小型商户支付保护资源

支付词汇表和信息安全术语

1.0 版 | 2016 年 7 月

PCI Security Standards Council®

简介

此*支付和信息安全术语词汇表*是对*《安全支付指南》*（小型商户支付保护资源的一部分）的补充。旨在以易于理解的语言说明相关的支付卡行业 (PCI) 和信息安全术语。

标有星号 (*) 的术语定义基于或源于*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、缩写和首字母缩略词词汇表*（3.2 版，2016 年 4 月）中的定义。

请访问以下网站，参阅*《安全支付指南》*及其他小型商户支付保护资源：

资源	网址
安全支付指南	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
常见支付系统	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
要请教供应商的若干问题	https://zh.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf

注：
最新版*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、缩写和首字母缩略词词汇表*被视为权威来源，有关当前和完整的 PCI DSS 和 PA-DSS 定义，必须参考此表。

词汇表

术语	定义
收单机构 *	参见*商业银行*和*支付处理商*。
杀毒软件 *	可检测、移除和防范恶意软件（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）的软件程序。又称为“反恶意软件软件”。
应用程序 *	在 PC、智能手机、平板电脑、内部服务器或网络服务器上运行的软件程序或程序组。
授权扫描服务商 (ASV) *	经 PCI 安全标准委员会的认证，可以实施扫描服务以识别常见系统配置漏洞的公司。另请参见 *ASV*。
ASV *	“授权扫描服务商”的缩写。
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： • 用户所知，如密码或口令 • 用户所有，如令牌设备或智能卡 • 个人特征，如生物特征
授权 *	在支付卡交易中，在收单机构与发卡机构/处理商验证交易后，商户获得交易许可时，则发生授权。
银行识别号 (BIN)	可识别向持卡人发放支付卡的金融机构的支付卡号前六位（或更多）数。
业务知情需要	根据用户的业务需求（仅限用户工作职能必需的业务需求）授予系统或数据访问权限的原则。
卡数据/客户卡数据 *	卡数据至少包含主帐户 (PAN)，可能还包含持卡人姓名和失效日。PAN 显示于卡片的正面，并且被编码到卡片的词条和/或嵌入式芯片中。又称为持卡人数据。有关可能包含于支付交易中的，但不得在交易获得授权后进行存储的其他数据元素，另请参见*敏感验证数据*。
芯片	又称为“EMV 芯片”。在根据 EMV 交易国际规范处理交易时使用的支付卡上的微处理器（或“芯片”）。

词汇表

术语	定义
芯片和 PIN	消费者在购买商品或服务时，在可读取 EMV 芯片的支付终端上输入 PIN 的验证流程。
芯片和签名	消费者在购买商品或服务时，在可读取 EMV 芯片的支付终端上签名的验证流程。
凭证	用于识别和验证用户是否拥有系统访问权限的信息。例如，凭证通常为用户名和密码。凭证可包含指纹、视网膜扫描，或由便携式“令牌生成器”生成的一次性编号。当访问需要多个凭证时，安全性往往更强。
网络攻击	入侵计算机或系统的任何类型的攻击策略。网络攻击可包括在 PC 上安装间谍软件、入侵支付系统窃取卡数据，或者尝试破坏电网等关键基础设施。
数据泄露	数据泄露是指敏感数据可能被未授权方查看、窃取或使用的事件。数据泄露可能涉及卡数据、个人健康信息 (PHI)、个人可识别信息 (PII)、商业机密，或知识产权等等。
默认密码	新款软件或硬件自带的简单密码。默认密码（如“admin”或“password”或“123456”）很容易被猜中，并且通常可以通过联机搜索获取。它们被用作占位符，并不能提供真正的保护，安装新软件或硬件后必须将其更改为安全系数更高的密码。
电子现金出纳机 (ECR)	可以登记和计算交易并打印收据，但不接受客户卡支付的设备。又称为“收银机”。
加密	使用加密法以数学方法将信息转换为表单（除特定数字密钥持有者以外的人不可使用）的流程。使用加密法可通过降低信息对不法分子而言的价值来保护信息。另请参见*加密法*。
防火墙 *	可防止网络资源遭到未授权访问的硬件和/或软件。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计算机或网络间通信。
取证调查机构	PCI 取证调查机构 (PFI) 是获得 PCI 委员会认证的帮助确定卡数据泄露何时、如何发生的公司。他们使用经验证的调查方法和工具在金融业内实施调查。他们还会与执法机关合作，为涉及任何相关犯罪调查的利益相关者提供支持。

词汇表

术语	定义
黑客	试图绕过计算机系统的安全措施，以获取控制和访问权限的个人或组织。这么做的原因通常是为了窃取卡数据。
托管服务提供商 *	为商户和其他服务提供商提供各种服务，并通过提供商服务器托管或存储客户数据。典型服务包括多个商户在一台服务器上共用空间、为某一商户提供专用服务器或 Web 应用程序（例如带有“购物车”选项的网站）。
集成支付终端	可收取支付款项、登记并计算交易，并打印收据的集成于一台设备中的支付终端和电子现金出纳机。
集成商/经销商	集成商/经销商是指可以实施、配置并/或支持支付终端、支付系统和/或商户支付应用程序的公司。这些公司还可销售支付设备或应用程序以作为其服务的一部分。另请参见*合格集成商经销商 (QIR)*。
日志 *	当计算机系统或网络内部发生特定预定义（通常与安全有关）事件时自动创建的文件。日志数据包括日期/时间戳、事件描述，以及特定于该事件的信息。这些文件可用于对技术问题或数据泄露调查进行故障排除。又称为“检查日志”或“检查记录”。
恶意软件 *	恶意软件设计用于以窃取数据或损坏应用程序或操作系统为目的潜入计算机系统。这类软件通常会在许多业务许可活动进行中进入网络，例如通过电子邮件或浏览网站。恶意软件示例包括病毒、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。
商业银行 *	代表商户处理信用卡和/或借记卡支付的银行或金融机构。又称为“收单机构”、“收单银行”、“卡片处理商”或“支付处理商”。另请参见*支付处理商*。
移动设备	消费类电子设备（例如小型、便携式、可无线连入计算机网络的智能手机和平板电脑）的一般术语。
接受移动支付	使用移动设备受理支付交易。移动设备通常与商用读卡器配件配对。
多因素验证 *	验证两个或多个因素时的用户验证方法。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）。
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。

词汇表

术语	定义
操作系统 *	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软件。示例包括 Microsoft Windows、Apple OSX、iOS、Android、Linux 和 UNIX。
P2PE	PCI 委员会的点到点加密标准的缩写。详情请见 *www.pcisecuritystandards.org*。
PA-DSS *	PCI 委员会的“支付应用程序数据安全标准”的缩写。详情请见 *www.pcisecuritystandards.org*。
密码 *	用于验证用户的单词、短语或字符串。与用户名组合到一起后，密码旨在证明用户的身份，以便其访问计算机资源。
补丁 *	更新为增加了功能或修正了缺陷（或“bug”）的现有软件。
支付应用程序 *	可存储、处理或传输持卡人数据作为支付交易授权或结算一部分的有关 PA-DSS 的软件应用程序。
支付应用程序供应商	向 POS 集成商/经销商销售、分销或许可支付应用程序以便集成到商户支付系统，或直接将支付应用程序提供给商户以便其自行安装和使用的实体。
支付中间件	可将两个或多个可能不相关的支付应用程序连接到一起的软件的一般术语。例如，可以在支付终端上的应用程序和将卡数据发送至处理商的其他商户系统间传输卡数据。
支付处理商 *	由商户雇用的可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（商业银行）。又称为“支付网关”或“支付服务提供商”(PSP)。另请参见*商业银行*。
支付系统	包含在商户零售地点（包括商店/商铺和电商店面）接受卡支付的整个过程，并且可能包括支付终端、电子现金出纳机、连接支付终端的其他设备或系统（例如，用于实现互连的 Wi-Fi，或用于盘点的 PC）、带电子商务组件的服务器（例如支付页面），以及外连至商业银行的连接。
支付系统供应商	向商户销售、许可或分销完整支付解决方案的供应商。解决方案包括在店内处理支付所需的硬件和软件，并提供连接支付处理商的方法。
支付终端	用于通过刷卡、读卡、插卡或触卡方式接受客户卡支付的硬件设备。又称为“销售点 (POS) 终端”、“刷卡机”或“PDQ 终端”。

词汇表

术语	定义
PCI *	支付卡行业的缩写。
PCI DSS *	PCI 委员会的“支付卡行业数据安全标准”的缩写。详情请见 *www.pcisecuritystandards.org*。
遵从 PCI DSS	通过常规业务方法持续满足当前 PCI DSS 的所有适用要求。在某个时间点对遵从性进行评估和认证；但是否持续遵守要求以确保稳健的安全性取决于每个商户。商业银行和/或支付品牌对 PCI DSS 遵从性的正式年度认证有具体的要求。
经 PCI DSS 认证	证明所有适用的 PCI DSS 要求均在某个时间点得到满足。根据具体商业银行和/或支付品牌要求的不同，可通过适用的 PCI DSS 自我评估调查问卷，或源于现场评估的遵从性报告获得认证。
经 PCI 认证的支付应用程序	已根据 PCI 支付应用程序数据安全标准 (PA-DSS) 获得认证的、并且列于 PCI 委员会网站上的软件应用程序。
PCI 认可的支付终端	已根据 PCI PIN 交易安全 (PTS) 标准获得认可的、并且列于 PCI 委员会网站上的支付终端。
PCI 列出的点到点加密解决方案	已根据 PCI 点到点加密 (P2PE) 标准获得认证的、并且列于 PCI 委员会网站上的加密解决方案。
PED *	“PIN 输入设备”的缩写。客户用于输入其 PIN 的键盘。又称为“PIN 键盘”。
PIN *	“个人识别码”的缩写。只有用户和系统知道的用于验证登录系统的用户身份的唯一数字。一般的 PIN 用于预借现金交易的现金自动取款机，或者用于可代替持卡人签名的 EMV 芯片卡。PIN 有助于确定持卡人是否获得了卡片使用授权，并可在卡片失窃时防止非授权使用。
主帐户 (PAN) *	可识别持卡人帐户的唯一信用卡和借记卡卡号。
权限滥用	以滥用的方式使用计算机系统访问权限。示例包括系统管理员恶意访问卡数据，或某人恶意窃取和使用管理员的提升访问权限。
PTS *	PCI 委员会的 PIN 交易安全标准的缩写。PTS 是针对 PIN 认可交互点 (POI) 终端的一套模块化评估要求。详情请见 www.pcisecuritystandards.org。
QIR *	“合格集成商或经销商”的缩写。详情请见 *www.pcisecuritystandards.org*。

词汇表

术语	定义
合格安全性评估商 (QSA) *	获得 PCI 安全标准委员会的认可，可认证实体对 PCI DSS 要求的遵从性的公司。
定期支付	商户在一段时间内对其客户定期计费的一种计费方式，例如包月会员或订阅。对收单机构/处理商而言，实现卡数据令牌化有助于安全实施这种计费方式，从而确保对此方式予以保护，并免除商户的相关责任。
远程访问 *	从网络外部位置访问计算机网络。远程访问连接可自公司自己网络的内部发起，也可自远程位置发起。虚拟专用网络 (VPN) 是远程访问技术的一个示例。远程访问可在内部（如 IT 支持人员）发起，也可在外部（如服务提供商、第三方代理商、集成商/经销商）发起。
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。
路由器 *	连接两个或多个内部或外部计算机网络以“传输”或引导数据通过网络，并确保数据在网络间正确流动的硬件或软件。路由器还可以通过仅允许获得认可的流量并拒绝未获认可的流量提高安全性。
安全读卡器 (SCR)	连接手机或平板电脑，从而安全接受支付卡的 PTS 认可设备。PCI PTS 认可的 SCR 可以通过 SRED 保护并加密卡数据。另请参见 ***SRED***。
安全代码 *	印刷在支付卡正面或背面签名条上的三位或四位数值。此代码仅与单张卡片关联，可作为附加检查的依据，以确保此卡为法定持卡人所有，通常应用于无实卡交易期间。又称为卡安全码。
自我评估调查问卷 (SAQ) *	用于记录某实体的 PCI DSS 评估中自我评估结果的 PCI DSS 认证工具。
敏感验证数据 *	用于验证持卡人和/或授权支付卡交易的存储于卡片词条或芯片上的安全相关信息。
服务提供商 *	为商户提供各种服务的商业实体。通常，这些实体可代表另一个实体（例如商户）存储、处理或传输数据，或者是提供托管防火墙、入侵检测、托管和其他 IT 相关服务的服务提供商。又称为“供应商”。
盗用	直接从消费者的支付卡或商户所在位置的支付基础设施盗取卡数据，例如通过劣质手持式读卡器，或通过修改商户支付终端来盗取卡数据。其目的在于实施诈骗，对商户具有严重的威胁，并且可能会冲击任何商户环境。

词汇表

术语	定义
盗用设备	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。又称为“读卡器”。
小型商户	通常只有一个或可能有多个经营场所的、IT 预算有限或没有 IT 预算的，并且通常未配备在职 IT 工作人员的企业。
SRED	安全读取并交换数据的缩写。旨在对支付终端中的卡数据进行保护和加密的一套 PCI PTS 要求。PCI 委员会列出的点到点加密 (P2PE) 解决方案须使用 PTS 认可并列出的启用 SRED 并主动执行卡数据加密的支付终端。
独立终端	不依赖于连接商户环境内的任何其他设备，并且不执行任何其他功能的支付终端。运行的唯一要求就是通过互联网连接或电话线与处理商实现互连。如果某终端要求连接计算机化自动现金出纳机或具有多功能性（如移动设备），则不能将其视为独立终端。
强效验证	用于确认用户或设备的身份，以确保所保护系统的安全性。强效验证这一术语通常与多因素验证 (MFA) 互为同义词。
收银机	请参见*电子现金出纳机*。
令牌化	将主帐户 (PAN) 替换为名为令牌的替代值的过程。令牌可用于替代原始的 PAN，可在卡片缺失（例如失效、退款或定期计费）时发挥作用。令牌还可在卡片被盗时提高帐户安全性，因为在此情况下口令将不可用，因此对不法分子没有任何价值可言。
非加密数据	无需先进行加密即可读取的任何数据。又称为“纯文本”和“明文”数据。
供应商	为商户提供业务运作所需的产品或服务的商业实体。提供服务时，供应商可被视为服务提供商，并且需要访问商户环境中可能会影响卡数据安全的物理位置或计算机系统。另请参见*服务提供商*。
虚拟支付终端 *	基于 Web 浏览器访问收单机构、处理商或第三方服务提供商网站，以授权支付卡交易。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。商户通过安全连接的 Web 浏览器手动输入支付卡数据。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。

词汇表

虚拟专用网络 (VPN) *	VPN 由较大型网络（例如互联网）中的虚拟电路组成，而非通过物理线缆直接连接。VPN 的末端贯穿较大型的网络，以便创建私人、安全的连接。
病毒	在“受感染”计算机上，将自己的副本复制到其他软件或数据文件中的恶意软件。复制成功后，病毒便可以执行恶意有效负载，例如删除计算机上的所有数据。病毒可能会潜伏并于稍后执行其有效负载，或者也可能从不触发恶意操作。以电子邮件附件的形式或网络消息的一部分重新发送，从而进行自我复制的病毒称为“蠕虫病毒”。
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。
漏洞扫描	可在计算机上或网络中检测并分类潜在弱点（漏洞）的软件工具。可由组织的 IT 部门或安全服务提供商（例如授权扫描服务商）执行扫描。另请参见*授权扫描服务商 (ASV)*。
Wi-Fi *	无需物理连接线缆即可连接计算机的无线网络。
无线支付终端	使用各种无线技术中的任意一种连接互联网的支付终端。