支付卡行业（PCI）

支付应用程序数据安全标准

PA-DSS 3.0 版到 3.1 版的变更汇总

2015 年 6 月

简介

本文档为 PA-DSS 3.0 版到 PA-DSS 3.1 版的变更汇总。表 1 是对变更类型的概要。表 2 是对 PA-DSS 3.1 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 3.0 版	PA-DSS 3.1 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
全部	全部	在提及使用支付应用程序的实体时，将引用从“商户”更改为“客户”。	说明性
PCI DSS 适用性信息	PCI DSS 适用性信息	将引用从“金融机构”变更至“收购方、发行方”。澄清 PCI DSS 适用于任何存储、处理或传输帐户数据的实体。	说明性
2.3	2.3	在要求“注释”中澄清如果同一个 PAN 的散列或删节版本均由支付应用程序生成，则需要其他控制措施。添加了测试程序 2.3.c 以验证注释，并为后面的测试程序重新编号。	说明性
2.4	2.4	更新了指南内容以说明密钥加密密钥无需加密。但是，必须根据要求 2.4 的内容为其提供保护。	其他指南
2.5	2.5	将测试程序中的“加密术”更改为“密码术”以符合要求。	说明性
3.1.a	3.1.a	更新了测试程序，以说明《*PA-DSS 实施指南*》中的指导包括将安全验证分配给环境中所有默认帐户，此外应禁用或不使用任何未使用的默认帐户。	说明性
3.1.7	3.1.7	澄清必须至少每 90 天更改*一次*密码。	说明性
5.1.d	5.1.d	更新了测试程序以符合要求。	说明性

5.3.3.a 5.4.1.c	5.3.3.a 5.4.1.c	为保持一致性，更新了测试程序中的语言。	说明性
5.4.3.a	5.4.3.a	整合测试程序中的项目以去除冗余	说明性
5.4.5.b	5.4.5.b	更新了测试程序以符合要求。	说明性
6.3	6.3	从测试程序中删除冗余的语言。	说明性
8.2	8.2	将 SSL 从安全技术示例中删除。增加了一条注释，用以说明 SSL 和早期 TLS 不能视为强效密码术，支付应用程序不能使用或不能支持使用 SSL 或早期 TLS。也会影响要求 11.1 和 12.1 - 12.2。	不断进化的要求
8.3	8.3	对内容进行更新以与 PCI DSS 保持一致。	说明性
10.2.2	10.2.2	说明必须为每一位客户使用唯一验证凭证。	说明性
11.1	11.1	将 SSL 从安全技术示例中删除，并且添加了一项该要求的注释。参见以上 8.2 节的说明。	不断进化的要求
12.1 - 12.2	12.1 - 12.2	将 SSL 从安全技术示例中删除，并且添加了一项该要求的注释。参见以上 8.2 节的说明。	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