支付卡产业 PCI DSS 合规建设

——商户和服务提供商分级和验证要求

作者：白海蔚（atsec 中国）

2019 年 8 月

关键词：PCI、QSA、SAQ、合规建设、商户分级、验证要求

atsec(Beijing) information technology Co., Ltd

Floor 3, Block C, Building 1, Boya C-Center,

Beijing University Science Park, Life Science Park

Changping District, Beijing, Postcode: 102206

P.R.China
Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.cn

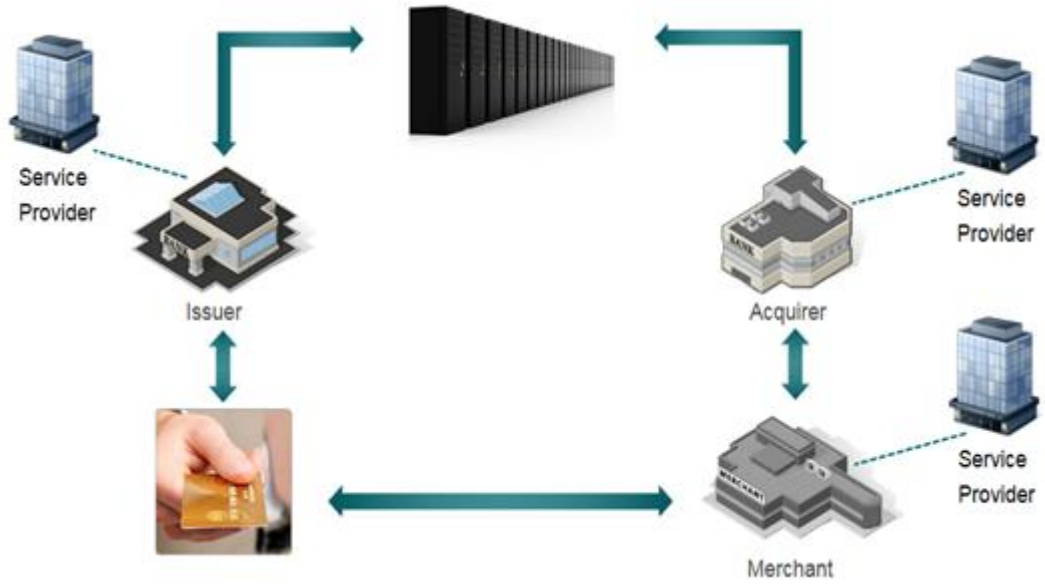
1 支付卡产业链以及 PCI DSS 合规建设的基本要求

PCI SSC（Payment Card Industry Security Standards Council）是由 Visa 国际组织、万事达（MasterCard Worldwide）、美国运通（American Express）、JCB、美国发现金融服务（Discover Financial Services）五家支付品牌在 2006 年秋共同筹办设立的统一且专业的信息安全标准委员会。

1.1 支付卡产业链

完整的支付链包含持卡人、商户、收单机构、卡品牌、发卡机构以及服务提供商几个不同的角色。本文不探讨 POS 等终端设备刷卡支付、扫码支付，以及线上的互联网支付、手机 APP 支付等具体业务流程，因为 PCI DSS 重点关注于获得支付卡数据后针对数据的传输、存储和处理的安全保护。

首先作为持卡人（消费者），到商户进行消费，持卡人的卡数据通过网络传送给收单机构（也称为收单银行或者商户银行），收单机构要通过国际卡品牌的网络把数据传输给卡片的发卡机构，确认后再通过卡品牌的网络回复给收单机构，收单机构将得到的确认信息通知给商户，以此完成支付的授权流程。最终商户完成这笔交易，把货品交给消费者，也从收单机构处获得货款，而持卡人接到发卡机构的账单完成还款，以此完成清算和结算。基于以上描述，整个的支付过程包括清算、结算和授权。产业链上涉及的角色参见下图：



1.2 PCI DSS 合规建设的基本要求

PCI 产业维护了一整套完整的标准体系，包括但不限于 PCI DSS、PA DSS、P2PE、PTS、3DS、PIN Security 等等，而针对每一个标准都会有独立的被授权的资质。以 PCI DSS 为例：PCI DSS 标准被授权的合规审核机构称为 QSAc，该审核机构的审核人员经过考试后成为有资质的 QSA 审核人员，年度的合规审核工作则需要有资质的 QSA 机构执行。

1.2.1 PCI DSS 标准的整体要求

PCI DSS（Payment Card Industry Data Security Standard）支付卡产业数据安全标准，截至本文发布时现行版本为 v3.2.1，自 2019 年 1 月 1 日起强制执行。标准的不断升级代表了支付卡产业紧随 IT 发展步伐，但是标准的核心要求以及框架始终稳定，基本标准要求如下：

建立和维护安全的网络	1. 安装并维护防火墙配置以保护持卡人数据 2. 系统口令和其它安全参数不使用厂商默认设置
保护持卡人数据	3. 保护存储的持卡人数据 4. 对公共开放网络上传输的持卡人数据加密
维护漏洞管理程序	5. 使用并定期更新防病毒软件 6. 开发和维护安全的系统和应用
实施访问控制措施	7. 限制对持卡人数据的访问到必需的业务访问 8. 对计算机访问用户分配唯一的帐号 9. 限制对持卡人数据的物理访问
定期监控和测试网络	10. 跟踪并监控对网络资源和持卡人数据的所有访问 11. 定期测试安全系统和流程
维护信息安全策略	12. 维护信息安全策略，以解决内外部的安全问题

1.2.2 PCI DSS 中扫描服务供应商（ASV）要求

基于 PCI DSS 标准要求的 11.2 条款：

PCI DSS 要求	测试程序	指南
11.2 至少每个季度运行一次内部和外部网络漏洞扫描，并且在网络有任何重大变化（例如安装新的系统组件，更改网络拓扑，修改防火墙规则，产品升级）时也运行漏洞扫描。 *注：可在季度扫描流程中综合多次扫描报告，以表明所有系统均已扫描，且所有漏洞均已解决。可能需要其他文档记录来确认解决过程中有未修复的漏洞。* *如果评估商确认 1）最近的扫描结果为通过，2）实体具备要求每季度扫描一次的书面政策和程序，3）扫描结果中指出的漏洞在重新扫描中显示为已修复，则不要求四次季度扫描均通过才能认定最初 PCI DSS 合规。在最初 PCI DSS 审核后的几年里，必须出现四次季度扫描结果均为通过的情况。*	11.2 检查扫描报告和支持文档记录，确认已按如下方式执行内部和外部漏洞扫描：	漏洞扫描是一个针对内外部网络设备和服务器运行的自动或手动工具组合，旨在暴露可能被恶意个人发现和利用的潜在漏洞。 PCI DSS 要求的漏洞扫描有三种： • 由合格工作人员执行的内部季度漏洞扫描（不要求使用 PCI SSC 认证的授权扫描服务商（ASV）） • 外部季度漏洞扫描，必须由授权扫描服务商执行 • 重大变更后需要的内部和外部扫描 一旦识别这些漏洞，实体应予以修复，并重复扫描直至修复所有漏洞。 及时发现并解决漏洞可减少漏洞被利用以及系统组件或持卡人数据被破坏的可能性。

QSA 机构或者合规建设机构自评估时执行年度审核都需要查验来自 ASV 机构的四个季度通过的扫描结果，且该扫描结果需要有资质的 ASV 机构针对被审核机构的持卡人数据环境范围内的公网 IP 地址执行季度 ASV 扫描。

面向公共网络的系统应按照标准要求，针对已知的脆弱性执行定期的扫描。更多详细信息可参见：https://www.atsec.cn/it-security-services/pci/pci-services/pci-qsa/index.html

2 商户和服务提供商的分级和验证要求

根据支付产业对 PCI DSS 标准的推动要求，支付产业链上的每个角色都需要针对自己运维的支付环境进行安全的合规建设，并有责任和义务监督和管理有数据共享时或者有业务合作时机构的环境安全性以及合作伙伴的 PCI 合规状态。例如，国际卡品牌 VISA、万事达等会要求合作的发卡和收单机构达到 PCI 的合规要求；收单机构会要求接入支付环境的服务提供商或者商户同样达到 PCI 的合规要求。

基于支付产业链上的服务提供商和商户，国际卡组织为了更好的管理和提供服务，对这两个角色进行分级管理来平衡业务发展和合规建设的有效性。卡组织通过服务提供商或者商户的年交易量作为分级的主要标准，截至目前各卡品牌官方发布的商户分级信息如下：

	American Express	**Discover**	**JCB**	**Mastercard**	**Visa, Inc.**
Level 1	> 2.5 Mio	> 6 Mio	> 1 Mio	> 6 Mio	> 6 Mio
Level 2	50 K – 2.5 Mio	1 – 6 Mio	all other	1 – 6 Mio	1 – 6 Mio
Level 3	all other	all other	not used	20 K – 1 Mio	20 K – 1 Mio
Level 4	not used	not used	not used	all other	all other

VISA、Mastercard 把商户分为 4 个级别；American Expree 和 Discover 把商户分为 3 个级别；而 JCB 仅把商户分为 2 个级别。而针对服务提供商这个角色，American Express 和 JCB 是不分级的，其他三个卡品牌更是针对年交易量达到 30 万笔的服务提供商定义为一级服务提供商。

	American Ex-press	**Discover**	**JCB**	**Mastercard**	**Visa**
Level 1	all[A]	> 300 K	all[A]	all TPPs, DSE > 300 K	> 300 K
Level 2		all other		all other	all other

针对不同级别的商户或者服务提供商，PCI DSS 提出了不同的验证要求，具体要求参见下表：

Merchants

	Level 1	Level 2	Levels 3 and 4
Type of Assessment:	Onsite Assessment	Self Assessment	Determined by payment brand or acquirer
Reporting Requirements:	ROC and ASV scan report	SAQ and ASV scan report	Determined by payment brand or acquirer

Service Providers

	Level 1	Level 2	Level 3 (American Express)
Type of Assessment:	Onsite Assessment	Self assessment	Self Asessement
Reporting Requirements:	ROC and ASV scan report	SAQ and ASV scan report	SAQ and ASV scan report

就以上提及不同级别的商户和服务提供商，按照产业要求当涉及卡数据的传输、存储以及处理时则需要合规 PCI DSS 标准。PCI DSS 的验证要求分为 QSA（Qualified Security Assessor）和 SAQ（Self-Assessment Questionnaires）两种。而无论验证要求是哪一种，商户和服务提供商在技术标准的合规建设中都需要统一遵从现行的 PCI DSS 标准版本。

3 PCI DSS QSA 和 SAQ

如上文提及 PCI DSS 的验证要求分为 QSA 和 SAQ 两种。QSA 是由 PCI 安全标准委员会授权的 QSA 机构执行，SAQ 顾名思义是机构可以执行自评估（非第三方验证）。接下来我们就一起了解下这两种验证要求的执行方法。

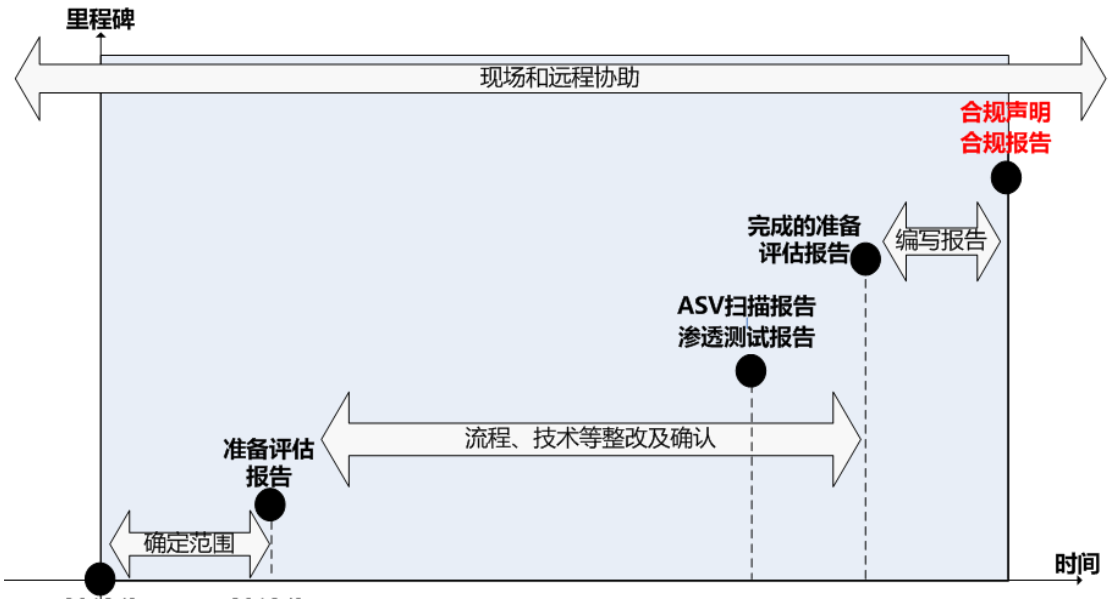
3.1 PCI DSS QSA 和 SAQ 的定义和区别

PCI DSS 支付卡产业数据安全标准是一个被开发支持和提高持卡人数据安全和卡组织采用的全球化一致性的数据安全措施，提供了一套保护持卡人数据的技术和操作的基线要求。无论是高级别还是低级别的商户或者服务提供商都需要根据 PCI DSS 标准要求进行合规建设。

3.2 PCI DSS QSA

PCI DSS QSA 涉及有资质的独立第三方对商户或者服务提供商的持卡人数据环境执行中立的评估和测试，并发布第三方的合规报告 ROC（Report on Compliance）和合规证明 AOC（Attestation of Compliance）。

atsec 作为被授权的 QSA 机构，有能力对被定义为一级商户或者一级服务提供商的机构执行年度 QSA 审核。atsec 执行 QSA 合规审核工作的阶段工作示意图参见如下：



PCI DSS QSA工作完成后，合规结果需要提交给合作的收单机构或者卡品牌，提交的内容由以下组成：

- PCI DSS合规报告ROC
- PCI DSS合规证明AOC
- ASV扫描报告

3.3 PCI DSS SAQ

3.3.1 确定 SAQ 的类型

所有商户和服务提供商必须始终遵守适用于其环境的PCI DSS。PCI DSS自我评估问卷（SAQ）是一种验证工具，旨在帮助商户和服务提供商自我评估他们是否符合PCI DSS。PCI DSS SAQ有多个版本可满足各种情况。指南（Instructions and Guidelines）可以帮助您的机构确定哪种SAQ最适合您的环境。执行自评估的商户和服务提供商也被要求提交PCI DSS合规报告（ROC），SAQ既是所需的验证工具。有关PCI DSS验证要求的详细信息，商户和服务提供商都需要咨询收单机构或支付品牌以确定验证要求。

不同的SAQ类型简要的显示在下表中，更详细的描述可参见指南（Instructions and Guidelines）。商户和服务提供商需要根据下表中的描述来初步判断哪个SAQ适用于您的环境，然后查看详细描述以确保满足该SAQ的所有要求。

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of cardholder data on merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: ▪ Imprint machines with no electronic cardholder data storage, and/or ▪ Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed Point-to-Point Encryption (P2PE) solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete an SAQ.

如上表所示，SAQ共分为SAQ-A、SAQ-A-EP、SAQ-B、SAQ-B-IP、SAQ-C-VT、SAQ-C、

SAQ-P2PE、SAQ-D八类，其中SAQ-D为商户和服务提供商分为不同的模板。商户和服务提供商需要根据描述选择适用于自身的问卷模板，如果适用于机构环境的PCI DSS要求没有包含在给定的SAQ中，则可能表明这个SAQ不适合您的环境。

3.3.2 执行 PCI DSS SAQ

PCI DSS SAQ 由商户或者服务提供商自评估，并针对评估后的问卷由该机构负责人签发即可，不强制由有资质的第三方 QSA 公司验证并签字。目前产业内也有商户和服务提供商为了准确地理解 PCI DSS 标准要求，以及充分的识别自身持卡人数据环境的差距或者正确填写 SAQ 问卷，而选择联系有资质的 QSA 机构提供咨询服务并邀请 QSA 机构协助评估在 SAQ 问卷上签字。SAQ 工作会由商户或者服务提供商自行签发 SAQ 问卷和合规证明 AOC。

被卡组织定义并要求执行SAQ的低级别商户或者服务提供商，可以进行SAQ自评估和ASV扫描工作。SAQ自评估是指由商户或者服务提供商自己依照PCI DSS标准进行评估，并根据指南（Instructions and Guidelines）完成适用性问卷的填写。

https://www.pcisecuritystandards.org/documents/SAQ-InstrGuidelines-v3_2_1.pdf?agreement=true&time=1564724644874

PCI DSS SAQ工作完成后，合规结果需要提交给合作的收单机构或者卡品牌，提交的内容由以下组成：

- SAQ问卷
- SAQ的合规证明AOC
- ASV扫描报告

当然，不论QSA还是SAQ评估符合PCI DSS，机构都必须遵守所有适用的PCI DSS标准要求。为了更好的保护支付卡数据且改进数据安全，我们更加鼓励商户或者服务提供商执行独立的QSA评估，协助完善信息安全并进行第三方的验证。

欢迎联系atsec咨询PCI DSS QSA和SAQ服务：

https://www.atsec.cn/it-security-services/pci/index.html

4 资源

[1] Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures

[2]Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire Instructions and Guidelines

[3] Understanding the SAQs for PCI DSS

[4] https://www.pcisecuritystandards.org/document_library

[5] https://www.atsec.cn/it-security-services/pci/pci-services/pci-qsa/index.html