

Q/CUP

中国银联股份有限公司企业标准

Q/CUP 007.2.1—2014

银联卡受理终端安全规范 第2卷：产品卷 第1部分：销售点（POS）终端

Security Specifications for Terminal Accepting UnionPay Card
Volume 2: Product Requirements
Part 1: Point of Sale Terminal

2014-11-30 发布

2014-12-01 实施

中国银联股份有限公司 发布

中国银联股份有限公司（以下简称“中国银联”）对该规范文档保留全部知识产权权利，包括但不限于版权、专利、商标、商业秘密等。任何人对该规范文档的任何使用都要受限于在中国银联成员机构服务平台（<http://member.unionpay.com/>）与中国银联签署的协议之规定。中国银联不对该规范文档的错误或疏漏以及由此导致的任何损失负任何责任。中国银联针对该规范文档放弃所有明示或暗示的保证,包括但不限于不侵犯第三方知识产权。

未经中国银联书面同意，您不得将该规范文档用于与中国银联合作事项之外的用途和目的。未经中国银联书面同意，不得下载、转发、公开或以其它任何形式向第三方提供该规范文档。如果您通过非法渠道获得该规范文档，请立即删除，并通过合法渠道向中国银联申请。

中国银联对该规范文档或与其相关的文档是否涉及第三方的知识产权（如加密算法可能在某些国家受专利保护）不做任何声明和担保，中国银联对于该规范文档的使用是否侵犯第三方权利不承担任何责任，包括但不限于对该规范文档的部分或全部使用。

目 次

前 言 III

1 范围 1

2 规范性引用文件 1

3 基础安全要求 1

4 传输安全要求 1

5 账户数据保护 1

6 终端管理和应用安全 2

7 辅助安全要求 2

中國銀聯
版權所有

前 言

本标准对受理银联卡（包括磁条卡和IC卡）终端的硬件和安全做具体规定。

本标准由以下部分组成：

——第1卷：基础卷

——第1部分：术语

——第2部分：设备安全

——第3部分：管理安全

——第4部分：硬件要求

——第2卷：产品卷

——第1部分：销售点（POS）终端

——第2部分：无人值守（自助）终端

——第3部分：个人支付终端

——第4部分：独立部件

——第5部分：电话终端

——第6部分：智能销售点终端

——第7部分：mPOS通用技术安全

——第3卷：检测卷

——第1部分：基础安全检测要求

——第2部分：产品分类安全检测要求

——第3部分：硬件技术检测要求

——第4卷：辅助卷

——第1部分：终端防切转网技术安全指南

——第2部分：航空机上支付技术安全指南

——第3部分：POS互联网接入系统部署方案

——第4部分：基于地理位置定位的终端非法移机监控技术方案

本部分为《银联卡受理终端安全规范》第2卷第1部分。

本部分由中国银联提出。

本部分由中国银联技术部组织制定和修订。

本部分的主要起草单位：中国银联。

本部分的主要起草人：李伟、吴水炯、谭颖、周皓、吴潇、张志波、张晓欢、曹宇、俞纹雯、周英斌、汪毅、周思捷。

银联卡受理终端安全规范

第2卷：产品卷

第1部分：销售点（POS）终端

1 范围

本部分对POS终端安全提出要求。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡标注日期的引用文件，对于标注日期之后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，但是，鼓励根据本标准达成协议的各方研究是否可使用这些引用文件的最新版本。凡不标注日期的引用文件，其最新版本均适用于本标准。

Q/CUP 007.1 银联卡受理终端安全规范-第1卷：基础卷

Q/CUP 007.4 银联卡受理终端安全规范-第4卷：辅助卷

PCI PIN Transaction Security Point of Interaction-Modular Security Requirement 交互点个人识别码交易安全-模块安全要求

3 基础安全要求

POS终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求。

POS终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第3部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

对于分体式终端（终端主机与独立密码键盘配合使用），在无其他功能要求和说明的情况下，终端主机亦可参照第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求以提升主机安全性。

4 传输安全要求

若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。

5 账户数据保护

在设备中传输账户数据（主要指完整磁道信息）时，应满足以下安全要求（下文中最终的账户数据加密设备，指对第6章所述加密磁道信息的工作密钥进行存储并完成加密运算的模块，例如密码键盘等）：

——应保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改。攻击总分至少16分，同时攻击阶段分值至少8分。

——如果最终的账户数据加密设备和读卡器不是一体的,或两者是一体的但传输线路不在保护区域内,则数据必须通过加密传输。识别该加密传输涉及的密钥,或者是对所涉及的公钥进行未经授权的修改或替换,均至少需要26分的识别分值和最小13分的攻击阶段分值。

《银联卡受理终端安全规范-第1卷:基础卷-第2部分:设备安全》(Q/CUP 007.1.2-2014)中第9章模块七账户数据保护为终端可选模块要求。建议终端支持。

6 终端管理和应用安全

6.1 操作员编号和密码

POS的每个操作员应有独立的编号和密码。操作员编号至少为2位数字或字母,密码至少为4位数字。POS终端应具备操作员密码校验功能,校验失败时禁止交易。

6.2 二级密钥体系

POS终端密钥分为二级:终端主密钥(TMK)和工作密钥(WK)。

6.2.1 终端主密钥(TMK)

用于对工作密钥(WK)进行加密保护,POS中心为每台POS终端分配唯一的TMK, TMK应至少采用双倍长密钥。

TMK必须要有安全保护措施,只能写入并参与运算,不能被读取。

6.2.2 工作密钥(WK)

通常用于对个人标识码(PIN)加密的PIK、进行报文鉴别(MAC)的MAK、进行磁道加密的TDK(磁道数据密钥)。

工作密钥(WK)由POS前置机的加密机产生,在POS终端每次签到时从POS中心利用TMK加密后下载,并由TMK加密存储。

POS终端工作密钥在下载时必须以密文传送,严禁明文传送。

6.3 安全加密

采用安全、可靠的加密算法,保证POS交易数据的完整性和隐私性。POS终端PIN加密应至少采用双倍长密钥。

POS终端应对上送的磁道信息进行加密,加密方式与POS中心约定。

7 辅助安全要求

本节所述要求为推荐性要求,非受理终端安全认证强制项。

7.1 地理位置信息

终端宜具备地理位置信息获取和上送能力。

若终端支持该项功能,应满足以下要求:

- 应对地理位置信息获取和上送的相关软硬件模块进行保护,防止被不正当移除、关闭或破坏;
- 应对地理位置信息进行有效保护,防止其被篡改。

7.2 防切机转网

终端可根据管理机构要求支持防切转网功能,具体参照《银联卡受理终端安全规范-第4卷:辅助卷-第1部分:终端防切机转网技术安全指南》(Q/CUP 007.4.1-2014)要求。