PCI 产业概述和产业发展动态分享

atsec 白海蔚 2024 年 3 月底

关键词：支付卡产业、PCI DSS、数据安全、支付交易

*如有兴趣了解早期产业信息请参见作者于 2021 年 4 月发布信息：
PCI 产业标准家族和相关体系简介发展动态

1 PCI 产业概述

1.1 传统支付产业链和基本的交易流程

传统的支付流程参与者通常包括持卡人、商户、收单机构、卡组织、发卡机构和服务提供商。

- 持卡人（Cardholder）是支付卡拥有者，将通过卡呈现（Card Present）或卡不呈现（Card Not Present）的交易方式来购买商品或服务。
- 发卡机构（Issuer）是代表支付卡品牌或直接由支付卡品牌发行支付卡的银行或其他组织。例如：Visa 和 MasterCard 是不直接发卡的，他们的卡是通过银行或其他组织发行的。
- 商户（Merchant）是支付环节收款的组织，通常是为了销售或分发商品或服务，且参与支付。
- 收单机构（Acquirer）可以被称为银行、商业银行、处理者（Processor）或独立销售组织（ISO）。就美国运通、Discover 和 JCB 而言，收单机构本身也可以是支付品牌之一。最终，收单机构是与商户有合同关系的银行或其他实体，以完成其涉及支付卡使用的交易。
- 卡组织（Payment Brand）包括但不限于 Visa、MasterCard、美国运通、Discover、JCB、银联。

下图是支付处理工作流程的基本概述：我们是从商户购买商品或服务的“支付卡的持卡人”，商户向收单机构发送支付交易数据，收单机构通过卡组织的支付网络向发卡机构发送支付业务数据。发卡机构是实际向持卡人发卡的机构，持卡人执行支付交易时，发卡机构都会向商户的收单银行提供交易授权或拒绝。收单机构和发卡机构需要交换支付信息来完成交易的过程称为“清算”（Clearing）。商户银行（收单机构）为持卡人的购买向商户付款以及持卡人的银行（发卡机构）向持卡人开具账单的过程称为“结算”（Settlement）。

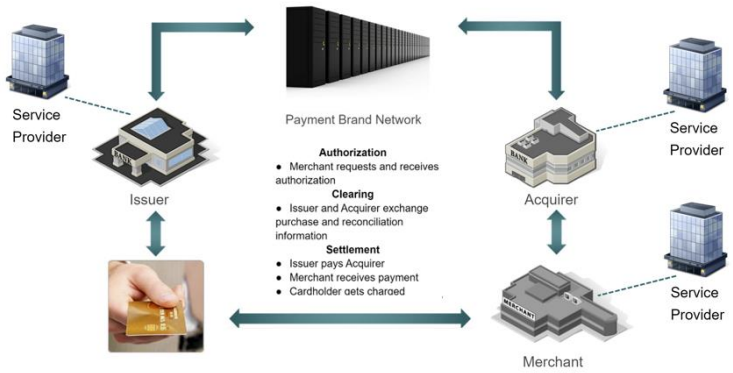

图 1：传统支付流程（源自 PCI SSC）

当消费者作为持卡人向发卡机构申请办理支付卡、当发卡机构委托制卡机构完成支付卡的生产和制造、当持卡人在商户购买产品或服务需要提供支付卡的数据，例如卡号、姓名、有效期或 PIN、CVV2 等信息，而这些支付卡数据在整个交易的支付流程中进行传输、存储和处理的安全性如何保障，实际的应用场景中支付卡产业可以采用的标准如何选择和使用，让我们一起梳理下支付卡产业安全标准与传统支付产业链的关系。

1.2 支付卡产业安全标准贯穿传统支付产业链

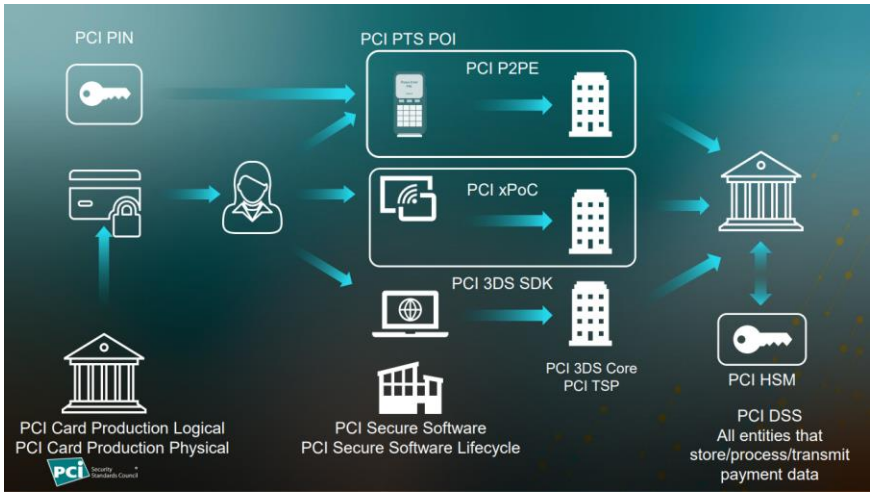

图 2：贯穿传统支付流程的 PCI 标准（源自 PCI SSC）

如文章前述所提及，发卡机构将把持卡人申请办理的支付卡信息提供给卡片制造供应商，以完成支付卡的生产和制造，故而该环节 PCI 产业要求针对卡厂执行物理安全和逻辑安全审核，即图中所示：PCI Card Production Physical 和 PCI Card Production Logical，现行版本为 2022 年 6 月发布的 v3.0.1。（可参见 atsec 早期文章：PCI 卡片生产和供应安全标准 V3.0.1 变更说明及合规流程）

在 ATM 和销售点（POS）终端进行联机和脱机支付卡交易处理期间，对 PIN（个人识别码）数据进行安全管理、处理和传输。所以针对收单机构、收单机构的商户、收单机构的代理服务商、处理 PIN 交易的机构、提供相关密钥管理功能的机构、支持 PIN 输入设备的机构等等将需要遵从 PCI PIN 安全标准，现行版本为 2021 年 3 月发布的 v3.1。（可参见 atsec 早期文章：PCI_PIN 标准相关截止时间的解读以及近期重要信息.pdf ）

日常支付场景中我们不难遇到 POS 机具用于刷卡交易，而在此场景中可以考虑采用点对点加密的解决方案、组件和应用，从而精简持卡人数据的流动降低交易风险。标准涉及加密和解密，密钥管理，安全设备管理等要求。通过对加密环境中 POS 终端所获取的数据进行加密，提高持卡人数据的安全保护；持卡人数据在需要的时候在解密环境通过解密环节获取，从而可以有效地在两点之间去除明文卡号数据，该解决方案的开发、认可和部署则需要满足 P2PE 标准要求，现行版本为 2021 年 9 月发布的 v3.1。

纵观整个支付卡产业，通常可以概括为从卡片制造、生产到卡片的使用，而在使用时则会需要依托网络、应用系统、软件和硬件设备以及人员来完成。为确保可靠且准确的支付交易，作为支付交易流程一部分的系统和软件的设计、开发和维护方式必须能够保护支付交易的完整性以及与支付交易相关的所有存储、处理或传输的敏感数据的机密性，那么针对支付应用软件可遵从软件安全框架体系（SSF：Software Security Framework）（原 PA DSS 支付应用数据安全标准），SSF 又包含面向软件厂商的安全软件生命周期（SLC：Secure Software Lifecycle）标准，现行版本是 2021 年 1 月发布的 v1.1，以及面向支付应用产品的安全软件（Secure Software）标准，现行版本是 2023 年 5 月发布的 v1.2.1。（可参见 atsec 早期文章：PA-DSS 到 PCI SSF 标准的过渡）

针对支付终端设备、加密机、支付移动设备应用等等，PCI SSC 则维护了 PCI POI、PCI HSM、CPoC、SPoC、MPoC 标准，详细信息可参见：https://www.pcisecuritystandards.org/document_library/。

而另一种日常支付场景就是目前越来越多的电子商务网站出现的线上无卡交易，电子商务 CNP 无卡交易的购买过程启用安全身份验证，以达到降低欺诈交易的风险就是采用了 3DS 协议。3DS 的安全身份验证协议基于三域模型作为协议核心基础，三个域分别是发卡域、商户/收单域和交互域。其中收单域和发卡域通过交互域连接，目的是在电子商务交易期间对持卡人进行身份验证或提供身份验证和账户确认。这些额外的安全防护有助于防止未经授权的 CNP 交易，并保护商家免受 CNP 欺诈。通常发卡域的访问控制服务器（ACS：Access Control Server）、商户或收单域的 3DS server 和交互域的目录服务器（DS：Directory Server）会关注 PCI 3DS 标准要求，现行版本是 2017 年 10 月发布的 v1.0。（可参见 atsec 早期文章：PCI 3DS 标准简介 ）

不难看出 PCI 支付卡产业经过多年发展，把整个传统的产业链进行了细分，致力于在每一个支付的环节做好支付卡数据的安全保护要求，并维护相关的产业标准。当一个支付交易流程完整时则构建了一个持卡人数据环境，交易流程则涉及支付卡数据的传输、存储和处理，故而通过 PCI DSS 标准来对持卡人数据环境进行合规建设，现行版本是 2022 年 3 月发布的 v4.0。（可参见 atsec 早期文章：PCI DSS v4.0 变更系列之一——变更概述.pdf ）

整个支付卡产业的相关标准家族仍然还在适应新的风险和支付形态进行演进，且良性的持续发展和改进，atsec 也投入了较大的工作并付出我们的贡献。

2 PCI 产业发展动态分享

2.1 一切似乎都变了

2.1.1 支付方式发生了变化 Payments Are Changing

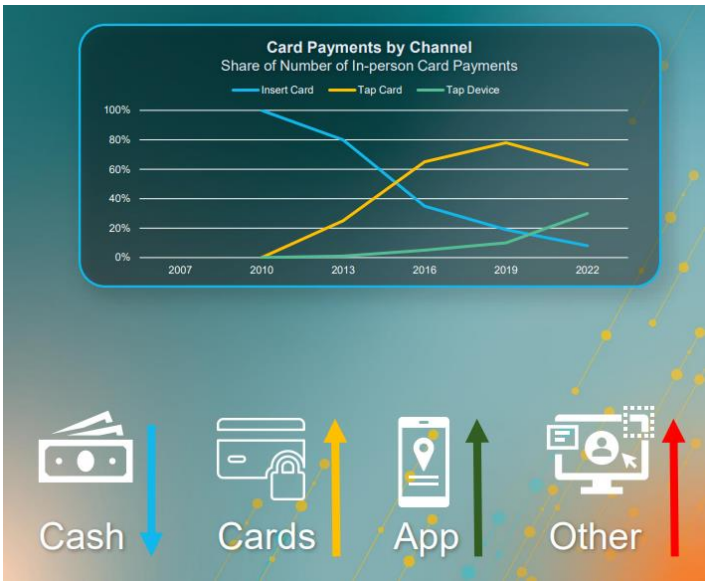

图 3：支付方式的变化（源自 PCI SSC）

伴随时代发展，不难发现人们的支付习惯正在发生变化，移动设备越来越成为支付体验的一部分；支付卡 BIN 升级为 8 位（可参见 atsec 早期文章：8 位长度银行卡 BIN 码在 PCI DSS 中的实践）；软件解决方案越来越常见，也越来越复杂；支付卡的形态也正在发生变化，多种多样的移动设备、智能手表等穿戴设备，仿佛让我们置身于一场奇幻的支付卡化妆舞会。

2.1.2 支付卡产业安全标准委员会发生了变化 PCI SSC Are Changing

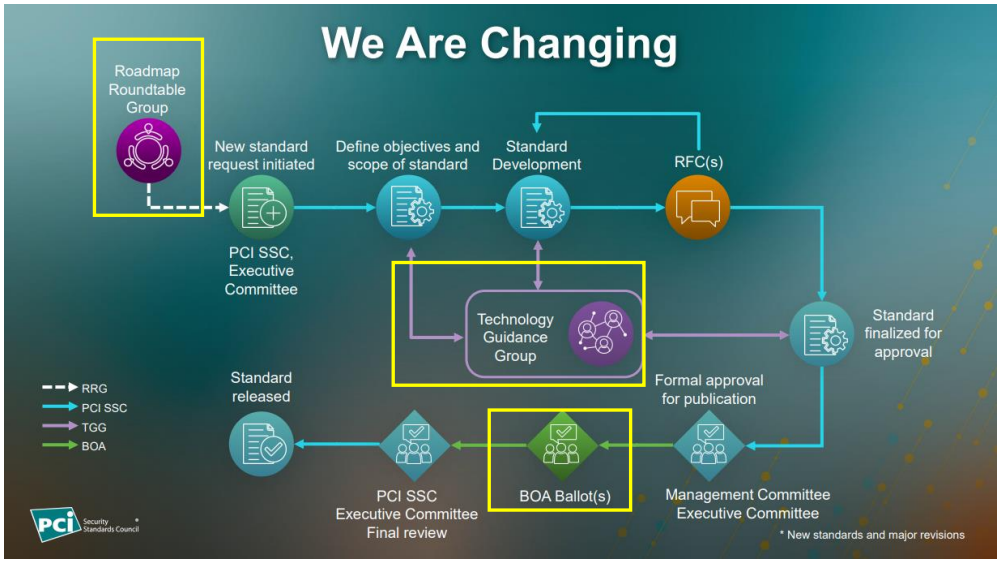

图 4：PCI SSC 标准发布流程的变化（源自 PCI SSC）

如上图所示，支付卡产业安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）创建和发布一个标准的过程：从启动新标准请求、确定标准的目标和范围、标准的开发、请求意见稿（RFC：Request For Comments）、标准报批、标委会的管理委员会和执行委员会正式批准、PCI 标委会最终审查，直到标准发布的过程中，PCI SSC 也在不断创新和变化。

- 成立圆桌会议 Roundtable
  - 2018 年，PCI SSC 设置和维护了全球执行评估机构圆桌会议（GEAR：Global Executive Assessor Roundtable），目的是获得 PCI SSC 有经验且优秀的合格安全评估机构的建议和意见。允许 PCI 合格安全评估机构的高级管理人员代表 PCI 评估员群体提出观点，就评估和评估员计划相关的问题向 PCI SSC 提供建议、反馈和指导。GEAR 也是为了进一步强化评估机构产业且开发高质量的培训体系，从而进一步致力于全球支付数据的安全保障。GEAR 希望产业优化和改进 PCI 评估人员和机构的能力和技能，从而更好地为金融机构（如商户、支付处理者）提供服务。近年来，包括 atsec 在内的 GEAR 和 PCI 高层团队就热门技术和标准发展展开了密切地讨论，并获得了诸多的成果，比如 PCI DSS v4.0 及其相关方法论、PCI SSF 等。
  - 2022 年，PCI SSC 成立了“Coffee with the Council”，开始着手制作播客系列节目，希望通过广泛被接受的传播形式吸引支付行业，分享新闻、最新动态、第三方的访谈、小组讨论或案例研究，也分享标委会活动的报道等等。
  - 路线图圆桌会议（RRG：Roadmap Roundtable Group）小组在标委会年度战略规划过程中发挥着关键作用，有助于推动标委会的发展方向和战略举措。
- 技术指导小组（TGG：Technology Guidance Group）为标委会的标准和计划提供积极的技术监督。成员有机会在 RFC 发布之前的开发过程中为标委会的标准提供意见。
- 推动 BOA（BOA：Board of Advisors）投票环节，在每个阶段，PCI SSC 将在适用的情况下，审查、处理并解决根据流程收到的所有意见，并将这些意见及其解决方案（如有）传达给顾问委员会，包括意见来源的归属等等。

2.1.3 标准发生了变化 Standards Are Changing

PCI 标委会自创立之初的 2 个支付卡产业标准发展至今已有 15 个相关标准，构成了支付卡行业的 PCI 标准家族。详细的标准家族列表可参见下图。

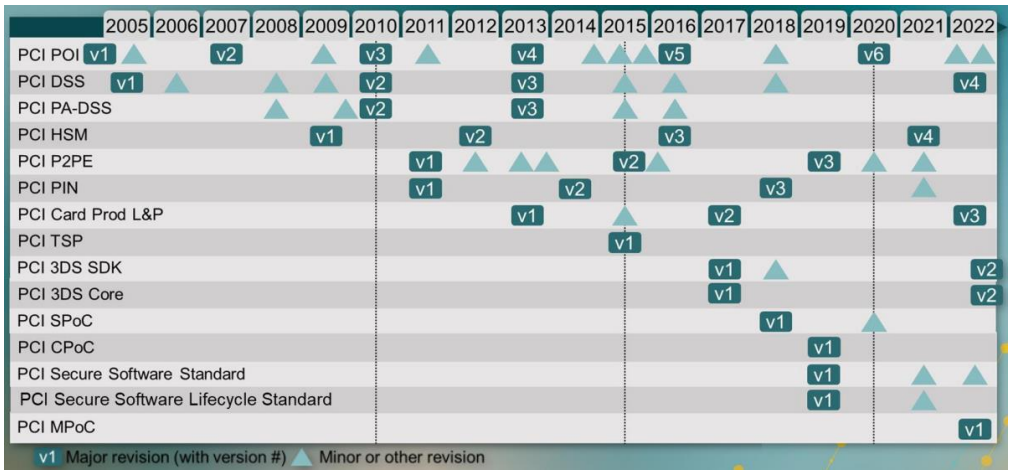

图 5：PCI 支付卡产业标准家族（源自 PCI SSC）

PCI 产业标准伴随支付业务的创新和发展，除了最基本的客观目标以外，越来越多地考虑与更多的利益相关者进行互动，以获取更加可以落地实施的标准建议。标准的行文格式不断优化以易于阅读和理解，并在充分考虑支付交易逻辑和支付形态的前提下，标准增加了灵活性，也增加了更多的指导方案和建议。目前就产业最新变化的 2 个标准信息分享如下：

- PCI DSS 标准 v4.0 版本自 2024 年 4 月 1 日起强制实施

PCI DSS 标准 v1.0 发布于 2006 年，发展至今历经 4 个主版本变化，其中 v1.2 和 v3.2.1 是顺应 IT 技术发展而更新的小版本，也在支付产业内稳定地使用了较长周期。PCI DSS v4.0 于 2022 年发布，为了帮助产业机构平稳过渡，新旧版本标准通常都会有一段时间共同使用的过渡周期。v3.2.1 版本标准在 2024 年 3 月 31 日强制退休，自 2024 年 4 月 1 日起，我们将正式步入 PCI DSS v4.0 时代。

图 6：PCI 标准发展大事记（源自 PCI SSC）

atsec 自 2018 年至今作为 PCI 标委会 GEAR 成员，积极参与产业标准工作，代表产业与 PCI SSC 紧密沟通并反馈相关建议。在最近的洛杉矶 GEAR 会议后，PCI 标委会经过与支付产业内相关者进行详细讨论后，决定终止且废除了 PCI DSS v4.0 中引入的 INFI（INFI: Items

Noted for Improvement）工作表，并于 2024 年 3 月 20 日通知立即生效，QSA 安全评估机构无需完成 PCI DSS 评估的 INFI 工作表。这也无疑体现了 PCI 产业积极聆听来自 GEAR 和 BOA 成员的声音并持续改进的工作方式。

- PCI SSF 标准自 2023 年 10 月替代 PCI PA DSS 支付应用安全标准

支付软件的安全性是支付交易流程中重要的组成部分，也是实现可靠和准确支付交易的关键。软件安全框架（SSF：Software Security Framework）体系包括安全软件生命周期（SLC：Secure Software Lifecycle）和安全软件（Secure Software）评估。PCI SSF 标准的评估目标是供应商的软件本身，是针对支付软件功能定义的一套安全需求，最终目的是为了保护支付交易与数据的机密性与完整性；SLC 标准评估目标是软件供应商，是针对软件供应商定义的一套安全需求，以验证供应商设计、开发与交付的流程，保障支付软件在整个生命周期的安全。PCI SSF 标准取代了 PA DSS 成为确保支付软件安全的主要标准。2022 年 10 月 28 日，PA DSS 已正式退出历史舞台。

自 2022 年 10 月底有效期结束后，所有之前完成 PA DSS 验证的应用软件已被移至“仅可接受预先部署”（Acceptable Only for Pre-existing Deployments）列表。

在 atsec 和产业内厂商的共同努力下，目前大陆地区诸多支付软件和厂商已完成 PCI SSF 包含软件本身和 SLC 的完整评估。

软件安全标准还有一个特点就是可以在主体标准要求的基础上不断根据新的软件形态和技术发展开发和发布新的模块（Module）。目前该标准的最新标准是 1.2.1，已经包括了三个模块，分别是 Module A：账户数据保护要求（主要为了达到原有已经废除的 PA DSS 的目的），Module B：终端软件要求（主要保护基于 POI 平台设备上的软件），Module C：Web 软件要求（为了保护基于互联网技术、协议和语言的支付交易）。相信未来 SSF 还将不断推出新的模块以适应更多的支付形态和技术，atsec 也将持续投入反馈相关建议。

2.2 似乎一切又没变

随着支付形态和标准的演进和发展，我们看到信息安全的许多根基的技术和方法还在延续，比如 ASV 外部扫描和渗透测试、边界防护、入侵检测等等。

产业相关机构的投入和热情并没有改变。

自 2006 年 PCI 产业标准委员会成立以来，atsec 作为独立且中立的第三方信息安全咨询和评估机构，成为 PCI SSC 授权的第一批 QSA 合格安全评估机构。atsec 伴随 IT 信息技术和整个支付产业的飞速发展，我们始终在这里：始终专注信息安全领域的技术；始终致力于做好数据安全标准的合规工作。

不论产业形态、技术方案、业务创新等一切是不是似乎都变了，atsec 专注信息安全、坚持做正确的事情是一直没变的。更多关于 PCI 相关标准的咨询和评估需求请查阅：[atsec - IT 安全测试和评估专家 - PCI DSS QSA, ASV, SSF，渗透测试，风险评估]。

参考资料：

1) https://www.pcisecuritystandards.org/

2) https://www.atsec.cn/