Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.4.2—2014

银联卡受理终端安全规范
第 4 卷：辅助卷
第 2 部分：航空机上支付技术安全指南

Security Specifications for Terminal Accepting UnionPay Card
Volume 4: Auxiliary Requirements
Part 2: Technical Security Guideline of Airline Payment

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4卷第2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
本部分的主要起草人：吴水炯、杜磊、李海滨、彭乾、王建新、安焘、蒋利兵。

银联卡受理终端安全规范
第 4 卷：辅助卷
第 2 部分：航空机上支付技术安全指南

1 范围

本部分为航空领域实现机上支付提供技术安全指南，供机构、厂商和航空企业参考使用。

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
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

3 支付系统

3.1 整体系统架构

本指南所述受理系统架构如图1。

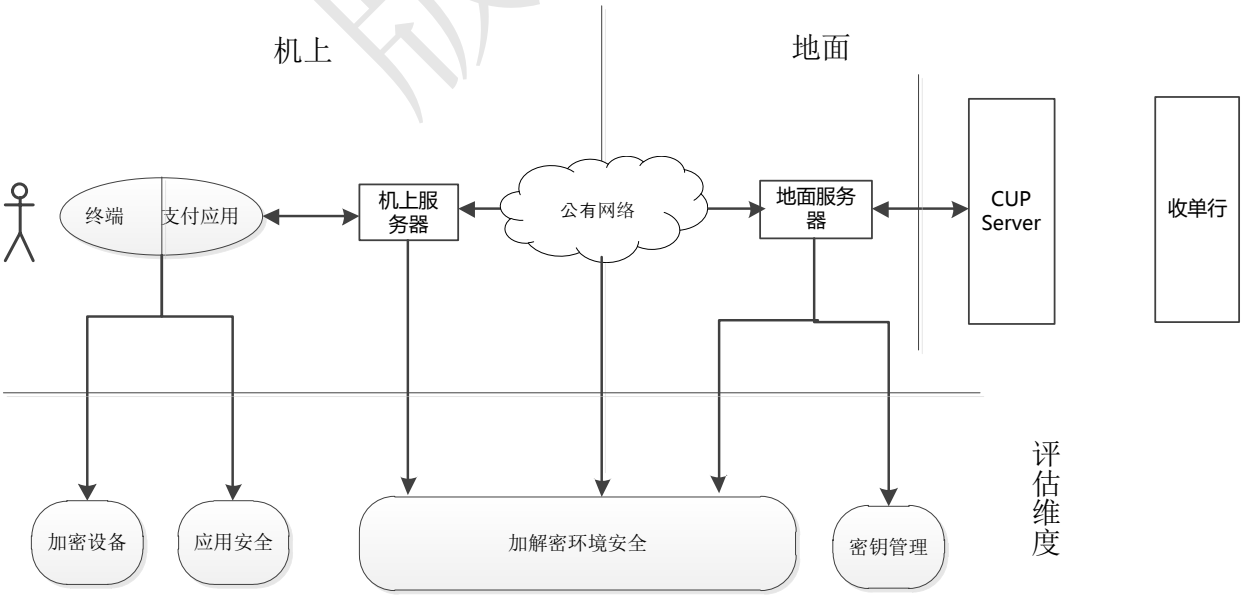

图1 系统架构

终端—— 加密设备：

实现与持卡人的交互，协助持卡人发起并完成交易，采集持卡人PIN等敏感信息以及PAN和账户信息等交易信息，并将全部交易数据加密后传送至机上服务器。

支付应用——应用安全：

运行于终端的硬件与固件之上的支付应用程序，实现与持卡人的交互，协助持卡人完成交易支付。

机上服务器——加密环境：

接收终端发送的交易加密信息，完成与交易相关的黑名单、交易限额检查等辅助功能。将加密的交易数据通过传输网络发送给地面服务器。接收地面服务器返回的加密交易数据，并传输至终端以反馈给持卡人。

传输网络——加解密环境间的传输：

可使用公共或私用传输网络，实现交易数据在航空机上服务器和地面服务器间的加密数据传输。

地面服务器——解密环境\密钥管理：

接收机上服务器的加密交易数据，对交易数据进行解密并完成交易报文组包，实现与银联后台服务器的对接。对自由密钥体系进行管理。

3.2 所处环境

根据航空器相关民航规章规定，公共航空运输企业不得运输拒绝接受安全检查的旅客，不得违反国家规定运输未经安全检查的行李。承运人运送旅客，应当出具客票。旅客乘坐民用航空器，应当交验有效客票，且乘客必须持有有效证件对身份进行核实后方能登记并对号入座。因此理论上讲，航班上的每位乘客持卡人都具有一定的可追溯性。

机载娱乐系统在飞机上属于封闭系统，系统不提供任何接口供旅客接入个人设备进行系统对接。飞行途中旅客对机载设备的任何恶意破坏都将可能影响飞机飞行安全，并且该行为将被视为非法行为，机长有权在飞行阶段对其进行处理。

娱乐系统更新需通过授权下的专业人员持专有设备进行，任何未经授权的改动都将被视为违规操作，并将导致娱乐系统在飞机放行时被视为不可用，即不能提供正常使用。

飞机停场或维修阶段，除授权人员外，任何人不得接近航空器，否则将被视为违法行为。

飞机系统部件因故障被拆下，翻修后的设备必须经过专业检测并得到适航标签后，方可视为可装机件。除授权维修人员和授权维修单位外，任何人和单位不得对设备进行非法拆解和修理，否则部件将被视为不适航，无法安装入飞机。

4 安全目标

4.1 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，应保证数据在处理和传输过程中不被泄露、窃取和篡改。受理终端应对IC卡关键数据进行加密保护，使得上位机无法获取相关数据的原始信息。

任何设备和系统均不得存储敏感账户信息（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。

4.2 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、商户代码、交易流水号等关键交易信息在处理和传输过程中不被篡改。

4.3 安全提示

交易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。

4.4 交易真实性、完整性

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。

4.5 交易容错

交易过程中非可预测性的传输链路错误，或系统错误等不可控因素不会导致账户资金的丢失或差错。

5 安全要求

5.1 加密设备

5.1.1 PIN 输入设备安全要求

当终端具有PIN输入、加密以及传输功能，可支持IC卡、磁条卡等安全读卡器时，宜参考《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》规范模块一、模块二、模块三和模块四的安全要求，保证终端物理安全、逻辑安全、联机安全及脱机安全。

5.1.2 集成终端安全要求

当终端由不同组件集成而成，协同完成交易时，宜参考《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》规范中模块五集成安全要求，确保终端符合安全要求。

5.1.3 开放协议安全要求

当终端支持基于IP的通讯协议时，宜参考《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》规范中模块六开放协议要求，确保终端符合安全要求。

5.1.4 安全读取和数据交互账户数据保护安全要求

当终端具有非PIN数据即账户信息（PAN、磁道数据、持卡人信息等）的输入、加密以及传输功能的终端，可支持IC卡（包括接触式和非接触式）、磁条卡等介质的安全读卡器时，宜参考《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》规范中模块七账户数据保护要求，确保终端符合安全要求。

5.2 应用软件安全（受理终端上支付应用）

5.2.1 应用软件的下载、安装与更新

当需要远程下载（获得）应用时，需采用以下安全防护措施：

——采取有效手段保证软件传输过程的机密性和软件的完整性；

——应确保软件版本有更新时及时提示用户进行升级；

——使用签名信息嵌入软件保证安装包的合法性。

当需要本地人工安装、更新应用时，需采用以下安全防护措施：

——采取有效手段保证安装人员已经受到授权和批准；

——应确保软件版本有更新时及时提示用户进行升级；

——使用签名信息嵌入软件保证安装包的合法性。

5.2.2 应用软件的自检

应用软件启动时应执行自检程序，检查软件运行时所 必需的条件，确保软件自身和所处运行环境的安全性。

5.2.3 合法性认证和风险控制

应用软件与后台系统应具备合法性认证机制，通过签名验签等密码技术手段与后台系统进行双向认证，确保后台系统和应用软件的合法性，建立一条安全的信息传输信道。保持应用软件认证状态，防止未授权信息更改认证状态，并设置认证超时时间。

5.2.4 审计

应用软件应具备记录所有用户访问日志的功能，便于进行适当的审计和监控。在完成安装时应开始记录所有用户（特别是具有管理权限的用户）的访问，并且能将每次活动情况追踪至相应的个人。支付应用软件的日志记录功能应能自动启动，或可由用户自行启用，并应在相关指导文档中要求用户不得停用日志。

5.3 加解密环境

5.3.1 账户信息保护

账户信息的保护应满足银联风管委[2013] 9号《银联卡收单机构账户信息安全管理标准》第二章“基本要求”，以及第六章“账户信息生命周期安全管理”中6.2-6.5节的要求。

5.3.2 密钥管理

密钥管理应满足银联风管委[2013] 9号《银联卡收单机构账户信息安全管理标准》第六章“账户信息生命周期安全管理”中6.1节的要求。

5.4 基础设施安全

物理环境、网络安全、主机安全、应用系统安全和数据安全应满足中国银联《第三方机构入网技术安全规范》中第5章“基础设施安全”部分的要求。

6 银联标识

过检设备上应具备符合中国银联受理标识相关规范的明显银联标识。