# Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.2.2—2014

# 银联卡受理终端安全规范
# 第 2 卷：产品卷
# 第 2 部分：无人值守（自助）终端

Security Specifications for Terminal Accepting UnionPay Card
Volume 2: Product Requirements
Part 2: Unattended Payment (Self-Assist) 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。

本部分的主要起草人：李伟、吴水炯、周皓、谭颖、李洁。

感谢福建联迪商用设备有限公司和深圳市证通电子股份有限公司对本规范制定工作提供的支持。

# 银联卡受理终端安全规范
# 第 2 卷：产品卷
# 第 2 部分：无人值守（自助）终端

## 1 范围

本部分对无人值守（自助）终端提出安全要求。

## 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 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

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

无人值守（自助）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。

无人值守（自助）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 集成要求

无人值守（自助）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7章模块五集成安全的要求。

## 5 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。

## 6 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。

## 7 其他要求

### 7.1 一机一钥

无人值守（自助）终端的机柜钥匙应当实现一机柜一钥匙，不能多机柜共用一把钥匙，简称“一机一钥”的要求。

# 附 录 A
# （规范性附录）提供现金服务的无人值守（自助）终端抗破坏能力要求

## A.1 总体目的和要求

——试验的目的是检验无人值守（自助）终端的抗破坏能力。试验人员可在试验程序的范围内选择一系列攻击，并且在试验时间内尝试每个攻击方案。如果无人值守（自助）终端在指定的净工作时间内，在指定的点或面上，能够抵抗最严酷的攻击方法或几种攻击方法的最佳组合，那么该项试验可以通过。

——净工作时间是指对样品进行破坏的时间，不包括测试的准备时间、安全防范所需的时间、以及不可预期的延误时间。

——除了设陷取现，成功的攻击应该在特定的时间内，移走无人值守（自助）终端内至少10%的现金，或将现金暴露在外，以致它们都可以被移走。

——设陷取现必须成功地进行三次取现而不被发现或不打断无人值守（自助）终端的运行。设陷取现可以在操作中进行调节。

——所有的攻击应该由熟悉设计的一个或两个有经验的人员来进行。

## A.2 用户界面的试验-24h服务式

### A.2.1 概述

提供24h服务的无人值守（自助）终端对通过用户界面采用钓现、设陷取现及暴力取现的各种企图应能抵抗 30min。所有的试验只限于在用户界面上所进行的攻击。

### A.2.2 工具

试验中的攻击过程是相对安静的，其中所用的工具仅限于能被藏于两个试验人员衣服内的绳索、金属丝、钩子、撬棍、扳钳、螺丝刀、钢锯片及其类似工具。除像绳索、金属丝、钩子那样可被卷起或被折叠的工具外，其它工具的长度不应超过 0.6m。

### A.2.3 时间

一次试验可选用多种攻击方式，每种攻击可进行 30min。

每种攻击方式只可进行一次。如果两种攻击共用了 30min，那么第一种攻击所造成的破坏可延用在第二种攻击中。

### A.2.4 方法

钓现、暴力取现、设陷取现是由无人值守（自助）终端的设计所决定的。

在试验中，只使用不超过 1.4kg 重的锤子，或与长度不超过 0.6m 的凿子、钻孔机及螺丝刀等一起使用的时间最长不超过 30s。

## A.3 保险柜的试验——24h服务式

### A.3.1 概述

若无人值守（自助）终端具备保险柜，应满足A.3节要求。基本要求如下：

——A.3.4 中所述的任何一种或全部攻击方式均可选作从保险柜中取现的方法。

——样机的门间隙应代表以后生产产品的最大门间隙。

——提供附有材料规格的完整结构图。

——随样机应有两个按金属材料的拉伸测试 GB 228-1987 中所定的抗张力试验样品，此试验样品直径为 12.7mm，长为 50.8mm，并用制造样机门及机壳所用的钢所制成的。

——如果所用材料不是钢，则不需提供这些样品。

A.3.2 工具

试验工具包括普通的手持工具、机械式或便携式电动工具、锉、硬质合金钻、挖凿工具，但不包括磁性钻床及其它应用压力的机械、砂轮和电锯。

普通的手持工具为重量不超过3.6kg的凿子、冲具、扳钳、螺丝刀、锤子及撬杆，长度不超过1.5m的撬棍及割锯工具，以及套筒。

挖凿工具为普通型或标准型，但不应被特别设计用于一个特别的产品。便携式电动工具指规格为12.7mm的高速手持电钻。

A.3.3 时间

24h 服务式的保险柜应能抵抗15min破坏攻击。可选用A.3.4中所述的一种方法或所有方法，采用指定的工具，每种方法可持续15min。

每种攻击方法只可进行一次。如果两种攻击共用了 15min，那么第一种攻击所造成的破坏可延用在第二种攻击中。

保险柜应该如正常营业时一样装载现金。成功的攻击以满足A.1.3中所述的要求为准。

A.3.4 方法

打孔和钻孔的组合——通过用凿掘工具、金属线、钩子或其它的普通手持工具敲掉密码锁的拨号盘，在转轴上打孔或钻孔以打开锁紧机构。

锁紧机构——试图接近锁盒、接线片、拨杆或其它机械部分，通过打孔、撬凿或切断来松开锁舌。

锁舌——通过门上的开口切断或移动主要锁舌使其脱离连接。

切断锁舌——刺穿门的旁柱并切断主要锁舌。

通过打孔、钻孔来开锁——通过在密码拨号盘轴上打孔、钻孔，同时用力转动门把手以打开锁紧机构，也可以用挖凿工具或其它的手持工具打开锁紧机构。

把手施力——通过扳手或金属杆在门闩操作杆上加力，以旋转门闩把手，或通过在门闩把手上打孔，使锁被打开。

撬开或劈开门——用楔子、凿子和撬刺破或打开门以取走现金。

开口——通过在保险柜上钻一圈很密的孔，然后用铁锤凿开这部分金属，以在保险柜上打出一个洞。

保险柜边缝——通过保险柜设计中的上边缝、侧边缝及下边缝用暴力打开保险柜并从其中钓现。不能使用电动、风动以及类似的能源驱动的工具攻击保险柜。