PCI PIN Security 标准简介

作者：atsec 张志鹏

PIN Security 的标准演进

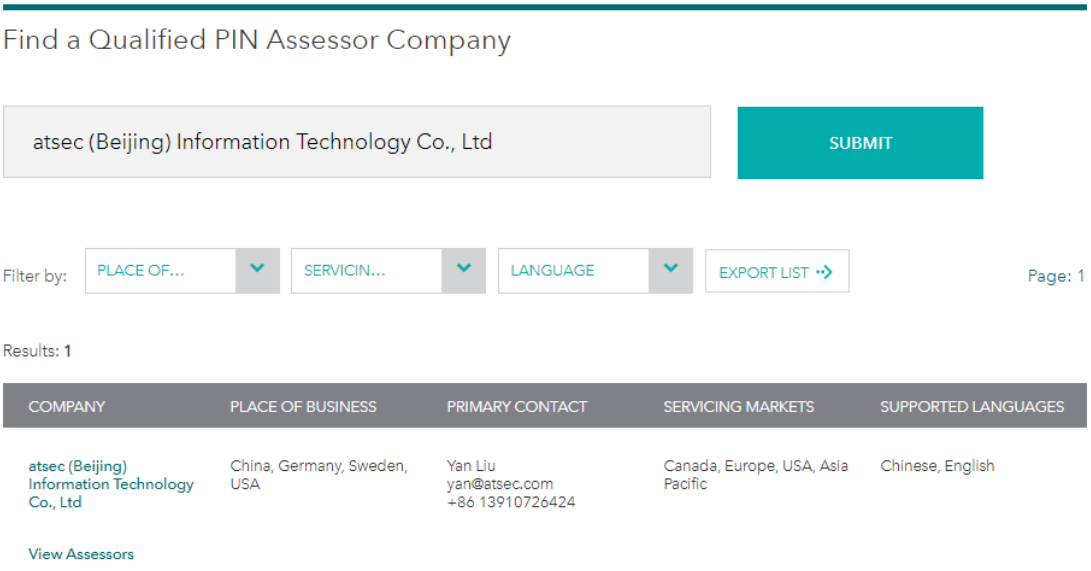
随着电子支付交易的爆发式增长导致了网络犯罪的不断增加，尤其是针对信用卡盗刷的案件逐年上升。因此，联机交易和脱机交易中保护机密数据（例如 PIN：personal identification number 以及用于保护 PIN 的相关密钥等）比以往任何时候都变得更加重要。

PIN 作为交易敏感认证数据经常会用于高风险场景，例如大额支付交易、脱机交易等。因此对保护支付安全有更大的意义。本文所要介绍的正是用于保护 PIN 数据以及相关密钥数据的安全标准-PCI PIN 安全要求和测试程序（PCI PIN Security Requirements and Testing Procedures）。该标准包括：在 ATM 以及有人看守和无人看守销售点（POS：point-of-sale）终端处理联机交易或者脱机交易时，针对个人识别数字（PIN）安全管理、处理和传输的完整的要求。

该安全要求标准早在 2011 年 10 月，就已经由支付卡产业（PCI：Payment Card Industry）安全标准委员会（SSC：Security Standards Council）发布初始版本 v1.0，2014 年 12 月发布 v2.0 版本，2018 年 8 月发布 v3.0 版本。2019 年 1 月以前，PIN 安全审核公司的资质是由各个卡品牌自己来维护和管理。而 PCI SSC 于 2019 年 1 月发布了合格 PIN 安全评估者（QPA： Qualified PIN Assessor）管理方案，简称 QPA 方案。意味着今后 PIN 审核公司的资质统一由 PCI SSC 管理和维护。在 PCI SSC 的网站列表上可以查询到已获得审核资质的 QPA 公司和个人

（https://www.pcisecuritystandards.org/assessors_and_solutions/qpa_assessors）。

只有获得 QPA 资质的审核公司和人员，才可以执行 PIN Security 的合规性审核。截至 2019 年 12 月，取得该资质的公司全球有 51 家，中国本土具有 QPA 资质的审核机构只有 atsec 一家，且 atsec 的两位审核员是中国地区最早的 QPA 审核员。atsec QPA 资质列表截图如下。



PIN Security 标准介绍

该标准具体包括 7 个控制目标（Control Objective）和 33 个安全要求（Requirement），标准的结构分为标准主体部分，标准附录（Normative Annex）A，B，C，以及一个补充附录 Appendix A。

- 标准主体部分 - 是针对交易处理操作（Transaction Processing Operations）中，关于 PIN 保护的安全要求，包括了 7 个控制目标，这 7 个控制目标是由 33 个安全要求组成的：
  - 控制目标 1（Control Objective 1）：采用确保安全的设备和方法处理本标准所管控

的交易 PIN。(PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure.)

- 控制目标 2 (Control Objective 2): 用于 PIN 加密/解密的密钥以及相关的密钥管理的创建流程，应确保不可能预测任何密钥或者确定特定的密钥比其他密钥更大的可能性。(Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.)
- 控制目标 3 (Control Objective 3): 密钥应在安全的方式下运送和传输。(Keys are conveyed or transmitted in a secure manner.)
- 控制目标 4 (Control Objective 4): HSM 的密钥载入和 PIN 输入设备应在安全的方式下处理。(Key-loading to HSMs and PIN entry devices is handled in a secure manner.)
- 控制目标 5 (Control Objective 5): 密钥的使用应禁止或能够检测未授权的使用。(Keys are used in a manner that prevents or detects their unauthorized usage.)
- 控制目标 6 (Control Objective 6): 密钥采用安全的方式进行管理。(Keys are administered in a secure manner.)
- 控制目标 7 (Control Objective 7): 用于处理 PIN 的设备和密钥应在安全的方式下管理。(Equipment used to process PINs and keys is managed in a secure manner.)

➢ 标准附录 A (Normative Annex A) – 采用非对称技术进行对称密钥分发 (Symmetric Key Distribution using Asymmetric Techniques)

- A1 – 采用非对称技术操作进行远程密钥分发 (Remote Key Distribution Using Asymmetric Techniques Operations)

- A2 – 证书和注册授权 CA&RA 操作（Certification and Registration Authority Operations）

➢ 标准附录 B（Normative Annex B） – 密钥注入设施（KIF：Key-Injection Facilities）

➢ 标准附录 C（Normative Annex C）- 核准算法的最小密钥长度要求和算法之间的等效关系

➢ 补充附录（Appendix A）- 标准要求的适用性列表 Applicability of Requirements

合规价值

PCI PIN 标准适用于涉及支付卡帐户 PIN 交易处理的所有收单机构和相关供应商，例如收单银行、服务提供商、POS 机具生产厂商，密钥注入设施 KIF 和证书处理机构 CA&RA。

当机构管理、处理和/或传输 PIN 数据时，PCI PIN 安全合规可能会被卡品牌、监管机构以及合作机构所强制要求。比如 VISA 要求所有处理 VISA PIN 数据的服务提供商（包括代表 VISA 客户进行 PIN 处理、转换、接受，和/或密钥管理服务）应完全符合 VISA PIN 安全体系安全要求和 VISA 规定的验证截至日期，这些机构包括但不限于：获取 PIN 的第三方 VisaNet 处理者（VNP：VisaNet Processor）、作为服务提供商获取 PIN 的客户 VNP、获取 PIN 第三方服务者（TPS：Third-Party Servicers）、加密和支持组织（ESO：Encryption and Support Organizations）。

成功提交 PIN AOC（PIN Attestation of Compliance）给 VISA 证明其合规状态的 VISA PIN 安全体系参与者将会被列在 VISA 服务提供商网站的全球服务提供商注册系统中。

根据 VISA 规定，没有完成合规评估的罚则规定如下：

➢ 最初的违背以及未合规的每个月，至多最初违背之后的四个月：每个月 10,000 美元罚

金

- 违背四个月之后，以及其后的每个月：每个月 25,000 美元罚金

以上信息可见卡品牌对 PIN Security 不合规机构的惩罚力度是非常严厉的。因此，涉及 PIN 交易处理，以及针对 PIN 保护的密钥管理的机构，一定要和相关卡品牌确认好合规要求。做到先期规划好合规要求，以保障业务的安全开展。

atsec 作为具有 QPA 资质的安全审核评估机构，期待为产业支付安全做出贡献！