atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

众人拾柴火焰高，共筑支付安全

2012-02-05

作者：atsec，白海蔚

PCI DSS 背景和现状

自 2006 年美国运通（American Express）、美国发现金融服务（Discover Financial Services）、JCB、万事达（MasterCard Worldwide）和 Visa 国际组织五家支付品牌共同筹办设立统一且专业的支付卡产业安全标准委员会（PCI SSC: Payment card industry Security Standards Council）以来，整个支付产业链上的不同机构(发卡机构、商户、收单机构、服务提供商等)给予数据安全保护很大的重视。以我国为例，越来越多的网络商户和第三方支付服务提供商完成了 PCI DSS 数据安全标准的合规认证，且越来越多的银行开始致力于 PCI DSS 标准的合规建设。在 Visa、万事达等卡组织以及多方的努力和大力推动下，通过 PCI DSS 数据安全标准的合规认证来进行数据保护，对保护持卡人利益的重要性方面有了更高的提升。

截至目前，国内已完成 PCI DSS 数据安全标准合规建设的机构包括但不限于：快钱（99bill）、易宝支付（Yeepay）、Oncard Payments、首信易（PayEase）、盛付通、票务在线、安利（中国）等等。此外，诸多大型商业银行也已经启动并完成了 PCI DSS 的部分合规建设工作。

与此同时，atsec 作为 PCI 授权认可的第三方安全审核机构 QSA 和脆弱性扫描服务商 ASV，为了给中国的客户提供更加便捷且专业的服务。于 2011 年 8 月，atsec 中国在已往 atsec 全球品牌拥有 PCI QSA 和 ASV 资质的基础上，进一步以单独的实体正式向 PCI 安全标准委员会递交 QSA 和 ASV 资质申请，由此成为中国首家也是唯一一家在 PCI 安全标准委员会授权列表中的本土企业。在申请资质的过程中，标委会全面审核确认 atsec 中国的管理体系及审核方法论，严格考核团队每一位审核人员的信息安全经验和专业知识，评估提交的报告等证明。经过不同层面的审批，atsec 中国团队获得 PCI 安全标准委员会的进一步认可，并称赞 atsec 中国高效、严谨的工作风格，相信这是一个新的里程碑，将为我们中国的客户在执行 PCI DSS 合规建设的项目中提升更多的信心。atsec 中国团队将一如继往的为支付产业链信息安全工作做出贡献！PCI DSS 授权资质链接如下：
https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

为支付安全添砖加瓦

俗话说众人拾柴火焰高，正如支付产业链上环环相扣的数据保护一样。从数年前支付网关类公司最先执行 PCI DSS 标准合规，到陆续大型商户、收单银行等不同角色致力于标准的合规建设工作，PCI DSS 数据安全标准从交易流程着手，搭建并确定合理、有效的持卡人数据环境，从每个环节执行严谨和高安全性的保护措施，使得整个支付产业链安全、稳定地发展。

正如民生银行信用卡中心高海涛先生所述：
“随着网络经济和电子商务的兴起，网上消费已经成为了一种时尚和潮流。但是这种便捷的消费模式背后，却蕴藏着很大的交易风险和安全隐患。在整个支付卡产业链条中，无论是收单商户还是发卡银行，任何一个环节处理不好，轻则泄露客户隐私，重则影响客户的资金安全。近年来，

随着第三方支付和其他一些新兴支付手段的出现，更是将这种风险快速放大。在这种背景下，如何保障持卡人的数据安全，就显得尤为重要。

持卡人的数据安全需要支付卡行业各参与方的整体提升，这就要求每个支付卡行业的参与主体，包括发卡银行、收单机构以及商户的共同努力。那么如何才能快速提升整个行业的信息安全管理水平，我觉得提高技术准入标准就是一个很好的抓手，由于国内的支付卡行业起步较晚，这方面的技术标准和规范还十分欠缺，而国外的支付卡行业已经经历了几十年的发展，积累了大量的经验和最佳实践，借鉴国外成熟的做法和经验无疑是推动整个行业快速成长的一条捷径。

PCI-DSS 是 VISA、MasterCard 等国际卡组织参与制订的专门针对支付卡行业数据安全的技术标准，该标准适用于支付卡产业链条中的所有参与主体，包括发卡机构、收单机构以及商户，国内外大量的实践证明，通过实施 PCI-DSS 合规项目，可以有效提升企业的信息安全管理水平，增强客户的信任度和品牌影响力。

民生银行信用卡中心历来十分重视持卡人的信息安全保护，目前我中心正在以收单系统为试点实施 PCI-DSS 合规项目，在 atsec 咨询团队的帮助下，项目正在有序推进。通过实施该项目，我中心人员的安全意识得到了明显的提升，技术措施和管理手段也得到了进一步的完善。该项目实施完成后，我们有信心为民生银行的信用卡持卡人提供一个更加安全的用卡环境，同时也借此机会，向 atsec 的民生服务团队表示感谢，在项目实施过程中，你们表现出了强烈的服务意识，严谨的工作态度和专业的技术素养。谢谢你们为民生银行信用卡中心信息安全工作做出的努力和贡献！”

atsec 作为 PCI 安全标准委员会授权认可的第三方审核机构，倡议支付产业链上的不同角色加入到标准委员会的参与机构当中，将自身企业在采用 PCI DSS 标准进行合规建设的经验和心得共同分享。参与机构包括协会组织或商业机构、金融机构、各类商户、POS 厂商、支付处理机构和其他机构。截至目前，已有参与机构达 640 家，可在如下列表查看：
https://www.pcisecuritystandards.org/get_involved/member_list.php

在以往的审核中，atsec 与支付产业链上不同角色机构合作执行 PCI DSS 的合规建设。针对已经完成 PCI DSS 合规建设并持续合规的机构，直接参与合规建设的项目管理者或者执行者也纷纷提出了他们的感言：

- “安全、信赖是电子支付日渐走入大众生活的根本，同样支付服务方也应以资金安全、信息安全为提供服务的根本和基础。快钱率先通过 PCI DSS 最新版本的审核认证是权威组织对于快钱的肯定，同时也宣告快钱拥有国际领先的安全支付系统及信息安全解决方案。”另外，关国光表示，“支付企业积极参与 PCI 认证审核也有助于中国的支付行业更规范、专业。”——快钱 CEO 关国光

- “‘安全、可靠’是电子支付平台能够持续健康发展的基础，易宝支付早在 2007 年 3 月，就率先作为独立支付公司通过了国家信息安全测评中心的安全认证，此次再顺利通过 PCI DSS 合规性评估，意味着易宝支付的交易平台整体安全水平、风险控制体系已达到了一个新的高度。”——易宝支付 CEO 唐彬

- “BilltoBill 作为在中国领先的信用卡支付公司，在风险控制，防伪反欺诈以及系统的数据安全方面有着优良的记录。这次选择 atsec 是因为他们的资质，良好的反应速度以及专业的项目管理；通过本次 PCI 认证的合作，能够更好的增强 BilltoBill 支付系统的安全性，保护持卡人的数据安全。”——原 BilltoBill CEO 雷扬

- “作为电子商务行业，大麦网始终坚持确保客户机密信息的安全和完整，此次与 atsec 团队携手，采用国际安全标准，完善并巩固了大麦网的安全架构和内部风险控制系统。我们感谢 atsec 的努力，期待进一步的合作。”——大麦网董事长曹杰

- “PCI DSS 作为全球最严格的数据安全标准，我们能够顺利通过该认证，说明盛付通支付系统的安全性方面已经达到了国际要求，这也意味着用户在享受盛付通服务的时候，拥有了国际水准的安全保证。” ——盛付通的首席执行官王静颖

- “PCI DSS 的标准要求既具体又严格，尽管安利中国早已在信息安全领域通过了 ISO/IEC 27001 认证，但针对此次的台湾 POS 系统的 PCI DSS 合规建设项目，整个项目组仍然遇到不少技术层面的挑战。在项目过程中，atsec 顾问不仅认真细致地完成了差距分析和最终评估等各项工作，更难能可贵的是，他们凭借着在 PCI 领域的专业知识和丰富经验，为我们提供了很多有价值的意见和建议，使所有的技术难关得以攻克，并最终顺利实现 PCI DSS 合规。此次 PCI DSS 合规的实现，标志着安利中国为台湾 POS 系统的支付卡信息安全保护达到了国际标准的要求，意义重大。我们非常感谢 atsec 的指导和帮助，并期待与之进一步的合作。”——安利中国项目经理沈国华

- PCI DSS 可以帮助我们证明公司对于持卡人信息的相关安全保障满足行业性的安全标准要求，从而加强客户对于我们确保客户相关信息处理过程中的信息安全信心。——快钱刘锦祥

- 安全、信赖、可靠是电子支付平台能够持续健康发展的基础，盛付通此次顺利通过 PCI DSS 合规性评估，意味着盛付通的交易平台整体安全水平、风险控制体系已达到了一个新的高度。在此过程中，atsec 对盛付通进行外部渗透测试，以确定是否存在可能成为恶意攻击入口点的网络漏洞以及可被利用的安全性缺陷，并为盛付通提供了专业的工具和技术支持，以帮助我们更好地确保在支付处理环节中信用卡数据等机密信息的安全。——盛付通叶飞

- PCI DSS 合规评估对于支付公司来说，不管是监管要求、合作门槛，还是用户对品牌的安全体验，都具有重要意义。我司在五个月内能完成 PCI DSS 合规评估，和 atsec 团队高效、务实的工作是分不开的。项目中，我们也都感受到其认真、细致、严谨的工作态度和熟练扎实的专业技能。非常感谢 atsec 团队为我们安全体系建设做出的贡献，期待与 atsec 安全专家的再次合作！——盛付通杜磊

- 众所周知 PCI DSS 认证过程异常严格且复杂，必须通过自我安全检查、漏洞分析以及由协会执行的安全调查这三个步骤，审查范围包括了硬件、软件、工作流程、员工、用户等诸多内容，总共有 200 多项审查项目。在盛付通 PCI DSS 认证过程中，很好的体会到了 atsec 团队中咨询师自身扎实的专业技能，严谨认真的工作态度。在评估后期，由于项目时间紧，且接连出现了多个未预料的问题，atsec 的高向东先生在连续加班工作近 1 个月后，出现头痛发烧，仅是休息了一个下午，第二天又继续加班工作，我们能够顺利在计划内通过 PCI DSS 认证，高向东先生功不可没啊。感谢高向东先生，他在负责 PCI DSS 认证的相关制度文档审核工作，他是一个非常专业且严谨细心的人，帮我们标出了文档中不恰当的地方，并且给出了详细的修改意见，减少了我们文档的修改次数。——盛付通黄永飞

- 只有支付产业链上每一个角色包括银行、第三方支付公司以及所有的商户都做到数据安全的合规建设，让每一个环节都提高信息安全的意识，才能保障整个支付产业链的数据安全。工商银行作为世界 500 强企业，一直以来注重信息安全的保护，不论在技术手段还是管理流程上都力求做到最好。PCI DSS 合规建设项目目前正在紧锣密鼓的开展中。项目实施过程中，随着对 PCI DSS 标准的理解更加深入，让我们体会到该标准的全面性和严谨性，以及对技术的高要求。我们有信心在依照 PCI DSS 标准进行合规建设后我们的持卡人数据环境将更加健壮，将使得工商银行为客户提供更优质且有保障的服务。atsec 团队与我们并肩作战，紧密配合我们按照预期计划顺利的开展各项工作。我们感谢 atsec 给予我们的高度配合，期待我们的 PCI 认证项目圆满完成！——工商银行 黄汉波

不难看出，不论是已经完成了 PCI DSS 标准合规，还是正在致力于合规建设，获得 PCI DSS 合规认证的成功都需要各方的重视和大力的配合，而该合规的结果让企业自身具备了更完善、规范的管理体系，拥有了相对健康、安全的网络环境，而对于持卡人来说享受安全、便捷的交易方式无疑提升了对公司的知名度和信任度的认可。在全民进入卡生活时代的今天，保护持卡人的信息，筑建支付产业链的安全需要我们大家共同的努力！

关于 atsec 信息安全

艾特赛克信息安全（atsec information security）是一家独立且基于标准的信息技术（IT：Information Technology）安全服务公司（www.atsec.com），它很好地将商业导向的信息安全方法和深入的技术知识以及全球的经验相结合。atsec 在德国慕尼黑成立于2000 年，并且通过美国、德国、瑞典和中国的办公室开展了广泛的国际业务。atsec 提供的服务包括正式的实验室测试和评估、独立的测试和评估以及信息安全咨询。

atsec 提供美国国家标准与技术研究委员会（NIST：National Institute of Standards and Technology）和加拿大通讯安全协会（CSEC：Communications Security Establishment Canada）制定的密码模块验证体系下的密码模块和算法测试服务。atsec 同时提供NIST 个人身份验证体系（NPIVP）、密码算法测试（CAVP：Cryptographic Algorithm Validation Program）和安全内容自动化协议（SCAP：Security Content Automation Protocol Program）下的正式的测试，以及GSA FIPS 201 EP 下的产品认可测试。

atsec 同时提供PCI SSC 体系下的服务，并且是一家能够提供PCI DSS 和PA-DSS 标准的评估服务的QSA 公司。atsec 的渗透测试、应用安全、ASV（Approved Scanning Vendor）服务和信息安全咨询服务，作为评估服务工作的有力支撑。atsec 是授权的NASPO（North American Security Products Organization）第三方审计机构。

atsec 的客户包括全球首屈一指的公司如苹果、IBM、Hewlett and Packard、Samsung、Quantum Corporation、Red Hat、国民技术、握奇数据、华为和中兴通讯等，并一直维持密切合作关系。