Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.2.7—2014

银联卡受理终端安全规范
第 2 卷：产品卷
第 7 部分：mPOS 通用技术安全

Security Specifications for Terminal Accepting UnionPay Card
Volume 2: Product Requirements
Part 7: General Technical Security of mPOS

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7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、百富计算机技术（深圳）有限公司、福建升腾资讯有限公司、深圳市新国都技术股份有限公司、福建新大陆支付技术有限公司。

本部分的主要起草人：吴水炯、曹宇、吴潇、徐燕军、李伟、李洁、谭颖、汪毅、周思捷、刘志刚、安焘、倪国荣、姚承勇、杨超杰、万籁民、林尧禹、张贵潭、刘祥洪、卢佩新。

银联卡受理终端安全规范
第 2 卷：产品卷
第 7 部分：mPOS 通用技术安全

1 范围

本部分对受理银联卡（包括磁条卡及IC卡）开展商户收单业务的mPOS终端设备和相关应用及系统提出安全要求，包括受理终端、终端上位机（支付应用软件）、后台处理系统等受理体系各组成部分自身的安全要求，以及体系整体的端到端加密机制，旨在提升银联卡账户和交易数据在开放环境下的安全性。

mPOS为整体概念，包括终端设备和相关应用。具体指，通过移动通讯设备（所搭载的支付应用软件）进行商户收银操作，由外接专用受理终端完成银联卡相关信息的采集和加密，通过移动通讯设备与后台处理系统交互完成交易，这一过程涉及的前端专用软硬件设备。

开放环境包括公共传输网络、搭载开放式操作系统的终端上位机、以及处于受理终端（或上位机）与后台处理系统之间的所有非封闭式的信息传递路径及路径上所有设备和系统。凡使用开放协议（如TCP/IP协议等）进行传输的均认为处于开放环境中。

本部分为用于银联卡收单业务的终端设备和系统提供基础安全要求，个人支付终端设备和系统也可参照执行以进一步提升安全性。

采用封闭或定制操作系统运行环境、符合《银联卡受理终端安全-第2卷：产品卷》（Q/CUP 007.2-2014）定义的POS终端、无人值守（自助）终端和智能终端仍可遵照相应规范要求进行生产和认证。

无PIN输入要求且符合《银联卡受理终端应用规范 第3部分 银联卡（IC卡）脱机受理终端规范》（Q/CUP 009.3）定义的IC卡脱机受理终端仍可遵照相应规范要求进行生产和认证。

本部分仅对文中描述的直接受理银联卡（包括磁条卡和IC卡）支付的设备、应用和系统提出安全要求，条码（包括二维码）支付、声波支付、指纹支付等附加功能不在本要求范围内。

本部分适用于受理银联卡的终端生产企业、支付应用软件开发商及收单机构。

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

银联风管委【2013】9号 银联卡收单机构账户信息安全管理标准

银联风管委【2006】6号 银联卡账户信息与交易数据安全管理规则

第三方机构接入银联的技术安全要求

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Q/CUP 007 银联卡受理终端安全规范

3 基于开放环境的 mPOS 受理系统

3.1 整体架构

本要求所述开放环境下受理系统架构如图1。

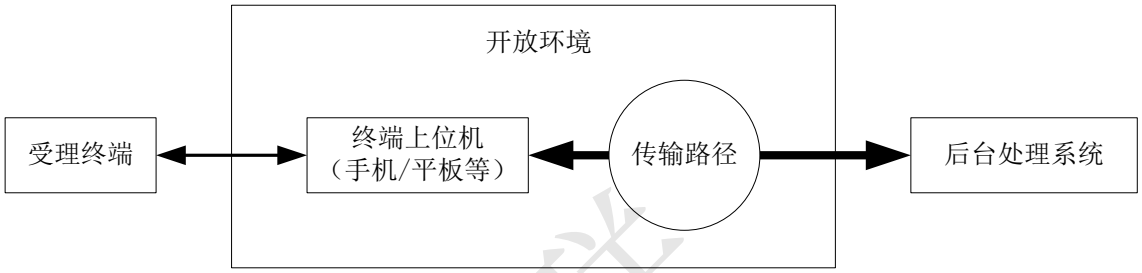

图1 mPOS应用及系统架构

mPOS包括硬件部分（受理终端）、软件部分（终端上位机搭载的应用软件），并需后台处理系统设计相应管理和处理流程进行配合使用。mPOS为整体概念，包括终端设备和相关应用。具体指，通过移动通讯设备即终端上位机（所搭载的支付应用软件）进行商户收银操作，由外接专用受理终端完成银联卡相关信息的采集和加密，通过上位机与后台处理系统交互完成交易，这一过程涉及的前端专用软硬件设备。

——后台处理系统：对由受理终端加密的数据解密，进行信息处理或转发。

——传输路径：受理终端与后台系统间所有非封闭式的信息传递路径及路径上所有设备和系统，用于进行账户和交易信息的传输和转发，如：公共网络、终端上位机与后台处理系统间的局域网、路径上可能涉及的用于存储、转发的设备等。

——终端上位机：搭载应用软件（如：支付应用软件、收银软件、商户或收单机构增值应用等）、具备与后台交易处理系统联网通讯功能的设备。上位机可以为收银机、POS主机，也可以为手机、平板电脑等通用移动设备，本要求主要指手机、平板电脑等。上位机不应支持读取和加密银行卡信息（包括磁条卡和IC卡），不应接受用户输入并加密个人标识码（PIN），上位机完成的报文加密或计算报文鉴别码（MAC）等操作不可替代受理终端应实现的相应功能。

——受理终端：经过检测认证、符合安全标准的可被信任的支付受理设备，可安全获取并保护账户信息、验证信息和交易报文，功能应包括：证书及密钥的安全存储，与后台系统之间的认证及建立安全通道，安全读取和加密银行卡信息（包括磁条卡和IC卡），接受用户输入并加密个人标识码（PIN），安全显示交易类型、金额、结果等交易提示信息，以及加密账户信息、计算报文鉴别码（MAC）等。受理终端借助上位机的应用处理和通讯能力与后台系统实现交互。本要求所述受理终端以满足商户收单安全为前提，个人支付终端遵循《银联卡受理终端安全规范 第7部分 个人支付终端安全规范》，但建议个人支付终端也可参照本要求提升其安全性。

3.2 开放环境

开放环境包括 3.1节所述传输路径和搭载开放式操作系统的上位机（如未经定制的手机或平板电脑）。

本要求所述“开放环境”指上位机和传输路径所构成的整体环境是开放的，例如：上位机搭载有通用操作系统、传输路径中包含公共网络传输等，即只要数据传输链条中存在任意一环节处于开放条件下，

该系统整体便为基于开放环境的系统，所使用的终端便为基于开放环境的受理终端。凡使用开放协议（如TCP/IP协议等）进行传输的均认为处于开放环境中。

非开放环境包括对资源访问权限、外设接口、系统和应用校验、数据存储和传输等进行安全设计或定制、并符合安全要求的专用设备（如：符合《银联卡受理终端安全规范》的POS终端、智能POS等专用安全设备），以及专线网络。

本要求中所述“经定制的手机或平板电脑”指在操作系统、硬件等方面进行了安全设置，使之能满足银行卡支付安全要求、达到银行卡账户和交易信息保护水平的专用设备，非通用电子设备。

4 安全目标

4.1 概述

本部分第5章至第7章所列举的通用要求均以满足第本章各项安全目标为前提，不应以未列举强制要求为由而妨碍下列安全目标的实现。

4.2 账户信息安全保护

受理终端应对账户信息进行安全保护。账户信息保护要求参见《银联卡收单机构账户信息安全管理标准》（银联风管委【2013】9号）和《银联卡账户信息与交易数据安全管理规则》（银联风管委【2006】6号）。

其中，完整磁道信息、PIN、卡片验证码、卡片有效期等敏感数据应被安全加密和解密，在受理终端和后台系统的硬件加密模块之外不得以明文形式出现，终端不应输出完整的主账号（卡号）信息，应保证数据在处理和传输过程中不被泄露、窃取和篡改。

任何设备和系统均不得存储敏感数据（即使已经加密），账户信息只用于完成当前合法银联卡交易，不得用于任何其他用途。

4.3 交易信息安全保护

除卡号、PIN、磁道信息、有效期、卡片验证码等交易信息（参见银联风管委【2013】9号和【2006】6号相关风险要求）之外，还应保证交易金额、交易类型、货币类型、商户号、终端号等关键交易信息在处理和传输过程中不被篡改。

4.4 安全提示

终端应提供相关机制，确保交易过程中流程关键环节（如：交易金额及交易类型确认，密码输入等）和交易结果能安全、有效地向持卡人和收银员进行强制提示，确认后才可进行下一步操作。

4.5 交易真实性

对交易报文的来源进行鉴别，保证交易真实性，防止信息伪造和重放攻击。

5 受理终端安全要求

5.1 基础安全要求

受理终端应满足《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。

受理终端应满足《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。

受理终端宜实现DUKPT或等效的一次一密机制，建议实施标准DUKPT机制。

5.2 终端功能限制

受理终端不应向上位机提供单独、直接的PIN和磁道等敏感数据加密计算功能，防止被用于伪造交易、密钥穷举破解等。

若受理终端向上位机提供MAC计算功能，则应对交易金额等4.3节所述交易信息进行强制校验或填充，防止交易信息被篡改后骗取合法MAC。

5.3 传输安全要求

若受理终端使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。

受理终端应保证能有效鉴别后台发送数据的真实性、完整性。终端输出数据的保护见4.2和4.3要求。

5.4 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9章模块七账户数据保护的要求。

5.5 交易信息安全要求

终端应保证所获得的交易金额、交易类型、货币类型、商户号、终端号、交易结果等关键交易信息在后续处理和传输过程中不被篡改。

5.6 终端唯一性和真实性要求

受理终端应保证具有唯一性，满足一机一密要求（例如：在主密钥和工作密钥组成的二级密钥体系中，应保证每台受理终端分配唯一主密钥；在DUKPT中，应保证每台受理终端分配唯一初始密钥序列号KSN）。

若涉及受理终端远程启用，终端与后台处理系统应进行联机认证，并上送受理终端设备序列号等信息，未通过联机认证不应进行支付交易。

6 上位机支付应用软件安全要求

6.1 基础安全要求

上位机安装的支付应用软件应符合《银联卡支付应用软件安全规范》（Q/CUP 056）的要求。

6.2 辅助信息要求

软件应具备地理位置信息获取和上送能力，且对所获取的地理位置信息进行保护，防止处理或传输过程中被篡改。

如软件可获取当前上位机唯一特征码（如IMEI号、设备MAC地址等），则应上传作为平台安全评估的辅助参考手段。

6.3 软件功能限制

IC卡应用处理内核（UICS Level 2、PBOC Level 2等）内核不应部署于上位机。

7 辅助安全要求

本节所述要求为推荐性要求或关联领域要求。

7.1 机构管理

建议收单机构采取有效手段加强对终端和对应商户的管理，并设计安全的交易处理流程和系统实现方案。

建议收单机构应采取必要的操作人员管理手段对支付应用软件的使用权限进行有效控制，采取必要管理手段确保应用软件（包含与支付相关以及与支付无关的所有应用软件）通过合法渠道获取并通过正版授权，由管理员统一管理安装。应设置严格的联机登录保护机制（例如通过复杂密码授权）才可进行操作。应确保系统运行在最低权限，不应有越狱或Root等行为。

7.2 后台处理系统

后台处理系统应配合受理终端、应用软件共同抵御重放攻击，防止加密数据和交易报文被重用。

对于后台处理系统，建议应能具备安全的加解密功能，维护安全运行环境，有效抵御病毒、DoS等网络攻击，防止非法终端对系统安全造成影响，并能及时对异常情况进行处理。其中账户信息层面具体安全要求参见《银联卡收单机构账户信息安全管理标准》（银联风管委【2013】9号）、《银联卡账户信息与交易数据安全管理规则》（银联风管委【2006】6号），非金融支付机构应满足《第三方机构接入银联的技术安全要求》。

7.3 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。

8 安全建议和风险提示

上位机和公共网络安全风险较大，在上位机上实现报文组包等关键交易处理逻辑存在较大安全挑战。在现有安全条件下，不建议以该模式部署。如因业务需要确实需进行此类部署，收单机构应充分评估其风险，设计强化的安全机制和配套的业务风险管理机制，并谨慎应用。

如后台处理系统实现报文组包等交易处理逻辑，应强制实现受理终端与后台处理系统建立数据传输的安全通道，并制定相应的密钥和信息交互安全机制。