Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.2.3—2014

银联卡受理终端安全规范
第 2 卷：产品卷
第 3 部分：个人支付终端

Security Specifications for Terminal Accepting UnionPay Card
Volume 2: Product Requirements
Part 3: Personal Payment Terminal

2014-11-30 发布　　2014-12-01 实施

中国银联股份有限公司 发布

目　　次

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3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、王兰、周皓、吴水炯、张志波、张晓欢、谭颖、曹宇、俞纹雯、周英斌。

银联卡受理终端安全规范
第 2 卷：产品卷
第 3 部分：个人支付终端

1 范围

本部分对通过手机、PC机等接入网络的个人支付终端设备提出安全要求，包括个人支付终端的硬件设备要求和安全体系要求。

本部分适用于持卡人本人使用终端，不适用于商户收单使用的支付终端，商用支付终端安全要求参见《银联卡受理终端安全规范》其它部分。

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 XXX 银联卡受理终端安全规范-第1卷：基础卷

Q/CUP XXX 银联卡受理终端安全规范-第4卷：辅助卷

Q/CUP 056 银联卡支付应用软件安全规范

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

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。

4 账户数据保护

终端对账户数据（包括磁条卡和IC卡）的保护宜满足《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9章模块七账户数据保护的要求。

5 其他要求

5.1 物理要求

输入PIN的模块或IC卡读写器应经过合理设计，以保证无法利用在零售市场上可买到的商品组件来组装PIN输入设备或IC卡读写器。例如，设备电子部件的外壳不是通用的。

5.2 逻辑要求

5.2.1 自检测试

终端要实现自检功能，其中包括完整性和真实性测试，包括开机以及每天检查，检测包括固件、表征篡改迹象的安全机制，以及终端是否处于被攻击状态。当自检失败时，终端及其功能可在安全的方式下失效。

5.2.2 固件更新

如果设备固件能够进行更新，那么设备必须通过加密机制验证更新固件的完整性和真实性。如果未确认其完整性和真实性，那么设备应拒绝进行固件更新或清除设备中所有的密钥。

5.2.3 内存清除

如设备具有PIN输入功能，设备在下面任一情况必须自动清空其内部保存的PIN信息：

——交易已经从终端正确发出；

——PIN输入后等待持卡人或商户的响应超时。

5.2.4 密钥存放管理

终端内应有独立的不可读区域，存放终端私钥、终端密钥等代表终端唯一性的重要信息。

不应存在机制，允许输出明文私钥、明文密钥或者明文PIN，或者使用本身可能已经泄露的密钥来加密密钥或PIN，或者从高安全级组件向低安全级组件传输明文密钥。

5.2.5 密钥替换

如果终端能够保存多个加密密钥而且能够在外部选择加密PIN的密钥，那么终端禁止未经授权的密钥替换和密钥滥用。

5.2.6 合法性认证

个人支付终端首次使用时应与持卡人进行有效身份绑定，每次应用之前需与后台进行合法性认证。

5.2.7 PIN 加密

在个人终端使用过程中应保证PIN的密文传输：

——对于PIN的输入，如通过终端设备输入，应在终端设备加密，加密算法可采用对称加密算法或非对称加密算法。对称加密算法应保证加密密钥一机一密，且密钥应保存在终端设备的安全芯片或处理器的安全区域中；采用非对称加密算法，应保证公钥不能被随意读取、更改、破坏，私钥应统一管理和分发，并确保私钥在服务器的安全存储。

——如PIN通过手机、PC机等主机设备进行输入，需采取技术措施防止密码盗取，技术手段可包括但不限于以下方式。对于反复尝试并输入错误密码超过一定次数的，进行软件登录和支付交易控制，必要时可根据业务规则予以交易阻断。

- 所有用户输入的客户端登录密码、银行卡密码等敏感信息不得在界面上显示明文；
- 密码等敏感信息采用软键盘方式输入；
- 敏感信息输入后需要立即采用健壮的算法加密。

5.2.8 账户信息保护

——终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡数据、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。

——磁道信息应由个人支付终端设备读取并在终端内完成加密，在终端以外不得以明文形式出现。

——对磁道进行加密的算法可采用对称加密算法和非对称加密算法。采用对称加密算法应保证加密密钥仅由本终端使用，且存储于安全芯片或处理器的安全区域中；采用非对称加密算法应保证公钥不能被随意读取、更改、破坏，私钥应统一管理和分发，并确保私钥在服务器的安全存储。

——如业务涉及卡号显示，须进行屏蔽保护，卡号的前六位和后四位正常显示，其余卡号位进行’*’屏蔽。

5.2.9 报文的完整性要求

应保证交易报文在通信过程中的完整性。防止交易报文中涉及的交易金额、交易日期、订单号等重要信息在交易过程中被非法篡改。

5.2.10 远程控制

终端应具备防远程控制安全机制，防止非法利用木马等病毒远程控制设备，进行非法交易。

6 辅助安全要求

6.1 对应支付应用软件要求

装载于手机、PC等设备，与受理终端配合使用的应用软件应满足《银联卡支付应用软件安全规范》（Q/CUP 056）要求。

6.2 后台系统控制

个人支付终端的使用前，应向业务后台系统提交终端信息，由业务后台系统完成对终端的认证。持卡人在终端上录入或由终端读取银行卡信息，供后台系统对终端和卡片进行关联，并在支付过程中控制终端可使用卡片的数量，以保证个人终端设备的个人使用。