Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.1.3—2014

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

Security Specifications for Terminal Accepting UnionPay Card
Volume 1: Fundamental Specifications
Part 3: Device Management Security

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 III
1 范围 1
2 规范性引用文件 1
3 设备生产阶段管理安全 1
4 设备部署前阶段管理安全 2

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1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、银行卡检测中心、福建联迪商用设备有限公司、福建新大陆电脑股份有限公司。

本部分的主要起草人：李伟、吴水炯、谭颖、周皓、张志波、杜磊、倪国荣、孟陆强、姚承勇、严明、卢佩新。

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

1 范围

本部分对终端管理安全提出要求。

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。

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 设备生产阶段管理安全

3.1 变更控制

在设备生产过程中应采取变更控制机制，保证当设备任何物理或逻辑特性发生变化时，设备都应按照本规范基础卷第一部分所有可适用的安全要求进行重新评估。

3.2 固件保护

对通过评估的固件要合理地保护和存储，防止被非法修改。应采用双重控制、标准化加密认证等方式对固件进行保护。

3.3 PIN 输入设备保护

在生产过程中，用于组装PIN输入设备的组件应通过核心安全要求（包括物理、逻辑、联机PIN处理、脱机PIN处理）和/或集成安全要求的评估，并且这些组件没有被非法替换。

3.4 软件安全控制

设备所安装的软件（例如固件等）在运送、存储和使用时，应遵循双重控制的原则，防止在未授权情况下对软件的修改和/或替换。

3.5 设备安全存放

在产品生产完成后出厂前，或在产品生产完成后经销商售出前，设备和其任何组件都应存放在受保护的、访问受控的区域内，或将设备封装在具有防攻击特性的包装中，以防止非法接触设备或其组件。

3.6 初始保密验证信息

如果设备在装载密钥或者最初部署时，需要对生产过程中装入设备的秘密信息进行验证。那么，该秘密信息对每台设备来说必须是唯一的，任何人都不可知和不可预测该信息，并且该秘密信息应在双重控制下装入设备，以确保在安装期间不被泄露。

3.7 安全文档

生产厂商应维护开发安全文档，包含所有与物理硬件、程序软件、流程、责任人员及其它安全相关的安全机制和措施（所涵盖内容对在开发环境下安全相关组件设计和实现的完整性保护是必要的）。

安全文档应提供证据，以说明与设备安全相关组件的开发、生产和维护均按照所制订的安全措施进行，且应证明所采取的安全措施对安全相关组件完整性的保护已达到必要的保护等级。

3.8 维修控制

维修的全过程以及维修后的检查、测试过程应有控制措施，确保不出现未授权的修改。

4 设备部署前阶段管理安全

4.1 概述

本节阐述设备在生产完成之后、初始密钥注入之前，或生产完成之后、设备首次布署之前，这一阶段内的管理安全。

4.2 修改保护

设备应具备防攻击的安全特性，防止未经授权的修改。

设备生产厂商应向客户提供有助于确认设备真实性和完整性的安全指导文档，文档可随产品一同运送或在线获得。

4.3 运输安全

设备在从生产厂商至初始密钥注入地或初始部署地的运输或传递途中，应进行审计控制，保证可在任何节点及时地确定每一台设备的具体地点。如涉及多方组织运输或传递，应确保所有运输参与方所负责的运输和存放均符合规定要求。

必须设计合理的流程将对设备管理的安全责任由生产厂商向设备初始部署方传递。如设备从生产厂商至初始部署地的运输或传递过程中的一个或多个环节通过中介机构（如经销商）进行，则中间机构从收到设备直至传递到下一个中介机构或者是初始部署地之前，均对设备负有责任。

设备从生产厂商向初始密钥注入方运输或传递的过程，应该具备下列条件中的一项或两项：

——应在具有防攻击特性的包装中存放并运送设备；

——设备在存放和运输时存有保密信息，当试图对设备做任何物理或功能的改变或攻击时，将导致该保密信息立即自动擦除；初始密钥注入方应能对该保密信息进行验证，未授权的个人无法获取该保密信息。

4.4 初始密钥注入

根据初始密钥注入是否由设备生产厂商完成，对厂商提出相应要求：

——如初始密钥注入由设备生产厂商完成，则厂商应对与设备安全相关的组件的合法性进行验证；

——如初始密钥注入不由设备生产厂商完成，则厂商应向初始密钥注入方提供确认设备安全相关组件合法性的安全指导文档。

4.5 设备标识

每台设备应贴有一个唯一的可见标识。

4.6 运营管理指南

设备生产厂商应维护运营管理指南，包含记录安全相关组件的整个生命周期管理以及将其集成到单个终端设备的方式，包括但不限于以下内容：

——生产和个人化的数据；

——物理位置和生产时间；

——维修；

——移除操作；

——丢失或被盗。