意或无意对系统构成威胁的缺陷或弱点。
WAN	“广域网”的缩写。覆盖大片（通常为整个区域或整个公司）计算机系统的计算机网络。
网络应用程序	通常通过网络浏览器或通过网络服务访问的应用程序。网络应用程序可通过互联网或专用内部网络提供。
网络服务器	接受网络客户端的 HTTP 请求并提供 HTTP 响应的计划（通常是网页）中所包含的计算机。
WEP	“有线等效加密”的缩写。用于加密无线网络的弱算法。行业专家已发现该算法的众多严重弱点，因此 WEP 连接可在数分钟内使用现成的软件破解。请参见 *WPA*。
通配符	应用程序版本方案中可能的字符构成的定义子集可替换的字符。就 PA-DSS 而言，可选择用通配符表示不影响安全的变更。通配符是供应商版本方案的唯一可变元素，用来说明用通配符元素表示的每个版本之间只有不影响安全的次要变更。
无线访问点	也称为“AP”。允许无线通信设备连接到无线网络的设备。AP 通常连接到有线网络，可在网络中的无线设备和有线设备间中继数据。
无线网络	不使用物理连接将计算机连成线的网络。
WLAN	“无线局域网”的缩写。不使用线缆链接两个或更多计算机的局域网。
WPA/WPA2	“WiFi 访问保护技术”的缩写。用于保护无线网络安全的安全协议。WPA 是 WEP 的继承者。WPA2 也称为下一代 WPA。