



## 固安全之本，应支付之变

### - 2025年支付卡产业动态和趋势分享

2026 年 1 月，中国 北京

atsec 白海蔚

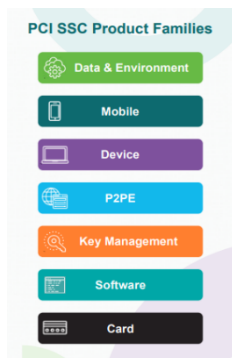
#### 引言

在过去的 2025 年度，atsec 作为支付卡产业（PCI: Payment Card Industry）产业全球执行评估机构圆桌会议（GEAR: Global Executive Assessor Roundtable）的工作成员之一，一如既往地关注着支付产业发展，积极参与产业交流和会议，为标准化发展提出我们的见解，分享我们在实际评估项目中的诸多经验。

本文参考了支付卡产业安全标准委员会（PCI SSC: Security Standard Council）发布的年度报告，结合 atsec 的参与和理解进一步分享相关的产业动态和未来趋势。我们有感于整个支付产业的信息安全标准化工作使得整个支付安全的标准化及其相关体系均在有条不紊的发展，一方面需要应对飞速发展的技术和支付模式的演进，另一方面信息安全标准所依赖的底层技术和架构根基非常的稳步且坚实。

PCI SSC 与产业协同工作，为了增强支付行业的支付安全做出了努力和贡献，也对支付产业的未来发展趋势产生了深厚的影响。指数级增长的交易数量使得数据安全风险大大提升，伴随支付形态和 IT 技术发展，PCI SSC 也在与时俱进的做出变化。人工智能成为 2025 年的一个关键焦点领域，PCI SSC 发布了关于 PCI 评估中人工智能的指导以及在支付环境中开发和部署人工智能系统时的高级原则。2026 年是 PCI SSC 成立 20 周年，atsec 作为第一批经过授权的安全评估机构也已伴随 SSC 走过 20 年，我们的共同目标始终没有变化，通过协作、创新和警惕来保护全球支付生态系统。

#### PCI 标准家族的总体发展趋势



如左图所示，PCI SSC 推出了七大产品（标准）系列，涵盖 PCI 产业现行全部 15 项标准，有力支撑前瞻性标准战略。七个前瞻性领域包括：数据和环境、移动、设备、P2PE、密钥管理、软件，以及卡。

这些产品（标准化文档）系列不仅关注标准本身，还包括 PCI SSC 所推出的辅助产品，旨在推动标准落地实施。此类辅助产品涵盖体系指南、经验证的产品与解决方案列表体系、支持性模板，以及培训资料等内容，目标是协调发布计划，确保所有产品（各类文档）同步推出，从而为产业内相关机构创造更高价值。

PCI SSC 整合和调整其标准分布，以确保一致性，减少标准间的重复。最重要的是，调整后的分布方法更加满足支付安全的未来需求。

#### 标准及其体系演进与优先级目标

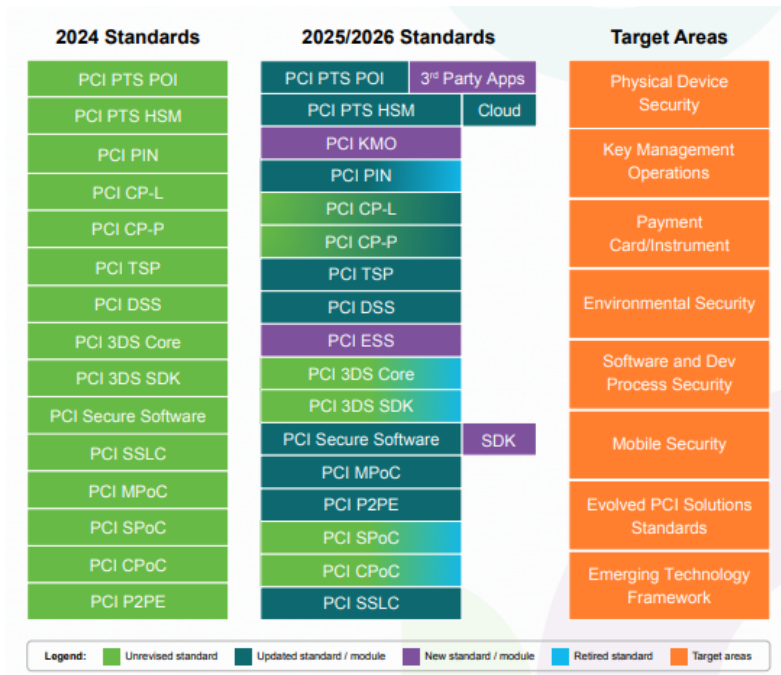
Product Components		Data & Environment	Mobile	Software	Card	Key Management	P2PE	Device
Standards	2024	• DSS • 3DS Core • PCI TSP	• MPoC • CPoC • SPoC	• PCI Secure Software • PCI Secure SLC • 3DS SDK	• PCI CP-L • PCI CP-P	• PCI PIN	• P2PE	• PCI HSM • PTS POI
	In Process	• DSS, ESS • 3DS Core • PCI TSP	• MPoC	• PCI Secure Software • PCI Secure SLC	• PCI CP-L • PCI CP-P	• PCI KMO	• P2PE	• PCI PTS HSM + Cloud • PCI POI+ 3rd Party Apps
	Target Areas	Environmental Security	Mobile Security	Software & Dev Process Security	Payment/Card Instrument	Key Mgmt. Operations	Payment Solution Security	Physical Device Security
Programs	Training	• QSA • AQSA (Jr QSA) • ISA • ASV • QIR • Acquirer • 3DS Core	Lab specific training	• SS Assessor Training • SS SLC Training • Knowledge Training	• Knowledge Training • CPSA (Card Production Security Assessor)	• Knowledge Training • QPA (Qualified PIN Assessor)	• P2PE Training • Knowledge Training	Lab specific training
	Listings (Assessors / Labs)	ASV Listing	• MPoC Lab • SPoC Lab • CPoC Lab • xPoc Solutions	• SSLC Vendors • Payment SW • 3DS SDK (Lab) • 3DS SDK (App)	None	• PCI PIN Service Provider • PCI KMO Listings TBD • PCI PIN	• P2PE Assessor • Application, Solutions, Components	• PTS Device • PTS Lab
	Company Qualification	QSA / ISA / 3DS Core	• Lab • Report submission • Listing	• Secure Software Company	• CPSA Company	• QPA company • KMO TBD	• P2PE Assessor & Application Assessor Company	• Lab • Report submission • PTS listing
	Individual Assessors	• QSA / AQSA / ISA • 3DS Core • ASV	None	• Secure Software • Secure SLC Assessor Employee	CPSA-PIL	• QPA assessor • KMO TBD	• P2PE Assessor • P2PE Application Assessor	None

如上图所示，不同的标准领域具有不同的推进计划和优先级目标，上图宏观的展示了过去两年标准的演进和发展状态。同时也从宏观层面提出了路线图，展示了未来如何巩固和重新调整标准。



## 具体标准的未来更新与淘汰计划

下图展示的目标领域（Target Areas）反映了产业预期标准将作为未来安全框架的一部分而演进的领域。这些目标领域直接与 PCI SSC 的产品系列保持一致，并为支付卡行业的标准未来演进提供了指引。



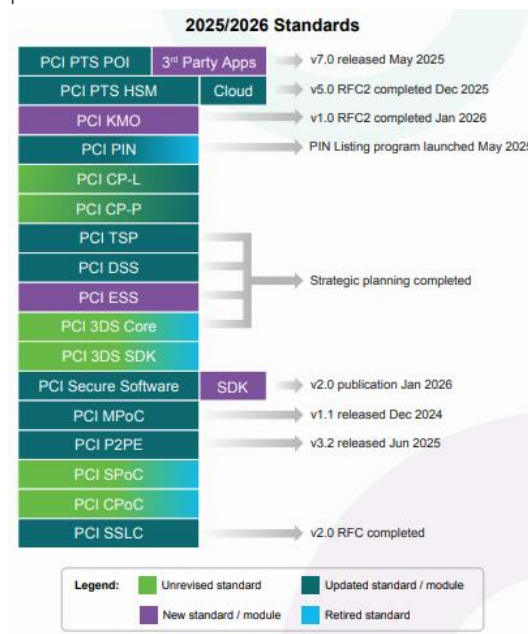
下图的路线图也展示了一系列未来的修订、新的标准和模块，以及一些现有标准的淘汰，以支持支付行业的持续演进。

新标准和模块包括但不限于：

- 制定新的密钥管理操作（KMO: Key Management Operations）标准
- 评估新的环境安全标准（ESS: Environmental Security Standard）
- 在 PTS POI 中添加了第三方应用程序模块
- 将 SDK 模块添加到安全软件标准中

随着整合和调整，一些标准可能会退役，包括：

- 计划将 PCI PIN 集成到 KMO 中
- 3DS SDK 正在集成到安全软件中
- SPoC/CPoC 集成到 MPoC（Mobile Payments on COTS）中
- 3DS Core 集成到 DSS 中





## 成果总结与展望

在 PCI SSC 发布的《2025 年度报告》中，也给出了下图所示的年度交付成果：

2025 Product Family Delivery Outcomes							
PCI SSC had a very productive year providing value to our stakeholder community. We planned holistically and paced our standards delivery based upon need and industry feedback. The product family operating model, combined with new collaboration tools, generated a record number of stakeholder touchpoints that contributed to PCI SSC delivery outcomes.							
5+	RFCs Conducted	Key Management	Device	P2PE	Software	Mobile	Data & Environment
2+	Standard Publications	Request for Comment (RFC)			Guidance Docs		
8	Guidance Documents	✓ KMO v1.0 (#1) • KMO v1.0 (#2)	✓ HSM v5.0 (#2)	✓ P2PE v3.2 (#1)	✓ Secure Software v2 ✓ Secure SLC v2	✓ PCI MPoC Guidance	✓ E-Commerce ✓ SAQ Instructions & Guidance ✓ Vulnerability Mgmt.
1	New Listing Program	New Listing Program ✓ PIN Listing	Standards Publication ✓ PTS POI v7	Standards Publication ✓ P2PE v3.2	• Secure Software v2		
3+	Program Guides	Program Guide			• Secure Software v2	✓ MPoC v1.1	SAQ Revision ✓ SAQ A
1	SAQ Revisions	✓ QPA Program Guide	✓ PTS Program Guide				
98+	FAQs	FAQs					
20+	Supporting Documents	Tech FAQ ✓ PCI PIN-2	Tech FAQ ✓ PTS HSM-2 ✓ PTS POI-16	Tech FAQ ✓ P2PE-6	Tech FAQ ✓ Secure Software-2 ✓ Secure SLC-0	Tech FAQ ✓ MPoC-11 ✓ CPOC-1 ✓ SPoC-1	FAQ ✓ New: 11 ✓ Updated: 25 ✓ Retired: 19
4+	New Trainings	Supporting Documents					
		✓ QPA Qualification Requirements	✓ PTS Lab Report Template	✓ P-ROV Updates	• PCI 3DS Data Matrix • SecSW Sensitive Asset Identification • AOV Template • ROV Template	✓ MPoC v1.1 Integration Report ✓ MPoC AOV Updates	✓ PCI DSS Quick Reference Guide ✓ Prioritized Approach Tool ✓ Prioritized Approach for PCI DSS
		New Training					
		• PTS POI Test Artifacts	✓ Re-qual Training ✓ Transition Training	• New Assessor Training	✓ MPoC Lab Training ✓ MPoC Lab Test Artifacts		✓ CP-Logical and Physical Security Reqs AOC Updates
		CROSS-PRODUCT FAMILY GUIDANCE: ✓ AI Principles ✓ Cryptography ✓ Authentication (+ Infographic) ✓ AI in PCI Assessments					

可以看到，无论是从各个标准系列的反馈投入、新标准以及相关指导文档的发布，还是体系性的优化，整个支付产业都呈现了非常良好和积极的趋势。

PCI SSC《2025 年度报告》记录了一段在全球支付行业以进步、协作与影响力为主题的发展历程。从优化标准与项目交付方式，到深化利益相关方协作，扩大全球代表性，再到应对人工智能等新兴技术挑战，展现了 PCI SSC 如何持续推进我们保护支付生态系统的共同使命。

atsec 在 2025 刚刚度过了全球品牌的 25 周年庆祝，实现了产业内诸多的里程碑性的项目成果，协助全球范围内诸多的机构实现了 PCI 的合规；2026 年 atsec 将继续投入到诸多的信息安全审核，将安全合规更好的服务于被评估机构的业务拓展，atsec 也将持续的投入标准化工作中，为产业发展做出我们的微薄之力。

atsec 将与支付产业共同庆祝 PCI SSC 成立 20 周年的历史性时刻。atsec 作为连续多年的 GEAR 全球圆桌会议成员愿携手产业各方同仁，与 PCI SSC 一起见证 2025 年取得的成果，指导、建议和持续合作共同打开支付产业数据安全的新篇章。

参考资料：

[1] PCI SSC 2025 年度报告

[2] [www.atsec.com](http://www.atsec.com)