Atiitt 支付系统安全标准PCI DSS

目录

[1.1. PCI 数据安全标准 2](#_Toc13614)

[1.1.1. 6 个目标，12 项要求 2](#_Toc13050)

[1.1.2. 支付应用数据安全标准PA-DSS 2](#_Toc11713)

[1.1.3. 数据安全标准DSS 3](#_Toc3670)

[2. ADSS（银联卡收单机构账户信息安全管理标准） 3](#_Toc12680)

[2.1. 要内容 3](#_Toc4622)

全称Payment Card Industry (PCI) Data Security Standard,第三方支付行业(支付卡行业PCI DSS)数据安全标准，是由PCI安全标准委员会的创始成员(visa、mastercard、American Express、Discover Financial Services、JCB等)制定，立在使国际上采用一致的数据安全措施，简称PCI DSS。

PCI DSS对于所有涉及信用卡信息机构的安全方面作出标准的要求，其中包括安全管理、策略、过程、网络体系结构、软件设计的要求的列表等，全面保障交易安全。PCI DSS适用于所有涉及支付卡处理的实体，包括商户、处理机构、购买者、发行商和服务提供商及储存、处理或传输持卡人资料的所有其他实体。PCI DSS包括一组保护持卡人信息的基本要求，并可能增加额外的管控措施，以进一步降低风险

**保护持卡人信息**

3、保护存储的持卡人资料。

4、加密通过开放的公用网络传输的持卡人资料。

**维护漏洞管理程序**

5、使用并定期更新杀毒软件或程序。

6、开发并维护安全系统和应用程序。

**实施严格的存储控制措施**

7、限制为只有业务需要的人才能存取持卡人资料。

8、为具有电脑存取权的每个人指定唯一的ID。

9、限制对持卡人资料的实际存储。

**定期监控并测试网络**

10、追踪并监控对网络资源及持卡人资料的所有存取。

11、定期测试安全系统和程序。

**维护信息安全政策**

12、维护满足所有人员信息安全需求的政策。

## PCI 数据安全标准

PCI DSS 有超过 250 条子要求，总体分为 6 个目标和 12 项主要求。

### 6 个目标，12 项要求

|  |  |
| --- | --- |
| **目标** | **PCI DSS 要求** |
| 建立并维护安全网络 | 1：安装并维护防火墙配置，保护持卡人数据   2：不得将供应商提供的默认值作为系统密码和其他安全参数 |
| 保护持卡人数据 | 3：保护所储存的持卡人数据  4：对持卡人数据在公共开放网络之间的传输进行加密 |
| 维护漏洞管理程序 | 5：使用杀毒软件并定期更新  6： 建立并维护安全系统和应用 |
| 采取强大的访问控制措施 | 7：根据业务须知限制获取持卡人数据的权限  8：为每个有电脑访问权限的用户分配唯一的 ID  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 |
| 维护信息安全政策 | 12：维护信息安全政策 |

### 支付应用数据安全标准PA-DSS

软件开发者和支付应用整合者会对持卡人数据进行存储、处理，在向第三方出售、分销或提供特许应用时的结算和授权过程也会传输持卡人数据。支付应用数据安全标准（PA-DSS）正是针对以上情形而制定。

PA-DSS 要求第三方支付应用的供应商采取合适的安全控制措施，以保护持卡人数据。支付应用数据安全标准（PA-DSS）中有许多控制措施专门用于处理导致信用卡数据丢失的常见漏洞。

### 数据安全标准DSS

# ADSS（银联卡收单机构账户信息安全管理标准）

[编辑](https://baike.baidu.com/item/ADSS/javascript:;) [讨论](https://baike.baidu.com/planet/talk?lemmaId=13238077" \t "https://baike.baidu.com/item/ADSS/_blank)

本词条缺少****概述图****，补充相关内容使词条更完整，还能快速升级，赶紧来编辑吧！

全称Account Data Security Standard ，即银联卡收单机构账户信息安全管理标准，由中国银联风险管理委员会审核通过，旨在加强银联卡收单网络账户信息安全管理，进一步明确和细化对收单业务各参与方账户信息安全管理要求，防范账户信息泄漏风险，简称ADSS。

## 要内容

[编辑](https://baike.baidu.com/item/ADSS/javascript:;)

1、总则：标准目的、适用范围

2、基本要求：相关机构对于银行卡信息和持卡人资料的使用、存储的保护要求

3、政策制定：要求相关构按本标准建立账户信息安全管理体系

4、组织管理：要求相关机构设立相关岗位、明确岗位职责、细化人员管理

5、访问控制：对权限管理、身份验证、账户密码管理、系统登录控制、远程访问控制、无线和移动网络访问控制、用户配置文件管理、日志管理、物理访问控制的要求

6、账户信息生命周期安全管理：对账户信息加密、秘钥管理、账户信息的传输、使用、存储与备份，以及账户信息的销毁的要求

7、系统及网络安全管理：对网络及防火墙管理、设备安全管理、防病毒管理、系统补丁管理、系统安全检查、安全开发流程、变更管理、Web安全管理、安全配置管理的要求

8、银联卡受理终端及支付应用软件安全管理：对各类受理终端、支付应用软件及其插件的安全要求

万事达卡PCI数据安全标准（DSS）的合规性.html