Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.8—2013

银联卡受理终端安全规范
第 8 部分 智能销售点终端安全规范

Specification for Terminal Accepting CUP Cards

Part 8 Smart Point of Sale

2013－06－03 发布　　2013－06－03 实施

中 国 银 联 股 份 有 限 公 司　　发 布

目　　次

前　言

本标准由以下八个部分组成：
——第1部分：销售点（POS）终端安全规范
——第2部分：银联卡受理信息系统安全规范
——第3部分：自助终端安全规范
——第4部分：预留
——第5部分：电话支付终端安全规范
——第6部分：PIN输入设备安全规范
——第7部分：个人支付终端安全规范
——第8部分：智能销售点终端安全规范
本部分为《银联卡受理终端安全规范》的第8部分。
本标准按照GB/T 1.1-2009给出的规则起草。
本部分由中国银联提出。
本部分由中国银联技术管理部组织制定和修订。
本部分的主要起草单位：中国银联电子支付研究院、技术管理部。
本部分的主要起草人：李伟、程志强、吴水炯、才华、王海冰、李洁、周皓、汪毅

智能销售点终端安全规范

1 范围

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范。规定了通过智能终端接入网络的智能销售点终端（本规范以下简称“智能终端”）设备的安全规范，包括智能终端的硬件设备要求、安全要求、生产管理要求和密钥体系等。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2312-1980 信息交换用汉字编码字符集基本集

GB/T 4943.1-2011 信息技术设备的安全

GB/T 6833.2～6833.6-1987 电子测试仪器的电磁兼容性试验规范

GB/T 9254-2008 信息技术设备的无线电干扰极限值和测试方法

GB/T 14916-1994 识别卡物理特性

GB/T 15120.1-.5-1994 识别卡 记录技术

GB/T 15694.1-1995 识别卡 发卡者标识编号体系

GB/T 17552-1998 识别卡 金融交易卡

JR/T 0008-2000 银行卡发卡行标识代码及卡号（2001-01-01实施）

JR/T 0025-2013 中国金融集成电路(IC)卡规范（PBOC 3.0）

Q/CUP 019-2010 非接触式读写器接口规范

Q/CUP 007 银联卡受理终端安全规范

ISO 7812-2-1993 识别卡 发卡方的标识

ISO 7816 识别卡 带触点的集成电路卡

ANSI X9.8 银行业 个人标识码的管理和安全

ISO/IEC 8802-11-1999 Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications

3 术语和定义

3.1

银行卡 bank card

商业银行等金融机构及邮政储汇机构向社会发行的，具有消费信用、转账结算、存取现金等全部或部分功能的信用支付工具。

3.2

持卡人 card holder

银行卡的合法持有人，即与卡对应的银行账户相联系的客户。

3.3

磁条卡 magnetic stripe card

物理特性符合GB/T 14916标准，磁条记录符合GB/T 15120、GB/T 15694-1、ISO 7812-2、GB/T17552标准的银行卡片。

3.4

集成电路（IC）卡 integrated circuit card

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

3.5

个人标识码 personal identification number；PIN

即个人密码，是在联机交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中任何环节都不允许PIN以明文的方式出现。

3.6

销售点终端 point of sale；POS

能够接受银行卡信息，具有通讯功能，并接受柜员的指令而完成金融交易信息和有关信息交换的设备。

3.7

智能销售点终端 smart POS

商户在支付及认证过程中使用的一种智能终端设备，该设备支持磁条卡、IC卡等银行卡数据的读取，能实现卡片及PIN信息的加密保护，可通过互联网接入智能销售点终端后台系统，与后台系统共同实现银行卡交易受理。本规范以下简称“智能终端”。

3.8

智能销售点终端操作系统 smart POS operating system

在智能销售点终端搭载并运行的操作系统，能实现应用的加载和运行、资源的调用、以及安全防护等功能。本规范以下简称“智能终端操作系统”。

3.9

银联卡支付客户端 unionpay payment client

运行于智能终端的支付客户端，提供银行卡的受理入口。

3.10

银联卡智能销售点终端后台系统 unionpay cloud payment background system

银联卡支付客户端的后台系统，具有银行卡交易处理、终端管理等功能。本规范以下简称“智能终端后台系统”。

3.11

应用管理客户端 AppStore client

运行于智能终端的多应用管理客户端，其提供的功能包括但不限于应用下载、应用发现、应用搜索、应用安装、应用卸载等功能。

3.12

应用管理后台系统 AppStore background system

作为应用管理客户端的后台系统，其提供的功能包括但不限于多应用的生命周期管理等功能。

3.13

敏感数据（信息） sensitive data (information)

是指磁道信息、PIN和加密密钥等终端或持卡人独有的数据或信息，敏感数据进行有效保护，防止泄露、被修改或被破坏。

3.14

密钥 key

加密转换中控制操作的一组符号。

3.15

对称密钥 symmetric key

又称专用密钥加密，即发送和接收数据的双方必须使用相同的密钥对明文进行加密和解密运算。对称密钥加密算法主要包括：DES、3DES、IDEA、FEAL、BLOWFISH等。

3.16

工作密钥 working key; WK

也称为数据密钥，包括但不限于PIN加密密钥，该密钥存储于设备的硬件安全芯片中。

3.17

非对称密钥 asymmetric keys

非对称密钥，需要使用一对密钥来分别完成加密和解密操作，一个公开发布，即公开密钥，另一个由使用者秘密保存，即私用密钥。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。

3.18

公钥 public key

在一个实体使用的非对称密钥对中可以被公众使用的密钥。在数字签名方案中，公钥定义验证函数。

3.19

私钥 private key

在一个实体使用的非对称密钥对中仅被该实体使用的密钥。在数字签名方案中，私钥定义签名函数。

3.20

数字证书 digital certificate

由发行证书的认证中心使用其私钥对实体的公钥、身份信息以及其它相关信息进行签名，形成的不可伪造的数据。

3.21

数字签名 digital signature

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被篡改。

3.22

认证中心 certificate authority; CA

CA是证书的签发机构，是负责签发证书、认证证书、管理已颁发证书的机关。它负责制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权。

3.23

SSL 和 TLS

安全套接层协议（Secure Sockets Layer，SSL）和传输层安全协议（Transport Layer Security，TLS）对网络连接实现加密，是为网络通信提供安全及数据完整性的一种安全协议。

3.24

IPSEC

IPSEC（Internet Protocol Security），是通过对IP协议（互联网协议）的分组进行加密和认证来保护IP协议的网络传输协议族（一些相互关联的协议的集合）。

4 硬件要求

4.1 设备模块要求

4.1.1 显示屏

应可显示字符、汉字、图片、动画等。

可支持多点触控（可选）。

4.1.2 存储器

RAM和Flash的容量均在512MB以上。

4.1.3 证书管理与加密运算模块（安全模块）

证书管理与加密运算模块也可称安全模块。该模块应支持用于操作系统安全、终端与智能终端后台系统间通信链路安全、应用软件安全等方面所需密钥和证书的安全存储和处理，包括但不限于以下几类：

——用于操作系统内核安全验证的证书和公钥；

——用于应用软件安全验证的证书和公钥；

——用于终端与后台系统间通信链路双向认证的证书和密钥。

证书管理与加密运算模块应支持终端应用与后台系统交互过程中对传输数据进行加密所需密钥的安全存储和运算。对银行卡账户密码、磁道信息等数据加密的密钥（PIK、TDK等）应在密码键盘（见本规范4.1.6节所述）中安全存储和运算。

证书管理与加密运算模块至少满足但不限于以下功能要求：

——模块集成在智能终端硬件主板或嵌入在CPU中；

——模块应支持对称密码算法（如：3DES等）和非对称密码算法（如：RSA等）的运算处理。

证书管理与加密运算模块容量大小应确保至少能容纳以下全部内容：

——至少10个证书文件（若证书采用RSA非对称密钥算法，算法私钥长度支持2048位及以上）；

——至少10个3DES密钥或者128位以上长度的AES密钥。

4.1.4 读卡器

4.1.4.1 磁条阅读器

磁条阅读器应能够准确阅读在磁性标准正常范围内的磁道信息，并应同时读取磁条卡的二、三磁道数据，能正确读取2,750奥斯特的高抗磁条卡。凡符合GB/T 14916、GB/T 15120、GB/T 15694-1、GB/T 17552标准的磁条卡都能读取。刷卡方向可采用单向或双向，刷卡速度范围为10厘米/秒～100厘米/秒，磁条读卡器寿命应达到400,000次以上。

注 1：磁条阅读器在读取卡号时应优先通过磁条卡的第二磁道数据读取，如第二磁道数据无法正常读取，可从第一磁道或第三磁道读取，受理方原样上送磁道信息，由发卡方判断合法性。

注 2：当磁条阅读器读取到磁条信息错误的卡时，应提示“重新刷卡”或“按取消键退出”字样。

4.1.4.2 IC 卡阅读器

接触式 IC 卡读卡器是必须具备的，用来接受用户 IC 卡插入并与 IC 卡进行命令数据传递通讯，该读卡器模块包括机械、电气和逻辑协议等部分，见 JR/T 0025.3-2010。

非接触式 IC 卡读卡器属于可选模块，用来接受非接触 IC 卡挥卡，并与非接触 IC 卡进行数据交互，其中不可编程的非接触 IC 卡读写器的相关要求，见 JR/T 0025.11-2010；可编程的非接触 IC 卡读写器的相关要求，见 Q/CUP 019-2010。

如果读卡器有锁卡功能，则应保证在掉电、设备异常或交易取消时能释放卡。

在特殊场合下，非接读卡器应提供稳固的置放平台，确保卡片不会因为滑落或者接触时间过短，导致交易失败。

4.1.5 通信模块

终端通讯应支持以下一种或几种通信方式：

——以太网通讯；

——Wifi；

——3G。

对于以太网方式，应支持RJ45接口标准。对于WiFi方式，应支持802.11b、802.11g和802.11n这三种协议中的一种或多种（协议具体内容见ISO/IEC 8802-11-1999标准）。

4.1.6 密码键盘

密码键盘内部包含具有加密运算处理功能的专用器件，能够完成报文加密、解密、MAC计算和验证。密码键盘应能够安全地存储密钥，防止被读取。应可存储及选用多组密钥。

密码键盘可采用内置或外接形式成为支付终端整体的一部分。如采用外接方式，支持串口或者USB接口。敲击部分至少应具有10个数字键，若干功能键，功能键应至少包括清除和确认两种功能。

密码键盘输出密码至显示屏，不能显示明文，只能显示星号（*）。密码键盘与POS终端之间的信息传送应以密文的形式进行。

密码键盘的使用寿命应保证每键可敲击30万次以上。

密码键盘的更详细要求参见《银联卡受理终端PIN输入设备安全规范》（Q/CUP 007.6-2010），并满足该规范所设定的安全要求。

4.1.7 打印机

打印机选用热敏纸记录式打印机。打印的可显示的ASCII字符或汉字应符合GB5007.1、GB5199、GB13000.1、 GB 18030或GB2312的要求。无故障打印张数不少于50,000张凭证。打印机应具有过热保护功能。打印字迹清晰均匀、字体饱满无形变。打印精度大于203DPI/8点/毫米。

同时支持打印部分转义字符，如表示换行的\n、表示退格的\b、水平制表符\t、垂直制表符\v、回车符\r等等。

4.1.8 指示灯、蜂鸣器

对于具备非接触IC卡读写器的智能终端(包括外接式非接触IC卡读写器和内嵌非接触式IC卡读写模块的模式)，应具备指示灯和蜂鸣器，统一参见《非接触读写器接口规范》（Q/CUP 019-2010）中“6 读写器性能要求”。

4.1.9 语音提示（可选）

智能终端宜有默认语音提示，如在消费扣款后（前）语音提示“XX元”。

4.2 工作环境要求

智能终端一般能应在温度为0℃~40℃，相对湿度为20%~93%的环境下稳定工作。在特殊环境下工作的智能终端应能满足特殊环境的特殊要求。

要求在输入交流电压220V±15%，工作频率50Hz±1%的条件下能正常工作。

4.3 其他要求

4.3.1 电磁特性

本产品必须符合国家标准GB 9254-2008《信息技术设备的无线电骚扰限值和测量方法》和当地相关国家标准。

4.3.2 可靠性

除非特殊部件另有规定，平均无故障工作时间（MTBF）应不低于50，000小时。

4.3.3 其他安全性

智能终端硬件设备的其他安全性要求参考国家标准GB 4943.1-2011《信息技术设备的安全》.

5 安全要求

5.1 操作系统安全

5.1.1 系统内核加载安全

终端应保证操作系统内核加载安全，以防止非法厂商在终端上运行自身定制、不符合本安全标准的操作系统，具体要求包括但不限于：

——应保证操作系统内核加载过程的安全，应保证用于系统内核加载的相关模块在终端出厂后不能被篡改。

——操作系统内核受管理方（银行卡组织及其授权机构，或其他智能终端系统管理运营方及其授权机构）应对操作系统内核进行签名，终端应防止未被签名的内核运行。

5.1.2 系统更新与升级安全

终端应防止用户非法刷机及非法升级。如果系统存在更新或升级需求，应在安全环境下由终端管理机构或其授权机构进行更新或升级。

5.1.3 资源访问权限控制

操作系统应控制应用软件对设备资源的访问权限，包括对系统自身资源的访问和对外部设备的访问。

系统自身资源的访问权限由操作系统通用配置功能完成。

应用软件对外部设备资源的访问权限控制，通过定制操作系统实现。需设置权限控制的资源包括但不限于：

1. 磁条卡读卡器访问权限
2. 接触式IC卡读卡器访问权限
3. 非接IC卡读卡器访问权限
4. 证书管理与加密运算模块（安全模块）访问权限
5. 打印机访问权限
6. 密码键盘访问权限
7. 如存在电子签名设备、扫描设备等外设，应设置相应访问权限

以上资源访问权限均仅授予银联卡支付应用软件及经智能终端及支付系统管理方(银行卡组织及其授权机构、或其他系统管理运营方及其授权机构）认可的特定第三方行业应用软件，且对各资源的授权互相独立，访问权限应分别管理和授予。

5.1.4 应用隔离

运行于智能终端上的应用，应有独立的程序运行空间和私有的文件系统，保证本应用所涉及的数据不被其它应用在非法授权的情形下获得。

5.1.5 应用间数据交换

运行于智能终端系统上的多个应用间可以以进程间通信的方式交换数据，如IPC的方式等。进程间的通信必须保证的数据的安全，防止被其它非法授权的应用窥探。若应用程序需调用其他程序或者系统中的一些敏感程序的组件，应通过设置权限的方式保证系统和应用程序的安全。

5.2 硬件安全

5.2.1 证书管理与加密运算模块

证书管理与加密运算模块应具备的硬件安全功能包括但不限于：

——应提供对称和非对称等通用密码算法的专用计算功能；

——应提供随机数发生功能，以产生随机数辅助证书管理与加密运算模块实现其安全应用，如产生的随机数与敏感信息有关或与智能终端后台系统安全验证有关，则该随机数生成功能应经过评估，以保证产生的随机数无法被预测；

——应具备硬件防攻击机制，保障证书管理与加密运算模块在受到攻击后立即出于不可操作状态，并立即擦除模块中存放的私密信息；

——应具备异常处理机制，包括但不限于：

- 应具备环境异常检测处理机制，包括但不限于温度、电压、时钟频率等检测处理机制；
- 应具备程序执行异常检测处理机制；
- 应具备逻辑模块异常检测处理机制，例如算法模块溢出、寻址空间越界等异常的检测及处理机制；

——证书管理与加密运算模块应提供相应的访问控制策略，对模块的访问应遵循该机制，以防止对模块的非法越权操作；

——应具备相应删除机制，保证敏感数据在使用后立即从存储区域中删除；

——改变设备环境条件或操作条件不会影响证书管理与加密运算模块安全性。

5.2.2 密码键盘及其安全连接

密码键盘自身及其与其他设备共同使用过程中的安全要求，参见《银联卡受理终端安全规范第6部分：PIN输入设备安全规范》（Q/CUP 007.6）。

5.3 应用软件安全

5.3.1 安全开发和维护

开发软件应用应以业界最佳实践为基础，并将信息安全与整个软件开发生命周期相结合。

应保证应用软件安全。软件开发应遵循相应安全编码规则。应防止应用软件代码出现安全漏洞，通常会出现的编码漏洞包括但不限于：

——无效输入

——失效访问控制（例如，用户ID的恶意使用）

——失效的身份认证和会话管理（对于账户凭据和会话Cookie的使用）

——跨站脚本攻击（XSS或CSS）

——不安全存储

——拒绝服务攻击（DoS）

——不安全的配置管理

应用软件补丁应通过充分的评估和测试，应被确定不会与现有的安全配置相冲突。

5.3.2 应用下载、安装和更新

应用软件及相关补丁应通过银行卡组织或其他智能终端系统管理运营方管理或由其授权管理的合法渠道下载。

智能终端应用管理客户端具有安装应用的唯一权限，应用的安装应通过智能终端应用管理客户端并连接应用管理后台系统进行。应通过数字签名等技术手段，使下列应用不能够在终端上安装使用：

——从其他第三方行业应用下载的应用程序；

——通过Micro-SD卡或者其他USB接口设备拷入的应用程序；

——其他非智能终端应用管理客户端途径获得的应用。

在软件安装或更新过程中，应确保所安装或更新的应用软件版本有效，安装或更新过程应在安装包完整、安全的前提下进行。空中方式下载安装或更新客户端支付软件时需要采用安全报文，保证软件传输过程的机密性、完整性。

应用安装程序应通过智能终端应用管理后台进行签名，应用安装前，安装文件应首先通过智能终端应用管理客户端的签名验证。

5.4 数据安全

5.4.1 数据存储安全

在银行卡支付过程中，应保留最少的用户敏感数据，限制数据存储量和保留时间，达到恰好能满足业务、法律和管理规定需要的程度。同时应采取有效手段对敏感数据进行保护，防止信息泄露和被篡改。

禁止在支付结束后存储敏感认证数据，如银行卡磁道信息、卡号、密码、CVN2、有效期等（即使经过加密）。

提交账户信息时，应采用有效手段使PAN不可被非法获取。

如应用需要显示PAN，应参照银联卡POS屏蔽相关管理规定进行显示。

5.4.2 数据传输安全

银联卡支付客户端应用软件与后台系统进行交互时应保证数据传输安全，具体包括：

——在易被攻击者截获、篡改和重定向的网络上传输敏感信息时必须加密；

——使用强壮的加密算法和安全协议，例如安全套接字层（SSL 3.0及以上版本）/传输层安全（TLS 1.0及以上版本）或IP安全协议（IPSEC）来保护敏感数据在开放/公共的网络上的传输；开放/公共网络的例子包括Internet、WiFi、全球移动通信系统（GSM）和通用分组无线业务（GPRS）等；

——以wifi方式进行无线网络传输支付信息时，应使用WAP或WAP2或更高安全性的方式进行；

——终端及后台系统采用双向认证。

6 生产管理要求

密码键盘在生产期间和初始密钥注入之前的安全管理要求参见《银联卡受理终端安全规范第6部分：PIN输入设备安全规范》（QCUP 007.6）。

终端生产期间和密钥与证书注入之前，应保证证书管理与加密运算模块符合安全要求，具体可参考密码键盘的生产管理要求。

7 密钥体系

7.1 对称密钥

交易密钥指《银联卡受理终端安全规范第1部分 销售点终端安全规范》（QCUP 007.1）所述POS终端所使用的密钥。交易密钥分为二级：终端主密钥(TMK)和工作密钥(WK)。

7.1.1 终端主密钥

主密钥用于对工作密钥(WK)进行加密保护，POS中心为每台终端分配唯一的TMK，TMK应至少采用双倍长密钥。TMK必须要有安全保护措施，只能写入并参与运算，不能被读取。TMK应安全存储于密码键盘和智能终端后台系统中。

7.1.2 工作密钥

工作密钥（WK）由终端前置机的加密机产生，在终端每次签到时从POS中心利用TMK加密后下载，并由TMK加密存储。终端工作密钥在下载时必须以密文传送，严禁明文传送。

智能终端使用的工作密钥通常包括用于对个人标识码(PIN)加密的PIK、进行磁道加密的TDK（磁道数据密钥）。其中PIK应安全存储于终端密码键盘中，TDK应安全存储于终端密码键盘和智能终端后台系统中。

7.2 非对称密钥

7.2.1 操作系统内核安全加载的证书和密钥

运行于智能终端之上的操作系统内核受管理方（银行卡组织及其授权机构，或其他智能终端支付系统管理运营方及其授权机构）签名保护。其中涉及的证书和密钥包括：系统内核私钥、系统内核公钥证书、操作系统管理方公钥等。

——操作系统内核应由系统内核私钥签名，操作系统管理方应将该签名数据、系统内核公钥证书（由管理方私钥签名）及签名后的操作系统内核一同发布；

——操作系统管理方公钥存储于证书管理与加密运算模块中，用于验证系统内核公钥证书并获取内核公钥；

——加载操作系统时，应使用内核公钥对签名后的操作系统进行验证，仅当验证通过条件下操作系统才可被成功加载。

7.2.2 系统通信链路安全证书和密钥

运行于智能终端之上的银联卡支付客户端与银联卡支付后台系统间的通信应由管理方（银行卡组织及其授权机构、或其他智能终端系统管理运营方及其授权机构）采用SSL/TLS双向认证机制进行保护，要求智能终端认证后台系统，且后台系统认证智能终端。其中涉及的证书和密钥包括：终端私钥、终端公钥证书、终端管理方公钥、支付后台系统私钥、支付后台系统公钥证书、支付后台系统管理方公钥等。

——终端私钥用于终端向支付后台系统的传输加密，该密钥存储于证书管理与加密运算模块中；

——终端公钥证书（由终端管理方私钥签名）存储于证书管理与加密运算模块中，在建立通信连接时由终端发送给后台系统，后台系统使用管理方公钥对其进行验证并获取终端公钥，并使用该公钥验证终端发送信息的签名；

——支付后台系统私钥用于对后台向终端的传输加密，存储于后台系统；

——支付后台系统公钥证书（由支付后台系统管理方私钥签名）存储于后台系统，在建立通信连接时由后台系统发送给终端，终端使用管理方公钥对其进行验证并获取支付后台系统公钥，并使用该公钥验证后台发送信息的签名。

7.2.3 应用软件安全证书和密钥

运行于智能终端之上的应用应经过管理方（银行卡组织及其授权机构，或其他智能终端系统管理运营方及其授权机构）重签名。其中涉及的证书和密钥包括：应用软件私钥、应用软件公钥证书、应用软件管理方公钥等。

——应用软件应由应用软件私钥签名，应用软件管理方应将该签名数据、应用软件公钥证书（由管理方私钥签名）及签名后的应用软件一同发布；

——应用软件管理方公钥存储于证书管理与加密运算模块中，用于验证应用软件公钥证书并获取应用软件公钥；

——安装应用时，应使用应用软件公钥对签名后的应用软件进行验证，仅当验证通过条件下应用软件才可被成功安装。