Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.2.5—2014

银联卡受理终端安全规范
第 2 卷：产品卷
第 5 部分：电话支付终端

Security Specifications for Terminal Accepting UnionPay Card
Volume 2: Product Requirements
Part 5: Specifications of Telephone 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5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：王炎方、单长胜、周皓、黄发国、李伟、吴水炯、张志波、邱俊、李春欢

银联卡受理终端安全规范
第 2 卷：产品卷
第 4 部分：电话支付终端

1 范围

本部分对电话支付终端安全提出要求。电话支付终端的软件要求、终端的应用功能及接口和外设指令格式参见《电话支付终端应用规范》（Q/CUP 009.5）。不涉及电话支付业务交易主机端的规定。

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

Q/CUP 007.4 银联卡受理终端安全规范-第4卷：辅助卷

Q/CUP 009.5 银联卡受理终端应用规范-第5部分：电话支付终端应用规范

ANSI X9.19 Financial Institution Retail Message Authentication 金融机构零售业务信息认证

ANSI X9.8 Personal Identification Number (PIN) Management and Security 个人识别码管理和安全

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 电话终端 I 型

3.1 密钥体系和加密模块

签到密钥模式分为二级密钥：密钥加密密钥（KEK）和工作密钥（WK）。其中KEK又称终端主密钥，用于对工作密钥进行加密保护。终端主密钥存放于TSAM卡中，不同TSAM卡应注入不同的终端主密钥，实现“一机一密”要求。

电话终端I型由TSAM卡实现对磁道信息和PIN的加密，实现报文MAC计算。

3.2 工作密钥生成

工作密钥包括PIN加密密钥PIK、磁道加密密钥TDK和MAC计算密钥MAK。使用主密钥产生工作密钥的过程如下：

1、TSAM卡产生一个4字节的随机数；

2、TSAM卡提取随机数序号（4字节，以16进制表示），该序号在TSAM上每操作一次后自动加1；

3、TSAM卡将序号和随机数合并成8字节的计算因子（前4字节为序号、后4字节为随机数）；

4、用主密钥对计算因子做3DES运算获得工作密钥。

3.3 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。

3.4 其他要求

本节要求主要涉及电话终端I型的应用程序及后台处理系统。

3.4.1 PIN 和磁道加密

PIK和TDK在每次交易中应不同。PIN加密算法使用双倍长密钥算法进行加密，PIN加密必须使用3DES算法。

3.4.2 MAC 计算

从报文类型到有效数据域之间的部分构成MAC ELEMEMENT BLOCK（MAB），MAC的加密算法不强制要求，建议采用ANSI X9.19算法，详细算法见《中国银联电话支付终端应用规范》附录E。

3.4.3 账户信息

电话支付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，不得存储银行卡磁道信息、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。

电话支付终端应确保本规范所涉及键盘输入信息的安全，禁止通过重拨等功能获取相关资料。

3.4.4 终端关联

电话支付终端建立终端序列号（也称终端编号）、安全加密模块号（I型为TSAM卡号）、电话号码（或IMSI号码）三者的关联，对于三者中关联有一个不匹配的，电话支付中心应拒绝该终端发起的所有交易请求。

4 电话终端 II 型

4.1 基础安全要求

电话终端II型应满足《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。

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。

对于分体式终端（终端主机与独立密码键盘配合使用），在无其他功能要求和说明的情况下，终端主机亦可参照第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安全的要求以提升主机安全性。

4.2 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。

4.3 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。

4.4 其它要求

本节要求主要涉及电话终端II型应用程序及后台处理系统。

4.4.1 密钥体系

签到密钥模式分为二级密钥：密钥加密密钥（KEK）和工作密钥（WK）。其中KEK又称终端主密钥，用于对工作密钥进行加密保护，每台电话支付终端与电话支付中心共享唯一的主密钥。终端主密钥必须有安全保护措施，智能写入并参与运算，不能被读取。

终端主密钥应具有唯一性，即不同电话支付终端应设置不同的终端主密钥，实现“一机一密”。

工作密钥包括PIN加密密钥PIK、磁道加密密钥TDK和MAC计算密钥MAK。工作密钥由电话支付中心加密机产生，电话支付终端每次签到时从电话支付中心利用KEK加密后下载，并由KEK加密存储，严禁明文传送。每次签到更新不同的工作密钥对PIN、磁道信息等交易敏感信息进行加密。

4.4.2 MAC 计算

从报文类型到有效数据域之间的部分构成MAC ELEMEMENT BLOCK（MAB），MAC的加密算法不强制要求，建议采用ANSI X9.19算法，详细算法见《中国银联电话支付终端应用规范》附录E。

4.4.3 PIN 加密

PIN加密采用ANSI X9.8 Format（带主账号信息）算法进行格式化，再使用双倍长密钥算法进行加密。电话支付终端要支持以上两种算法。具体的方法见《中国银联电话支付终端应用规范》附录C。PIN加密必须使用3DES算法。

4.4.4 磁道处理

对于磁道信息，应将二磁道信息和三磁道信息（如果存在）合并，并采用TDK进行加密，相关算法详见《中国银联电话支付终端应用规范》附录D。

4.4.5 账户信息

电话支付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，不得存储银行卡磁道信息、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。

电话支付终端应确保本规范所涉及键盘输入信息的安全，禁止通过重拨等功能获取相关资料。

4.4.6 终端关联

电话支付终端应建立终端编号、安全加密模块号（II型为密码键盘序列号）、电话号码（或IMSI号码）三者的关联，对于三者中关联有一个不匹配的，电话支付中心应拒绝该终端发起的所有交易请求。

5 辅助安全要求

本节所述要求为推荐性要求，非受理终端安全认证强制项。

5.1 地理位置信息

终端宜具备地理位置信息获取和上送能力。

若终端支持该项功能，应满足以下要求：

——应对地理位置信息获取和上送的相关软硬件模块进行保护，防止被不正当移除、关闭或破坏；

——应对地理位置信息进行有效保护，防止其被篡改。

5.2 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。