PCI 卡片生产和供应安全标准 V3.0.1 变更说明及合规流程

作者：陈谨运（atsec 中国）

2022 年 10 月

关键词：PCI、CPSA、卡片生产和供应安全

atsec(Beijing) information technology Co., Ltd
Floor 3, Block C, Building 1, Boya C-Center,
Beijing University Science Park, Life Science ParkChangping District, Beijing, Postcode: 102206
P.R. China

Tel +86-10-53056681
Fax +86-10-53056678

1 卡片生产和供应安全标准简介

支付卡安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）是由 American Express，Discover，JCB，MasterCard 和 Visa Inc.作为创始成员，于 2006 年创立的关注支付产业安全的组织。UnionPay 于 2021 年正式成为 PCI SSC 的战略成员，与创始成员一起共同领导 PCI SSC 的发展。PCI SSC 维护了不同支付环节相关的安全标准，以下是 PCI SSC 维护的安全标准图示[1]：

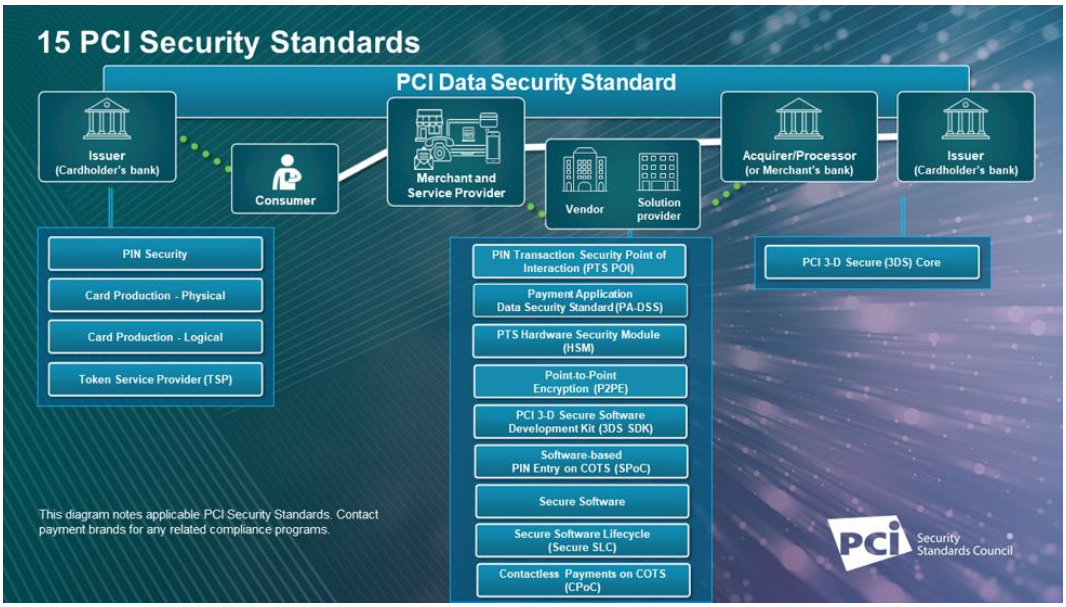

图 1：PCI SSC 维护的安全标准

在卡制造和供应安全环节，卡片生产和供应的机构的安全防护由 PCI SSC 维护的 PCI 卡片生产和供应安全标准提供保障。PCI 卡片生产和供应安全标准包含了“Payment Card Industry Card Production and Provisioning Physical Security Requirements and Test Procedures”（以下简称“PCI 卡片生产和供应物理安全标准”）和“Payment Card Industry Card Production and Provisioning Logical Security Requirements and Test Procedures”（以下简称“PCI 卡片生产和供应逻辑安全标准”），分别从物理安全和逻辑安全方面对卡片生产和供应的机构提出安全要求，以确保其所处理的数据得到安全保护。

1.1 PCI 卡片生产和供应物理安全标准

PCI 卡片生产和供应物理安全标准定义了涉及卡片生产和供应的机构全面的信息来源，其中可能包括制造商、个人化提供商、预个人化提供商、芯片嵌入商、数据准备和履行（fulfillment）的机构。该标准规定了机构在以下过程之前、之中和之后必须遵循的物理安全要求和程序：

- 卡片制造
- 芯片嵌入
- 个人化
- 存储
- 包装
- 邮寄
- 运输或交付
- 履行

除了上述卡片生产活动外，PCI 卡片生产和供应物理安全标准还定义了以下实体的物理安全要求和测试流程：

[1] *注：图 1 引自 https://www.pcisecuritystandards.org/pci_security/standards_overview*

- 执行基于云或安全元件（SE：Secure Element） 的供应服务
- 管理空中传输（OTA：Over-the-air）个人化、生命周期管理和个人化数据准备
- 管理相关密钥

PCI 卡片生产和供应物理安全标准的要求如下所示：

图 2：PCI 卡片生产和供应物理安全标准要求

1.2 PCI 卡片生产和供应逻辑安全标准

所有与卡片生产和供应相关的逻辑安全活动相关的系统和业务流程，如数据准备、预个人化、卡片个人化、PIN 码生成、PIN 码邮寄器以及卡片载体和分发都必须符合 PCI 卡片生产和供应逻辑安全标准。

PCI 卡片生产和供应逻辑安全标准还包括以下实体的逻辑安全要求：

- 执行基于云或安全元件（SE：Secure Element） 的供应服务
- 管理空中传输（OTA：Over-the-air）个人化、生命周期管理和个人化数据准备
- 管理相关密钥

PCI 卡片生产和供应逻辑安全标准的要求如下所示：

图 3：PCI 卡片生产和供应逻辑安全标准要求

1.3 标准版本历史

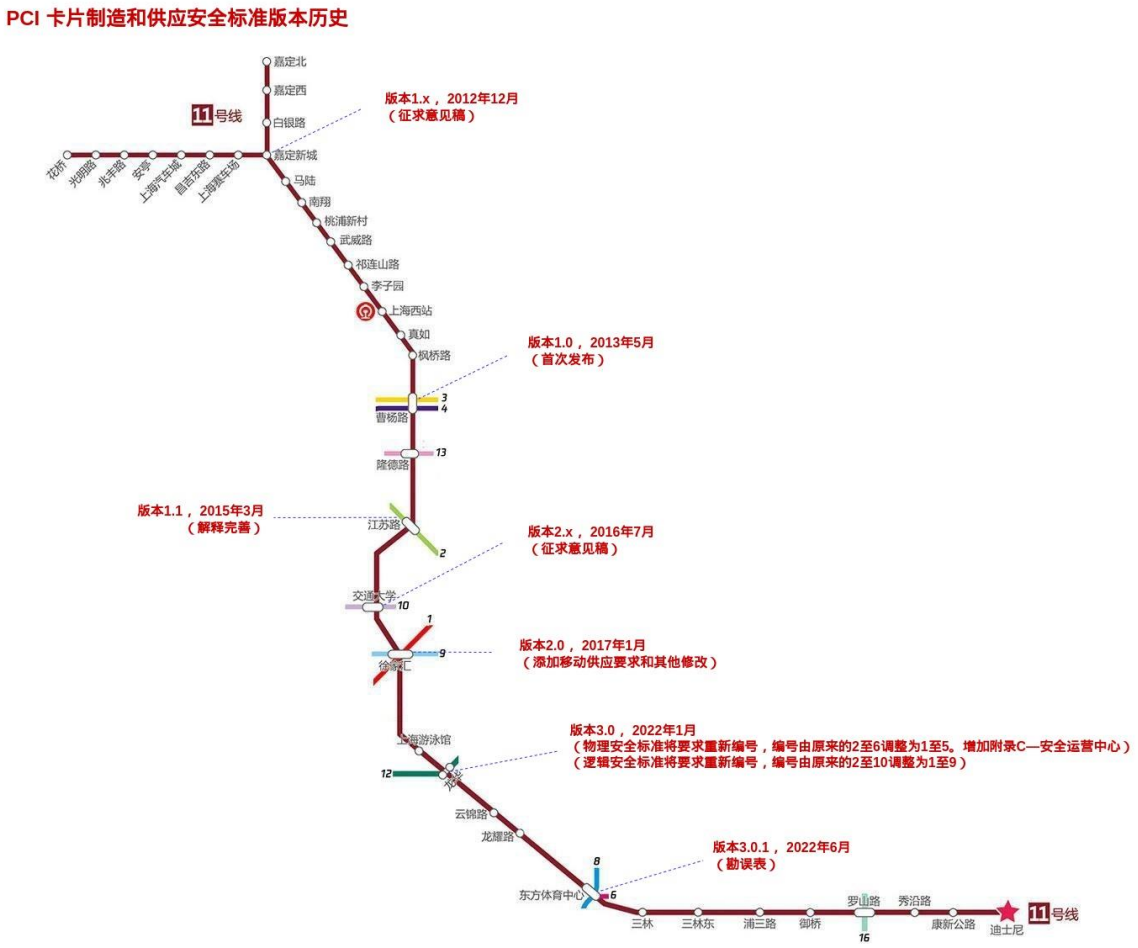

图 4：PCI 卡片生产和供应安全标准版本历史

PCI 卡片生产和供应安全标准的征求意见稿始于 2012 年 12 月，正式版本于 2013 年 5 月发布。当前最新的标准版本 3.0.1 发布于 2022 年 6 月。在标准设立之初，仅有少数卡品牌采用该标准对卡片生产和供应的机构进行安全要求，并且由卡组织进行标准的维护和审核机构的授权工作。直至 2017 年，PCI 卡片生产和供应安全标准 2.0 版本正式由 PCI SSC 进行统一的维护，并且由 PCI SSC 对审核机构进行授权，以及对审核人员进行资质授权和培训。

卡组织作为 PCI 卡片生产和供应安全标准推动的核心角色，主要负责以下职能：

- 跟踪和执行标准落实情况
- 制定罚款规则和费用、并确定服务商的合规期限
- 制定验证过程以及确定需要合规的机构
- 批准和公布合规实体
- 制定取证调查和账户数据泄漏响应的规则
- 监控并协助完成对账户数据泄露的调查

2 变更内容概述

以下表格内容描述了 PCI 卡片生产和供应安全标准从 2.0 到 3.0.1 变更内容的摘要，更具体的内容可以参考 PCI SSC 发布的《PCI_Card_Production_v3.01_Summary_of_Changes_v2_to_v3.01》。

2.1 物理安全要求的变化摘要

索引	物理安全要求的改变	类型
整体	在文件中增加了检验程序。	补充指导
整体	将要求从 2 到 6 重新编号为从 1 到 5。	补充指导
整体	将整个文件中的 “雇员”一词改为“人员”、“个人”、“卡片制作人员”或“顾问”（如适用）。	补充指导
整体	通篇修改徽章系统为访问控制系统。	要求改变
要求 1 - 角色和责任		
1.1.1 **供应商角色**	定义了必须由供应商的雇员担任的角色。	要求改变
1.1.6 **安全交流和培训**	澄清了有关供应商设施安全的信息可以通过海报、通知或电子媒介完成。	要求改变
1.2.1.1 **预先筛选**	对于签约的警卫，可以由警卫公司提供预审要求的证据，如执照副本等；但是，供应商必须收集和保留这些证据。 允许供应商使用自己的保险单，为签约警卫服务提供适当的责任保险。	要求改变
1.2.1.2 **管制/限制**	增加了管理层预先指定为急救人员的人员进入高安全区（HSA：High Security Area）的条件。	要求改变
1.2.2 **角色和责任**	对之前发布的常见问题（FAQ：Frequently Asked Questions）中关于非授权访问尝试用语的澄清回复。	要求改变
要求 2 -生产场所		
2.1.3 **外墙、 门和窗**	规定了外墙开口的标准，HSA 窗户必须是不可打开的。	要求改变
2.3.2.1 **位置和安全保护**	规定安全控制室的窗户必须是不可打开的。	要求改变
2.3.4.1 **访问控制**	允许使用声音警报。 规定访问控制服务器必须位于同一设施内。	要求改变
2.3.4.3 **实物材料的转移**	在货物-工具陷阱门（goods-tools trap）中增加了运输和交付区域，并重新定义为关于同一设施内不同 HSA 之间材料转	要求改变

	移的要求。 澄清了上述内容适用于实物材料。	
2.3.4.4 **安全控制**	澄清了防弹玻璃或铁条的要求适用于建筑物外墙或门上的窗户。	要求改变
2.3.5.6 **金库**	增加了 EN 1143-1 安全存储单元-要求、分类和防盗测试方法-第 1 部分：保险箱、ATM 保险箱、保险库门和保险库。6 级或更高的等级可作为等同于 UL 608 Class1 防盗认证。	要求改变
2.3.6.2 **运输和交付地区**	在为了释放房间内检测到的人员并停止报警的情况下，将相关日志的保留时间从永久改为两年。	要求改变
2.3.6.2 **运输和交付地区**	澄清了现有设施与新设施的外室要求。	补充指导
2.4.1 **警报系统**	澄清在任何了解报警系统终止密码的卡片制作人员离职时，必须停用该终止密码，并且只有警卫和安全团队成员才应了解该终止密码。	要求改变
2.4.2 **徽章管理**	通篇修改徽章系统为访问控制系统。	要求改变
2.4.2.1 **识别徽章**	包括挂绳（要求）也进行了修改。	要求改变
2.4.3 **徽章访问系统**	规定对于同一设施内的多座建筑，徽章访问系统的单一中心位置可以管理所有的建筑以及公共或私有网络的使用条件。	要求改变
2.4.3.3 **远程访问控制**	新的一节使用原有的要求。	补充指导
2.4.7.1 **半年度检查**	规定除了对所有安全设备和硬件进行检查外，还必须进行测试。	要求改变
2.4.7.2 **电池测试**	澄清了电池测试标准。	要求改变
要求 3 - 生产程序和审计跟踪		
3.7.1.2 **日志审查**	明确规定，除非另有说明，本文件中的所有日志必须至少保留两年。	要求改变
3.8.4 **热转印铝箔**	增加了解决热敏碳带的部分。	要求改变
要求 4 - 包装和交付要求		
4	修改了关于快递规定。 更新了术语的一致性。	要求改变

	澄清发送给发行人或支付品牌的样本卡或证明不在本要求的范围内。	
4.3 **打包**	澄清包装破裂强度描述。	要求改变
4.5 **交付要求**	指定的额外标准。	要求改变
4.5.1 **寄送卡片**	澄清了信封标准和预分类设施的使用。 增加了转移到邮件设施的标准。	要求改变
4.5.1.2 **信盒（等待送达）**	明确包装标签要求。	要求改变
4.5.2 **快递服务**	规定了非个人化批量卡的额外标准。	要求改变
4.5.3.1 **非装甲车**	调整了语言，增加了对空运和海运的补充。	要求改变
4.5.3.3 **空运**	增加了进出航空站的运输要求。	要求改变
4.5.3.4 **海运**	增加了进出港口设施的运输要求。	要求改变
4.5.3.5 **铁路货运**	增加了铁路货运的新章节。	要求改变
附录 B：逻辑安全要求 - CCTV 和访问控制系统（ACS）管理		
B.1 **用户管理**	规定了闭路电视和访问控制系统升级的最低能力。 澄清了远程管理访问的例外情况，如果与经批准的 SOC 一起使用。 增加了系统不支持的密码长度要求的例外。	要求改变
B.2.2 **特征和用途**	系统强制要求密码的长度至少为 12 字符或同等强度。	要求改变
附录 C		
附录 C	新章节，“安全操作中心 SOC”。	要求改变
词汇表		
词汇表	增加了词汇表的定义。卡片制作人员、双重控制、设施、参与的支付品牌和公共网络。	补充指导

2.2 逻辑安全要求的变化摘要

索引	对逻辑安全要求的改变	类型
整体	在文件中增加了测试程序。	补充指导
整体	将要求从 2 到 10 重新编号为从 1 到 9。	补充指导
整体	将整个文件中的“雇员”一词替换为“人员”或“卡片制作人员”（如适用）。	补充指导
整体	在涉及 FIPS 140-2 要求的地方增加了 FIPS 140-3 要求。	要求改变
整体	通篇修改徽章系统为访问控制系统。	要求改变
要求 1 - 角色和责任		
1.2 **安全职责的分配**	规定后备 CISO 和 IT 安全经理必须是供应商的雇员。	要求改变
要求 2 - 安全政策和程序		
2.1 **信息安全政策**	阐明了信息安全政策必须传播给所有相关人员（包括供应商和业务伙伴）。	要求改变
要求 3 -数据安全		
3.4 **持卡人数据的传输**	澄清了预授权来源的定义和记录。	要求改变
要求 4 -网络安全		
4.2 **一般要求**	澄清了持卡人和基于云的供应数据（cloud-based provisioning data）在环境中从其接收/生成到其生命周期结束的流程图必须保持最新。 增加了持卡人和基于云的供应数据在环境中从其接收/生成到其生命周期结束的流程图必须至少每 12 个月审查一次以确保准确性。	要求改变
4.6.1 **连接条件**	澄清了从设施外访问徽章物理访问控制系统的例外情况（如果与批准的 SOC 一起使用）。	要求改变
4.8.2 **渗透**	澄清了通用漏洞评分的使用。	要求改变
要求 6 - 用户管理和系统访问控制		
6.1	增加了多因素认证的额外标准。	要求改变

用户管理	增加了系统不支持的密码长度要求的例外。	
6.2.2 **特征和用途**	要求密码最小长度为 8 个字符改为 12 个字符。除非如果操作系统不支持 12 个字符，那么使用系统支持的最大字符数，但绝对不能少于八个字符的最小长度。	要求改变
要求 7 - 密钥管理。秘密数据		
7.4.2 **密钥经理**	明确规定副密钥经理必须是雇员。	要求改变
7.7 **密钥加载**	明确了密钥持有人和密钥经理在密钥装载中的角色。	要求改变
要求 8 - 密钥管理：机密数据		
8.1 **一般原则**	增加了使用随机或伪随机过程生成密钥和密钥组件的标准。	要求改变
规范性附件 A		
批准算法的最小和等效的密钥大小和强度	与其他标准一致的更新。 增加了 EdDSA 作为批准的算法。	补充指导
缩略语和术语词汇表		
缩写和术语词汇表	增加了以下术语的定义：卡片制作人员、设施、媒体、多因素认证、非控制台访问、参与的支付品牌、私有网络、公共网络和拓扑图；并澄清了远程访问。	补充指导

3 atsec PCI 卡片生产和供应安全标准的合规流程

atsec 作为 PCI SSC 授权的机构，具有 CPSA、PCI QSA、ASV、PFI（事后取证调研）、P2PE、QPA、3DS 评估机构、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。详细的 PCI SSC 授权 atsec 能执行评估的标准参见如下示意图：

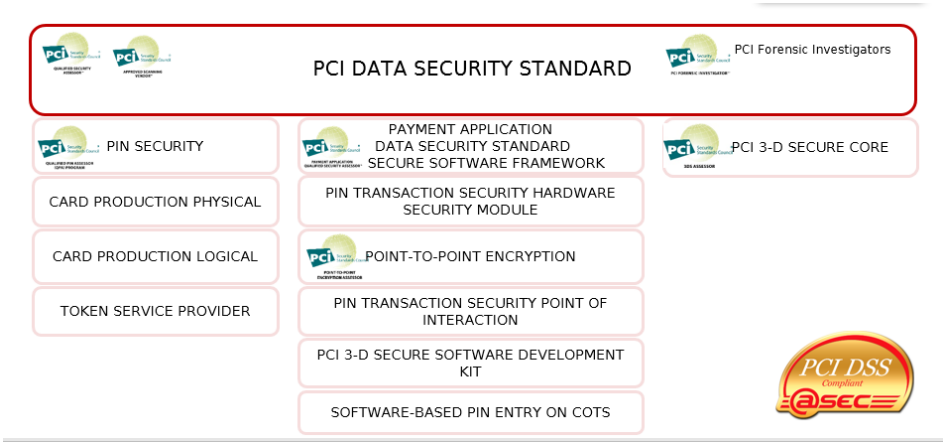

图 5：PCI SSC 授权 atsec 可执行评估的标准

PCI 卡片生产和供应安全标准的合规流程与其它 PCI 标准合规流程有一定的差异。该标准在开始执行评估前，需要由卡生产安全评估人员（CPSA：Card Production Security Assessor）与卡组织进行沟通，并确定卡组织对卡片生产和供应的机构的要求（如采用的标准版本，合规时间等方面的内容）。详细的评估步骤如下：

I. 制定评估计划
II. 评估准备
III. 现场检查
IV. 记录评估结果
V. 评估结果提交
VI. 整改检查过程发现的不合规项
VII. 证据保存
VIII. 安全事件响应

CPSA 的评估流程可参考如下示意图：

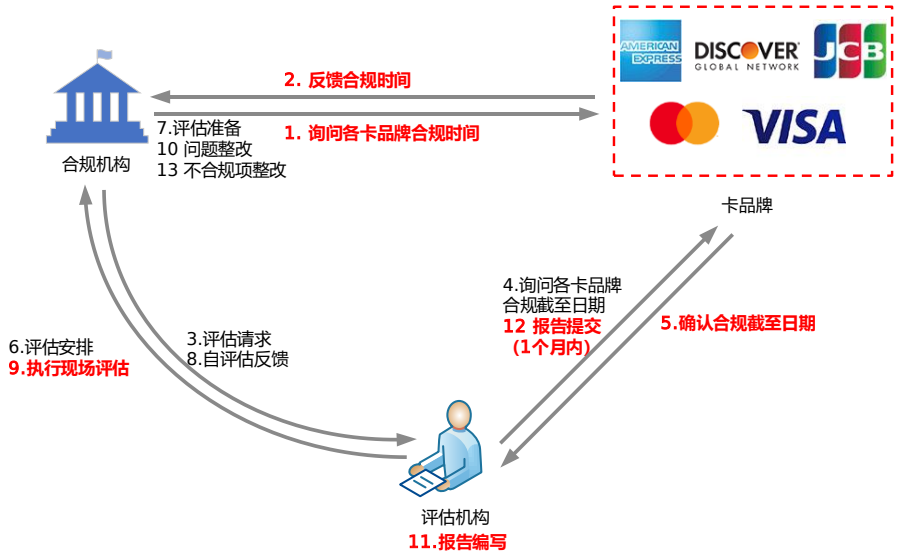

图 6：CPSA 评估流程

4 参考文档和链接

[1]. Card Production and Provisioning Logical Security Requirements: https://docs-prv.pcisecuritystandards.org/Card%20Production/Standard/PCI_CP_Logical_SR_TPs_v3.0.1_Final.pdf

[2]. Card Production and Provisioning Physical Security Requirements: https://docs-prv.pcisecuritystandards.org/Card%20Production/Standard/PCI_CP_Physical_SR_TPs%20v3.0.1_Final.pdf

[3]. Card Production Summary of Changes: https://docs-prv.pcisecuritystandards.org/Card%20Production/Supporting%20Document/PCI_Card_Production_v3.01_Summary_of_Changes_v2_to_v3.01.pdf

[4]. atsec 官网: www.atsec.cn