



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

---

**术语、缩略语**

**1.2 版**

2008 年 10 月

术语	定义
AAA	“验证、授权和记帐”的缩略语。根据可验证的身份验证用户、根据用户权限授权用户以及为用户的网络资源消费记帐的协议。
AES	“高级加密标准”的缩略语。NIST 于 2001 年 11 月采用的称为 U.S. FIPS PUB 197（或“FIPS 197”）的对称密钥加密法中使用的块密码。请参阅“ <i>强效加密法</i> ”。
ANSI	“美国国家标准协会”的缩略语。管理和协调美国自愿标准化和合格评估体系的私有非赢利性组织。
ASV	“授权扫描供应商”的缩略语。PCI SSC 批准的提供外部漏洞扫描服务的公司。
CIS	“互联网安全中心”的缩略语。非赢利性企业，旨在帮助公司减少技术性安全控制不足导致的业务风险和电子商务中断。
DMZ	“隔离区”的缩略语。为公司的内部专用网络提供额外安全层的物理或逻辑子网络或计算机主机。DMZ 在互联网和公司的内部网络间添加了另外一个网络安全层，这样从外部只能直接访问 DMZ 中的设备，而不能访问所有的内部网络。
DNS	“域名系统”或“域名服务器”的缩略语。将和域名有关的信息存储在网络（如互联网）分布式数据库中的系统。
DSS	“数据安全标准”的缩略语，也称为“PCI DSS”。
ECC	“椭圆曲线加密法”的缩略语。基于有限域上的椭圆曲线的公共密钥加密法。请参阅“ <i>强效加密法</i> ”。
FIPS	“联邦信息处理标准”的缩略语。美国联邦政府公开认可的标准，也供非政府机构和承包商使用。
FTP	“文件传输协议”的缩略语。通过公共网络（如互联网）在计算机间传输数据的网络协议。FTP 被广泛认为是不安全的协议，因为密码和文件内容在发送期间未受保护，并且以纯文本的形式发送。FTP 可以通过 SSH 或其他技术安全实施。
GPRS	“通用无线分组业务”的缩略语。GSM 手机用户可以使用的移动数据业务。因为能高效地使用有限的带宽而被认可。特别适合用于发送和接收小型数据流，如电子邮件和网页浏览。
GSM	“全球移动通信系统”的缩略语。它是手机和网络的常用标准。GSM 标准的普及使手机用户之间的国际漫游非常普遍，订户能在全世界的许多地方使用手机。
HTTP	“超文本传输协议”的缩略语。在万维网中传输信息的开放式互联网协议。
HTTPS	“安全套接层超文本传输协议”的缩略语。提供万维网验证和加密通信、用于安全敏感通信的安全 HTTP，如基于 Web 的登录。
ID	用于特定用户或应用程序的标识符。
IDS	“入侵检测系统”的缩略语。用来识别和提醒有人试图入侵网络或系统的软件或硬件。组成部分包括：生成安全事件的传感器，监控事件和警报并控制传感器的控制台，以及将传感器记录的事件记录至数据库的中心引擎。使用规则系统生成警报，对检测到的安全事件做出反应。

术语	定义
IETF	“互联网工程任务组”的缩略语。网络设计师、运营商、供应商和研究者的大型开放式国际机构，主要关注互联网体系结构发展和互联网的顺畅运作。IETF 没有正式成员，并且对任何感兴趣的人开放。
IP	“互联网协议”的缩略语。包含使包能找到路径的地址信息和某些控制信息的网络层协议。IP 是互联网协议套件中的主要网络层协议。
IP 地址	也称为“互联网协议地址”。唯一识别互联网中特定计算机的数字代码。
IP 地址假冒	恶意个人为了对计算机进行未经授权访问而使用的攻击技术。通过使用表明消息来自受信任主机的 IP 地址，恶意个人可向计算机发送欺骗消息。
IPS	“入侵防御系统”的缩略语。若超出 IDS，IPS 将采取其他措施阻止入侵企图。
IPSEC	“互联网协议安全”的缩略语。通过加密和/或验证所有 IP 包保护 IP 通信的标准。IPSEC 在网络层提供安全性。
ISO	通常称为“国际标准化组织”。由 150 多个国家/地区的国家标准机构网络组成的非政府组织，每个国家/地区有一名成员，中央秘书处设在瑞士日内瓦，由它协调整个系统。
LAN	“局域网”的缩略语。覆盖通常为一个建筑物或一组建筑物的小范围面积的计算机网络。
LDAP	“轻量级目录访问协议”的缩略语。用于查询和修改用户权限和授权访问受保护资源的验证和授权数据的存储库。
LPAR	“逻辑分区”的缩略语。将计算机总资源（即处理器、内存和存储）细分成更小单元的系统，这些单元能使用自身的、操作系统和应用程序的不同副本独立运行。逻辑分区通常用来允许在一个设备上使用不同的操作系统和应用程序。分区可以设置成是否允许互相通信或共享服务器的某些资源（如网络界面）。
MAC	“消息验证代码”的缩略语。在加密法中，它是用来验证消息的一小条信息。请参阅“ <a href="#">强效加密法</a> ”。
MAC 地址	“媒体访问控制地址”的缩略语。制造商分配给网络适配器和网络界面卡的唯一识别值。
MPLS	“多协议标签交换”的缩略语。旨在连接包转换网络组的网络或电信机制。
NAT	“网络地址转译”的缩略语。也称为网络伪装或 IP 伪装。将某个网络中使用的 IP 地址转换成其他网络中已知的不同 IP 地址。
NIST	“国家标准和技术研究所”的缩略语。美国商务部技术管理局的非限制性联邦机构。其任务是通过发展度量科学、标准和技术来改善经济安全和提高生活质量，以促进美国的创新和行业竞争。
NMAP	映射网络并识别网络资源中的开放端口的安全扫描软件。
NTP	“网络时间协议”的缩略语。在包切换、等待时间可变的数据网络上同步计算机系统时钟的协议。
OWASP	“开放式网络应用程序安全项目”的缩略语。2004 年成立的致力于提高应用程序软件安全性的非赢利性组织。OWASP 发布了 OWASP 前十位的漏洞，列出了最重要的网络应用程序漏洞。（请参阅 <a href="http://www.owasp.org">http://www.owasp.org</a> ）。

术语	定义
PAN	“主要账户号码”的缩略语，也称为“账号”。它是识别发卡机构和特定持卡人账户的唯一支付卡号码（通常用于信用卡或借记卡）。
PA-QSA	“支付应用程序合格安全性评估商”的缩略语，指 PCI SSC 批准的、根据 PA-DSS 评估支付应用程序的公司。
PAT	“端口地址转译”的缩略语，也称为“网络地址端口转译”。它是也转译端口号的 NAT 类型。
PCI	支付卡行业。
PDA	“个人数据助理”或“个人数字助理”的缩略语。具有手机、电子邮件或网络浏览器功能的手持式移动设备。
PIN	“个人识别码”的缩略语。只有用户和验证用户的系统知道的机密数字密码。只有用户提供的 PIN 和系统中的 PIN 相符才允许用户访问。通常，PIN 用于针对现金垫款交易的自动提款机。另外一种 PIN 类型是 PIN 代替持卡人签名的 EMV 芯片卡使用的 PIN。
POS	“销售点”的缩略语。用来处理商户所在地的支付卡交易的硬件和/或软件。
PVV	“PIN 验证值”的缩略语。编码在支付卡磁条中的任意值。
QSA	“合格安全性评估商”的缩略语，是指 PCI SSC 批准的从事 PCI SSC 现场评估的公司。
RADIUS	“远程拨入用户验证服务”的缩略语。验证和记帐系统。先检查通过 RADIUS 服务器的用户名和密码等信息是否正确，然后再授权访问系统。
RBAC	“基于角色的访问控制”的缩略语。特定授权用户基于工作职责用来限制访问的控制方式。
RSA	Ron Rivest、Adi Shamir 和 Len Adleman 于 1977 年在曼彻斯特技术研究所 (MIT) 阐述的公共密钥加密算法，RSA 是他们的姓氏的首字母。
SANS	“系统管理和网络安全审计委员会”的缩略语，是提供计算机安全培训和专业认证的机构。（请参阅 <a href="http://www.sans.org">www.sans.org</a> ）。
SAQ	“自行评估调查问卷”的缩略语。机构用来验证其 PCI DSS 合规性的工具。
SDLC	“系统开发生命周期”的缩略语。软件或计算机系统开发的各个阶段，包括规划、分析、设计、测试和实施。
SHA-1/SHA-2	“安全散列算法”的缩略语。与加密法散列相关的一系列或一组函数，包括 SHA-1 和 SHA-2。请参阅“ <a href="#">强效加密法</a> ”。
SNMP	“简单网络管理协议”的缩略语。针对要求管理员注意的任何情况，支持对网络附加设备进行监控。
SQL	“结构化查询语言”的缩略语。用来从关系数据库管理系统中创建、修改和检索数据的计算机语言。
SQL 注入	攻击数据库驱动型网站的一种形式。恶意个人通过利用连接到互联网的系统中的不安全代码执行未授权的 SQL 命令。SQL 注入攻击用来从数据通常不可用的数据库窃取信息和通过托管数据库的计算机获得对公司主机的访问权限。

术语	定义
SSH	“安全接壳”的缩略语。为网络服务（如远程登录或远程文件传输）提供加密的协议套件。
SSL	“安全套接层”的缩略语。为网络浏览器和网络服务器间的通道进行加密而制定的行业标准，目的是确保数据在该通道中传输的隐秘性和可靠性。
SysAdmin	“系统管理员”的缩略语。负责管理计算机系统或网络的具有高级权限的个人。
TACACS	“终端访问控制器访问控制系统”的缩略语。通常用于远程访问服务器和验证服务器间决定用户访问网络权限的通信网络的远程验证协议。
TCP	“传输控制协议”的缩略语。互联网基础通信语言或协议。
TDES	“三重数据加密标准”的缩略语，也称为“3DES”或“三重 DES”。通过使用三次 DES 密码而形成的块密码。请参阅“ <a href="#">强效加密法</a> ”。
TELNET	“电话网络协议”的缩略语。通常用来给网络设备提供面向用户的命令行登录会话。用户证书以纯文本格式进行传输。
TLS	“传输层安全”的缩略语。目的是确保两个正在通信的应用程序间的数据安全性和完整性。TLS 是 SSL 的后续。
VLAN	“虚拟 LAN”或“虚拟局域网”的缩略语。超过单个传统物理局域网的逻辑局域网。
VPN	“虚拟专用网”的缩略语。这种计算机网络内的某些连接是更大网络（如互联网）内的虚拟线路，而不是使用物理电线直接连接。虚拟网的终点据说是通过隧道扩展的更大的现实网络。普通应用程序通过公共互联网实现安全通信，但 VPN 可能有或没有强大的安全功能（如验证或内容加密）。
WAN	“广域网”的缩略语。覆盖较大区域（通常是地区或公司范围）的计算机系统的计算机网络。
Web 服务器	包含从 Web 客户端接受 HTTP 请求并提供 HTTP 响应（通常是网页）的程序的计算机。
WEP	“有线等效加密”的缩略语。用来加密无线网络的薄弱算法。行业专家已确认多个严重漏洞，以便在数分钟内用容易获得的软件断开 WEP 连接。请参阅“ <a href="#">WPA</a> ”。
WLAN	“无线局域网”的缩略语。不用电线连接两台或多台计算机或设备的局域网。
WPA/WPA2	“WiFi 访问保护”的缩略语。为保护无线网络安全而制定的安全协议。WPA 是 WEP 的后续，被认为能比 WEP 提供更好的安全性。WPA2 也是作为 WPA 的下一代协议而发布。
安全擦除	也称为“安全删除”，是用来从计算机系统永久删除特定文件的实用程序。
安全政策	规范公司管理、保护和分配敏感信息的一套法律、规则和惯例。
安全执行官	公司安全相关性事务的主要负责人。
备份	为了归档目的或防止损坏或丢失而复制数据副本。

术语	定义
补偿性控制	<p>当机构由于合法的技术限制或记录的业务限制，无法满足明确指定的要求，但已通过实施其他控制充分减轻了与此要求相关的风险时，可考虑补偿性控制。补偿性控制必须：</p> <ol style="list-style-type: none"><li>(1) 符合最初 PCI DSS 要求的主旨和严格程度；</li><li>(2) 提供和最初 PCI DSS 要求类似级别的防御机制；</li><li>(3) “超越”其他 PCI DSS 要求（不仅仅是符合其他 PCI DSS 要求）；以及</li><li>(4) 与不遵循 PCI DSS 要求而引发的其他风险相对应。</li></ol> <p>请参阅《PCI DSS 要求和安全评估程序》中的补偿性控制附录 B 和 C，获得使用补偿性控制的指导说明。</p>
补丁	<p>对现有软件的更新，以增加功能或纠正缺陷。</p>
不安全协议/服务/端口	<p>由于缺少对机密性和/或完整性的控制而引入安全问题的协议、服务或端口。这些安全问题包括传输数据和验证凭据（例如，互联网上的纯文本密码/密码短语）或在默认或配置不当的情况下容易允许利用数据的服务、协议或端口。不安全协议、服务或端口的一个例子就是 FTP。</p>
不受信任的网络	<p>公司网络之外的超出公司控制或管理能力的网络。</p>
操作系统/OS	<p>负责管理和协调所有活动和计算机资源共享的计算机系统软件。操作系统的实例包括 Microsoft Windows、Mac OS、Linux 和 Unix。</p>
程序	<p>对某项政策的解释性描述。程序是针对政策的“执行方式”，并描述了政策将如何实施。</p>
持卡人	<p>向其发放支付卡的非消费者或消费者客户，或者任何授权使用支付卡的个人。</p>
持卡人数据	<p>持卡人数据至少包含完整的 PAN。持卡人数据也可以指完整的 PAN 加上以下任何一种信息：</p> <ul style="list-style-type: none"><li>▪ 持卡人姓名</li><li>▪ 失效期</li><li>▪ 业务代码</li></ul> <p>请参阅“敏感验证数据”，了解可作为支付交易一部分来传输或处理的更多数据元素。</p>
持卡人数据环境	<p>存有持卡人数据或敏感验证数据的计算机系统网络区域和直接附加或支持持卡人处理、存储或传输的系统和分段。充足的网络分段可以将存储、处理或传输持卡人数据的系统与那些不进行这些操作的系统隔离开来，从而缩小持卡人数据环境范围及 PCI DSS 评估范围。持卡人数据环境由系统组件构成。请参阅“系统组件”。</p>
穿透测试	<p>穿透测试尝试利用漏洞来确定未授权访问或其他恶意活动是否有存在的可能。穿透测试包括网络和应用程序的测试以及围绕网络和应用程序的控制和流程，从网络外部尝试进入（外部测试）以及从网络内部都可以进行穿透测试。</p>
磁盘加密	<p>为设备（如硬盘、闪存驱动器）中存储的所有数据加密的技术（软件或硬件）。另外，文件级加密或列级数据库加密也可用于为特定文件或特定列的内容进行加密。</p>

术语	定义
磁条数据	也称为“磁道数据”。编码在磁条或芯片上用来在支付交易中进行授权的数据。可以是芯片中的磁条图形或磁条的磁道 1 和/或磁道 2 中的数据。机构在获得交易授权后绝不能保留全磁条数据。
动态包过滤	请参阅“状态检测”。
恶意软件/流氓软件	旨在不经所有者察觉或同意而渗透或破坏计算机系统的软件。这类软件通常会在许多业务批准活动中进入网络，导致系统漏洞被利用。包括病毒、蠕虫、木马（或特洛伊木马）、间谍软件、广告软件和黑客软件。
发卡机构	也称为“发卡银行”或“发卡金融机构”。向消费者和非消费者直接发放支付卡的机构。
防火墙	保护网络资源免受未经授权访问的硬件和/或软件技术。防火墙根据一套规则和其他标准允许或拒绝不同安全级别的网络间的计算机流量。
访问控制	限制信息可用性 or 信息处理资源只提供给授权人员或应用程序的机制。
非消费者用户	不包括访问系统组件的持卡人，包括但不限于员工、管理员和第三方。
分开保管	两个或多个实体分开拥有密码组件的情形，以便个人不能单独转移能产生结果的加密密钥。
风险分析/评估	该流程识别有价值的系统资源和威胁，根据评估频率和事件成本确定泄露（即潜在丢失）量，并（可选）建议如何给应对措施分配资源以减少总泄露量。
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 Web、数据库、应用程序、验证、DNS、邮件、代理和 NTP。
服务提供商	不属于支付品牌、直接参与处理、存储或传输持卡人数据的商业机构，也包括提供的服务能控制或可能影响持卡人数据安全的公司。示例包括提供受控防火墙、IDS 和其他服务的受控服务提供商以及主机提供商和其他机构。只提供不能访问通信链接应用程序层的通信链接的电信公司等机构不包括在内。
公共网络	电信提供商建立和运营的网络，专门用于为公众提供数据传输服务。数据在公共网络传输时可以被拦截、修改和/或转移。PCI DSS 范围内的公共网络示例包括但不限于互联网、无线和移动技术。
广告软件	安装后迫使计算机自动显示或下载广告的恶意软件类型。
合规性报告	也称为“ROC”。记录机构针对 PCI DSS 的合规状态的详细情况报告。
黑客软件	未经授权安装后能隐藏自身的存在并获得计算机系统管理控制的恶意软件类型。
加密算法	用于将未加密的文本或数据转换成加密文本或数据然后进行逆向操作的一系列数学指令。
间谍软件	安装后可不经用户同意拦截或部分控制用户计算机的恶意软件。
监控	使用系统或流程持续监视计算机或网络资源，以便在发生断电、警告或其他预定义事件时提醒相关人员。
交易数据	和电子支付卡交易有关的数据。
截词	通过永久删除 PAN 数据段使全部 PAN 不可读的方法。

术语	定义
卡验证值或代码	<p>是指以下任意一项：(1) 磁条数据，或 (2) 打印的安全特征。</p> <p>(1) 卡磁条中使用安全加密流程来保护磁条数据完整性、显示任何更改或伪造的数据元素。根据支付卡品牌称为 CAV、CVC、CVV 或 CSC。以下清单列出了每种卡品牌的称法：</p> <ul style="list-style-type: none"><li>▪ <b>CAV</b> – 卡验证值 (JCB 支付卡)</li><li>▪ <b>CVC</b> – 卡验证代码 (MasterCard 支付卡)</li><li>▪ <b>CVV</b> – 卡验证值 (Visa 和 Discover 支付卡)</li><li>▪ <b>CSC</b> – 卡安全代码 (American Express)</li></ul> <p>(2) 对于 Discover、JCB、MasterCard 和 Visa 支付卡来说，第二种类型的卡验证值或代码是打印在卡背面签名方格内的最右边的三位值。对于 American Express 支付卡来说，该代码是打印在支付卡正面 PAN 上方的四位阴文数字。该代码是与每张个人塑料卡相关联并将 PAN 附在塑料卡上的唯一代码。下面列出概况：</p> <ul style="list-style-type: none"><li>▪ <b>CID</b> – 卡识别码 (American Express 和 Discover 支付卡)</li><li>▪ <b>CAV2</b> – 卡验证值 2 (JCB 支付卡)</li><li>▪ <b>CVC2</b> – 卡验证代码 2 (MasterCard 支付卡)</li><li>▪ <b>CVV2</b> – 卡验证值 2 (Visa 支付卡)</li></ul>
可移动电子媒介	<p>存储数字化数据的媒介，可以很容易地移动和/或从一个计算机系统传输到另一个计算机系统。可移动电子媒介的示例包括 CD-ROM、DVD-ROM、USB 闪存驱动器和可移动硬盘驱动器。</p>
控制台	<p>允许访问和控制网络环境中的服务器或主机的屏幕和键盘。</p>
蓝牙	<p>使用短程通信技术简化数据在两个设备间短距离传输的无线协议。</p>
列级数据库加密	<p>对某个数据库特定列中的内容而不是整个数据库的所有内容进行加密的技术（软件或硬件）。另请参阅“<i>磁盘加密或文件级加密</i>”。</p>
令牌	<p>执行动态或双因素验证的硬件或软件。</p>
漏洞	<p>恶意个人可用来利用系统和破坏其完整性的系统中的弱点。</p>
路由器	<p>连接两个或多个网络的硬件或软件。查找地址并将信息传递到正确目的地的类似分类器和解释器的功能。软件路由器有时也称为网关。</p>
密码/密码短语	<p>用作用户验证码的字符串。</p>
密钥	<p>在加密法中，密钥是将纯文本转换成加密文本时决定加密算法结果的值。密钥的长度通常决定了将文本解密成指定消息的难度。请参阅“<i>强效加密法</i>”。</p>
敏感区域	<p>任何数据中心、服务器室或任何放置可存储、处理或传输持卡人数据的系统的区域。它不包括仅存在销售点终端的区域（例如零售店的收银区域）。</p>
敏感验证数据	<p>以纯文本或其他未受保护形式显示的用来验证持卡人的安全相关性信息（卡验证值/代码、全磁条数据、PIN 和 PIN 数据块）。</p>

术语	定义
强效加密法	<p>该加密法基于经行业测试并认可的算法，并且使用强效密钥长度和适当的密钥管理方法。加密法是保护数据的方法，包括加密（可逆）和散列（不可逆或“单向”）。SHA-1 就是一个经行业测试并认可的散列算法的例子。经行业测试并认可的加密标准和算法包括 AES（128 位和更多位）、TDES（最小双倍长度密钥）、RSA（1024 位和更多位）、ECC（160 位和更多位）和 ElGamal（1024 位和更多位）。</p> <p>请参阅 NIST 专刊 800-57 (<a href="http://csrc.nist.gov/publications/">http://csrc.nist.gov/publications/</a>) 了解更多信息。</p>
取证	<p>也称为“计算机取证”。它关系到信息安全，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威胁的原因。</p>
散列	<p>通过强效加密法使数据转换成固定长度的消息摘要、从而使持卡人数据不可读的流程。</p>
杀毒	<p>可以检测、删除和抵御各种形式的恶意软件（也称为“流氓软件”，包括病毒、蠕虫、木马或特洛伊木马、间谍软件、广告软件和黑客软件）的程序或软件。</p>
商户	<p>针对 PCI DSS 的目的来说，商户是指为产品和/或服务付款时接受支付卡的任何机构，这些支付卡具有 PCI SSC 五成员（American Express、Discover、JCB、MasterCard 或 Visa）其中一家的商标。请注意，如果销售的服务要以其他商户或服务提供商的名义存储、处理或传输持卡人数据，接受支付卡为产品或服务付款的商户也可以是服务提供商。例如，ISP 是接受支付卡为月度账单付款的商户，如果把商户当作客户托管，它也是服务提供商。</p>
审核日志	<p>也称为“审核记录”。系统活动的序时记录。对于从交易开始到最终结果、围绕或引导操作、程序或事件的一系列环境和活动，可提供足以允许重建、审核和检查的记录。</p>
收单机构	<p>也称为“收单银行”或“收单金融机构”。针对接受支付卡与商户启动并保持关系的机构。</p>
受信任网络	<p>在公司控制或管理能力范围内的公司网络。</p>
授权	<p>授予用户、程序或流程访问权或其他权限。对于网络来说，授权定义验证成功后个人或程序可以执行哪些操作。</p> <p>对于支付卡交易来说，它是指商户得到批准允许将支付卡用于特定交易的实例。</p>
输出过滤	<p>过滤经路由器从内部网络输出的流量的方法，使未授权的流量不会离开内部网络。</p>
输入过滤	<p>过滤经路由器进入内部网络的流量的方法，可以验证传入包确实是从请求的网络输入。</p>
双因素验证	<p>使用两个或多个已验证的因素验证用户的方法。这些因素包括用户拥有的某物（如硬件或软件令牌）、用户知道的某物（如密码、口令或 PIN）或者用户本身或要做的事情（如指纹或其他生物测定方式）。</p>

术语	定义
双重控制	用两个或更多不同的实体（通常是人员）保护敏感功能或信息的流程。两个实体对有漏洞交易中的材料承担相等的物理保护责任。不允许一个人单独访问或使用这些材料（例如，加密密钥）。对于手动生成密钥、传送、加载、存储和检索，双重控制要求将密钥在实体之间分开保管。（另请参阅“ <i>分开保管</i> ”。）
索引簿	在加密法中，一次性索引簿是文本与随机密钥结合在一起的加密算法，或者长度与纯文本一样并只能使用一次的“索引簿”。此外，如果密钥是随机、不重复使用和机密的，一次性索引簿则是牢不可破的。
索引记号	根据指定索引将 PAN 替代为不可预测值的加密记号。
特洛伊	也称为“特洛伊木马”。一种恶意软件类型，安装后允许用户执行常规功能，而特洛伊在不经用户同意的情况下对计算机系统执行恶意功能。
网络	连接在一起共享资源的两台或多台计算机。
网络安全扫描	使用手动或自动工具远程检查机构系统漏洞的流程。安全扫描包括探测内部和外部系统并报告暴露于网络的服务器。扫描可以识别恶意个人可能使用的操作系统、服务器和设备中的漏洞。
网络分段	通过减小持卡人数据环境大小缩减 PCI DSS 评估范围的方法。要达到这个目的，不存储、处理或传输持卡人数据的系统应该通过网络控制与存储、处理和传输持卡人数据的系统隔离开。请参阅《 <i>PCI DSS 要求与安全评估程序</i> 》的网络分段部分，了解使用网络分段的指导说明。
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。
威胁	也称为“数据威胁”或“数据漏洞”。侵入怀疑有未授权的泄露/盗窃、修改或销毁持卡人数据的计算机系统。
威胁	可能引起信息或信息处理资源有意或无意丢失、修改、泄露、禁止访问或其他对公司造成损害的情况或活动。
文件级加密	为特定文件的所有内容进行加密的技术（软件或硬件）。另请参阅“ <i>磁盘加密或列级数据库加密</i> ”。
文件完整性监控	检测某些文件或日志是否被修改的监控技术。当重要文件或日志被修改时，应该向相应的安全人员发出警报。
无害处理	从文件、设备或系统中删除敏感数据，或修改数据使数据在系统受到攻击被访问时无用的流程。
无线访问点	也称为“AP”。允许无线通信设备连接无线网络的设备。通常连接到有线网络，可以在网络中的无线设备和有线设备之间中继传输数据。
无线网络	不用电线物理连接方式连接计算机的网络。
系统组件	包括在持卡人数据环境中或与其连接的网络组件、服务器或应用程序。
现货供应	这一术语描述的产品不是特别定制或为特定客户或用户设计的库存项目，而是可立即使用的产品。
消费者	购买产品、服务或两者都购买的个人。

术语	定义
协议	网络内使用的一致同意的通信方法。具体描述计算机产品进行网络活动应遵守的规则和程序。
信息安全	确保信息机密性、完整性和可用性的信息保护。
信息系统	针对信息收集、处理、维护、使用、共享、传播或配置而组织的一套离散的结构化数据资源。
掩盖	在显示数据时隐藏某个分段的方法。没有查看整个 PAN 的业务需求时可使用掩盖。
验证	确认个人身份、设备或流程的流程。
验证报告	也称为“ROV”。记录支付应用程序针对 PCI PA-DSS 的合规状态的详细情况报告。
业务代码	磁条上位于磁道支付卡失效期后的三位或四位数值。可以有各种用途，如定义业务属性、区分国际和国内交易或识别使用限制。
应用程序	包括所有购买的和自定义的软件程序或程序组，包括内部和外部（如网络）应用程序。
远程访问	从通常来自网络外部的远程地点访问计算机网络。远程访问技术的一个例子是 VPN。
账号	请参阅“主账户 (PAN)”。
政策	管理可接受的计算资源、安全惯例和指导操作程序开发的公司范围的规则。
支付卡	针对 PCI DSS 的目的来说，是指任何具有 PCI SSC 创建成员（American Express、Discover Financial Services、JCB International、MasterCard Worldwide 或 Visa Inc.）商标的支付卡/设备。
职责分离	在不同个人间划分某项职能的步骤、使单独一人不能破坏整个流程的做法。
智能卡	也称为“芯片卡”或“IC 卡（集成电路卡）”。一种嵌入了集成电路的支付卡。电路也称为“芯片”，包含（但不局限于此）和磁条数据相等的支付卡数据。
重新加密	更换加密密钥的流程，目的是限制使用相同的密钥进行加密的数据量。
主机	驻留计算机软件的主要计算机硬件。
主机	用来处理大量数据输入输出和强调吞吐量计算的计算机。主机可以运行多个操作系统，看上去如同操作多台计算机。很多旧有系统都有主机设计。
主机提供商	为商户和其他服务提供商提供各种服务。服务范围从简单到复杂，从服务器上的共享空间到“购物车”选项的整个范围，从支付应用程序到支付网关和处理商的连接，以及每台服务器只供一位客户专用的托管服务。主机提供商可以是在一台服务器上托管多个实体的共享主机提供商。
专用网络	公司使用专用 IP 地址空间建立的网络。专用网络通常设计成局域网。应该使用防火墙和路由器适当保护从公共网络访问专用网络。
状态检测	也称为“动态包过滤”，是一种通过追踪通信包加强安全性的防火墙功能。只有正确响应（“建立的连接”）的传入包才允许通过防火墙。