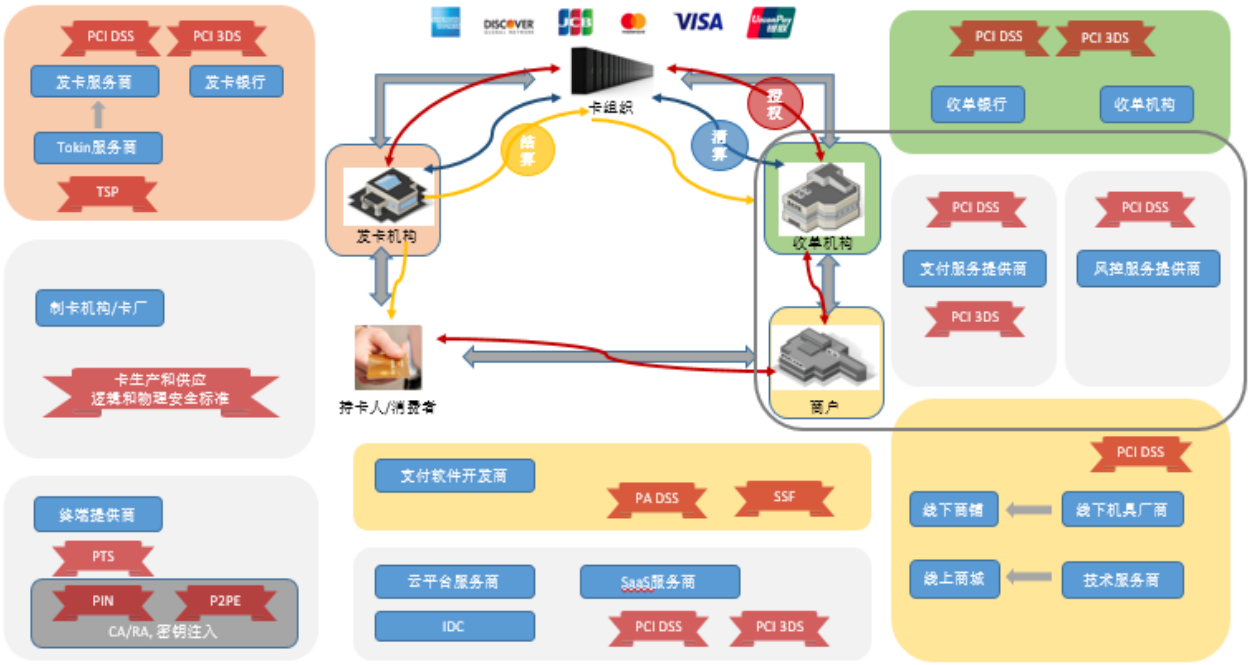
PCI 产业标准家族和相关体系发展动态

2021 年 4 月 atsec 白海蔚

atsec 作者谨以此文分享目前支付卡产业（PCI：Payment Card Industry）的安全标准及其相关体系的发展动态。

支付卡产业安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）推进全球范围整个支付行业的标准化进程，通过提供以业务驱动、灵活和有效的数据安全标准和评估验证体系，帮助产业的各个机构减少和防止发生数据泄露风险，从而提高支付的安全性。为了保证整个支付产业的安全防护能力，安全建设工作不仅仅是一家机构的工作。存储、传输或者处理持卡人数据的每个机构都必须发挥作用。所以 PCI SSC 为业界共同制定的安全标准和体系提供了一个开放的平台，从银行、商户和服务提供商到支付设备的制造厂商、软件开发商，寻求行业各机构的共同参与。

首先，通过下图展示传统的支付产业链中相关角色及其典型的支付交易模型。



图：传统支付产业链和相关标准示意

如上图所示，不同的机构在支付产业中发挥着各自的作用，同时也会面临不同的风险，故而 PCI 标准家族从各个层面的不同维度制定了不同的安全标准要求。支付卡产业安全标准委员会 PCI SSC 自 2006 年成立以来，整合支付卡产业相关资源，积极配合不断推进不同层面的安全技术标准发展和演进。截至 2021 年 4 月，PCI 安全标准家族包括但不限于如下主要安全标准：

PCI 标准家族

标准名称	发布时间/版本	授权评估机构	简要说明
PCI DSS： Payment Card Industry Data Security Standard 支付卡产业数据安全标准	v3.2.1 / 2018 年 5 月	PCI QSA（Qualified Security Assessor） PCI ASV（Approved Scanning Vendor）	最为广泛采用的标准，适用于涉及持卡人数据存储、传输和处理的所有金融机构，如商户、支付服务提供商、银行、清算机构等；目前产业正在积极编写最新版本，计划将于 2021 年底发布 v4.0 版本。
PA DSS： Payment Application Data Security Standard	v3.2 / 2016 年 5 月	PCI PA QSA	面向涉及授权和/或结算的支付应用的安全标准；已经被 SSF（下文介绍）所替代，2021 年 6 月

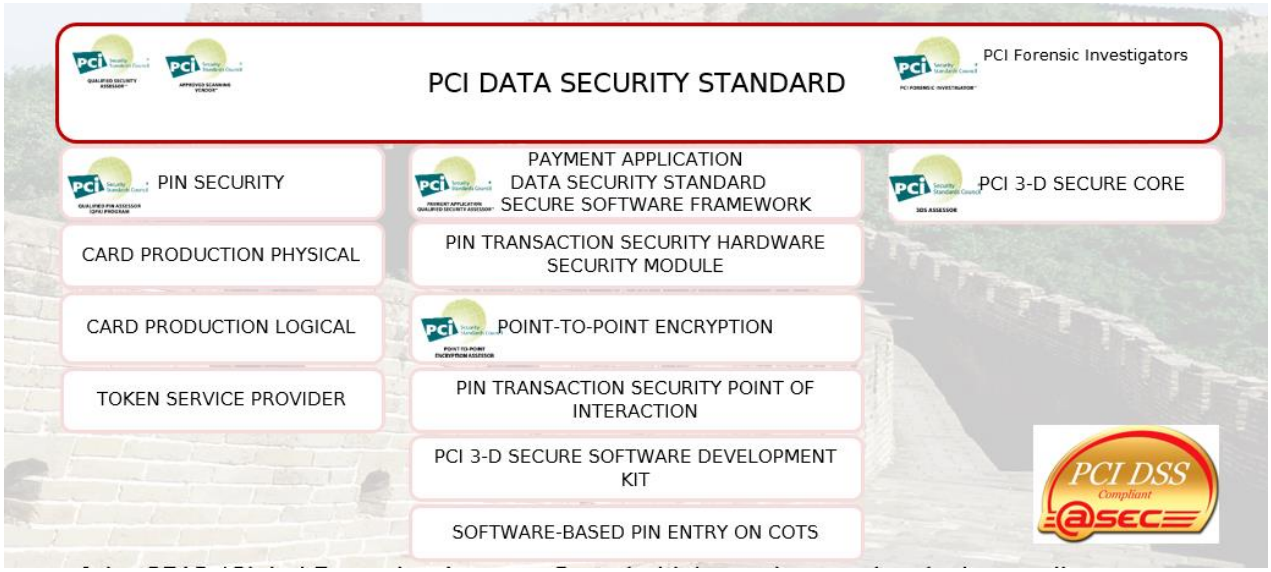
支付应用安全标准			停止接受 PA DSS 的评估验证申请。
P2PE：Point-to-Point Encryption 点对点加密	v3.0 / 2019 年 12 月	PCI P2PE QSA PCI P2PE PA QSA	面向点对点加密的解决方案、组件和应用，标准涉及加密和解密，密钥管理，安全设备管理等要求。参见： http://atsec.cn/it-security-services/pci/pci-services/pci-p2pe/index.html
PTS：PIN Transaction Security PIN 交易安全 -Hardware Security Module (HSM) -Point of Interaction (POI)	v3.0 / 2016 年 6 月 v6 / 2020 年 6 月	PCI Recognized Laboratories（PTS 列表）	面向硬件设备的检测，目前包括加密机 HSM 和 POI 设备两个主要标准。
Card Production and Provisioning Logical Security Requirements 卡生产和供应逻辑安全标准 Card Production and Provisioning Physical Security Requirements 卡生产和供应物理安全标准	v2.0 / 2017 年 1 月 v2.0 / 2017 年 1 月	CPCA：CARD PRODUCTION SECURITY ASSESSOR	面向卡片生产和制作机构，目前涉及两个标准，分别面向逻辑和物理安全要求。
PCI 3DS Core Security Standard PCI 3DS 核心安全标准	v1.0 / 2017 年 10 月	3DS ASSESSORS	PCI 3DS 核心安全要求用于保护 3DS 功能执行或者 3DS 数据存储所在的 3DS 环境。需要保护的特定功能包括：3DS 服务器（3DS server）、3DS 目录服务器（3DS Directory Server）和 3DS 访问控制服务器（3DS Access Control Server）。参见： http://atsec.cn/it-security-services/pci/pci-services/pci-3ds/index.html
Contactless Payments on COTS (CPoC™) Security and Test Requirements 基于 COTS 非接触支付（CPoC）	v1.0 / 2019 年 12 月	PCI Recognized Laboratories（CPOC 列表）	基于现货设备（COTS：commercial off-the-shelf）的非接触式支付安全和测试要求，比如智能手机或者平板电脑上的支付解决方案。基于软件的 PIN 输入是 CPoC 不允许的。
PIN Security Requirements and Testing Procedures PIN 安全要求和测试流程	v3.1 / 2021 年 3 月	QPA：QUALIFIED PIN ASSESSORS	在线或者离线交易过程中，针对个人识别数字（PIN：personal identification number）安全管理、处理和传输的要求。参见： http://atsec.cn/it-security-services/pci/pci-services/pin-

			security/index.html
Software-Based PIN Entry on COTS Security Requirements COTS 基于软件的 PIN 输入安全要求	v1.1 / 2020 年 6 月	PCI Recognized Laboratories（CPOC 列表）	面向 COTS 设备上 PIN 持卡人验证方法（CVM：Cardholder Verification Method）输入相关的安全要求。
PCI TSP Security Requirements PCI 令牌化服务器提供商安全要求	v1.0 / 2015 年 12 月	P2PE 评估机构可以执行 TSP 安全评估	针对生成或者发布 EMV 支付令牌的令牌化服务提供商（TSP）的物理和逻辑安全要求。
SSF：Software Security Framework 软件安全框架 -Secure Software Standard 安全软件标准 -Secure SLC Standard 安全软件生命周期标准	v1.0 / 2019 年 1 月 v1.1 / 2021 年 2 月	SOFTWARE SECURITY FRAMEWORK ASSESSORS 分别涉及安全软件评估机构 Secure Software 和安全生命周期评估机构 Secure SLC 两个不同的资质维护	安全软件框架目前涉及两个独立的标准，评估工作分别由两个不同资质的评估机构完成。此外安全软件标准具有扩展性，通过增加标准的模块的形式，完善更多的软件类型的安全要求。 参见：http://atsec.cn/it-security-services/pci/pci-services/pci-ssf/index.html

除了安全标准本身以外，PCI SSC 还维护了诸多的指导文档，比如渗透测试指导、ASV 的体系指导、维护 PCI DSS 合规的最佳实践、针对大型机构的 PCI DSS 合规、第三方安全保障、风险评估指导、实施安全意识程序的最佳实践，等等。

标准与资质的示意

如上表中所提及，不同的安全标准合规评估体系分别由具有相应资质的评估机构执行。比如 atsec 具有 PCI SSC 所授权的 PCI QSA、ASV、PFI（事后取证调研）、P2PE、P2PE PA、QPA、3DS 评估机构、PA QSA、SSF 安全软件评估和安全生命周期评估等相关资质，可以为不同机构提供较为全面的支持和评估服务。参见如下示意图：



PCI 产业涉及的相关机构 - 机构 PO 和 GEAR

全球范围支付产业中的相关机构，例如商户、银行、支付服务提供商、软硬件提供商都可以成为 PCI 的参与机构（PO：Participating Organizaitons），积极参与标准化相关的工作以及相关交流活动。

截止到目前（2021 年 4 月），全球共有 736 家参与机构。全球参与机构分布如下：

参与机构所在地区	参与机构数量
ASIA PACIFIC	72
CEMEA	17
EUROPE	153
SLA & CARIBBEAN	36
USA	414
CANADA	44

此外，中国银联于 2020 年成为了 PCI 的战略成员（STRATEGIC MEMBER）。

在全球范围各机构的共同参与之下，PCI SSC 为了进一步强化评估机构产业且开发高质量的评估和培训体系，从而进一步致力于全球支付数据的安全保障，自 2018 年开始设置和维护全球执行评估机构圆桌会议（GEAR： Global Executive Assessor Roundtable）。圆桌会议希望能够获得更多的 PCI 评估体系的建议和意见，包括但不限于培训内容和资格要求，以及面对不断发展的市场提高评估人员的服务水平。此外，产业希望优化和改进 PCI 机构和评估人员的能力和技能，从而更好地为金融机构（如商户、支付处理者）提供服务。

PCI SSC 全球执行评估机构圆桌会议是支付安全评估机构的高级领导者和 PCI SSC 高级领导者之间沟通的直接渠道。atsec 作为独立的第三方安全评估机构，始终积极跟进产业标准和资质的维护，鼓励完成合规建设的机构加入并成为参与机构。并且，atsec 从 2018 年第一届 GEAR 成立开始，是 GEAR 成员之一，长期积极参与相关标准化和研讨工作，为产业和标准的演进付出微薄之力。