支付卡行业 (PCI)

支付应用程序数据安全标准

PA-DSS 3.1 版到 3.2 版的变更汇总

2016 年 5 月

简介

本文档为 PA-DSS 3.1 版到 PA-DSS 3.2 版的变更汇总。表 1 是对变更类型的概要。表 2 是对 PA-DSS 3.2 版中重大变更的汇总。

表 1：变更类型

[1]变更类型	定义
说明性	说明要求的目的。确保该《标准》中简洁的措辞传达出要求的预期目的。
其他指南	解释、定义和/或说明，用以加深理解，或就某一特定主题提供更多信息或指南。
不断进化的要求	相关变更用以确保该《标准》与市场中出现的新威胁和各种变化保持同步。

表 2：变更汇总

章节		变更描述	类型 [1]
PA-DSS 3.1 版	**PA-DSS 3.2 版**		
全部	全部	解决了细微印刷错误（语法、标点、格式等），并兼并了小版本更新以提升文件的易读性。	说明性
要求			
综述	综述	删除了许多要求中的“强大”或“安全”协议示例，因为这些内容可能会随时发生变更。	说明性
综述	综述	将示例从许多要求和/或测试程序移至指南栏，并在适当情况下添加了指南。	说明性
2.2	2.2	更新了要求，以阐明仅有正当业务需要者才能看到除前六位/后四位以外的 PAN。添加了常见掩盖情况相关指南。	不断进化的要求
2.3.a	2.3.a	更新了*《PA-DSS 实施指南》*的测试程序，以包括以下说明：如果已启用除错日志（例如，为了进行故障排除而启用），且该除错日志包含 PAN，则须根据 PCI DSS 保护日志、在完成故障排除后尽快禁用日志，并在不再需要使用时安全删除日志。	不断进化的要求
3.1.a	3.1.a	更新了*《PA-DSS 实施指南》*的测试程序，以包括通过管理访问识别应用程序中的所有角色和默认帐户。	
5.1.7	5.1.7	阐明开发人员培训须及时更新，并至少每年开展一次。	说明性
	7.2.3	添加了*《PA-DSS 实施指南》*要求，以包括安全安装补丁和更新的相关说明。	不断进化的要求
8.3	8.3	阐明正确术语为“多因素验证”，而非双因素验证，因为可以使用两个或两个以上因素。	说明性
10.1	10.1	阐明正确术语为“多因素验证”，而非双因素验证，因为可以使用两个或两个以上因素。	说明性

章节		变更描述	类型 [1]
PA-DSS 3.1 版	PA-DSS 3.2 版		
要求 12	要求 12	将要求标题更改为“保护所有非控制台管理访问”，以更好地体现此要求的内容。	说明性
12.2	12.1.1	进行了重新编号，以作为要求 12.1 的子要求。	说明性
	12.2	新要求针对适用于可对应用程序进行非控制台管理访问的所有工作人员的多因素验证。 *符合 PCI DSS 要求 8.3.1。*	不断进化的要求
附录 A：《PA-DSS 实施指南》的内容概要	附录 A：《PA-DSS 实施指南》的内容概要	更新以反映要求部分的变更情况（如适用）。	说明性