ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0120.1—2016

银行卡受理终端安全规范
第1部分:销售点(POS)终端

Security specification for bank card terminals—

Part 1: Point of sale terminal

2016-09-06 发布　　2016-09-06 实施

中国人民银行　发布

目　次

前　言

JR/T 0120—2016《银行卡受理终端安全规范》由以下五个部分组成：

——第1部分：销售点(POS)终端；

——第2部分：受理商户信息系统；

——第3部分：自助终端；

——第4部分：电话支付终端；

——第5部分：PIN输入设备。

本部分按照GB/T 1.1—2009 给出的规则起草。

本部分为《银行卡受理终端安全规范》的第1部分。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位：中国人民银行科技司、中国银联股份有限公司。

本部分起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、中国光大银行、招商银行、中国邮政储蓄银行、中国金融电子化公司、中金金融认证中心有限公司、北京银联金卡科技有限公司、银联商务有限公司、福建联迪商用设备有限公司、飞天诚信科技有限公司、无线网络安全技术国家工程实验室、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、信息产业信息安全测评中心。

本部分主要起草人：李伟、王永红、陆书春、李兴锋、杜宁、陈则栋、曲维民、汤沁莹、王禄禄、吴永强、赵哲、贾铮、周皓、王兰、李伟（中国银联）、吴潇、张志波、潘润红、邬向阳、杨倩、刘运、张晓欢、谭颖、严伟锋、曹宇、俞纹雯、周英斌、夏庆凡、王治纲、王伯铮、于华东、李同勋、冯健诚、代伟、钱菲、李穗申、李石超、顾才泉、侯智勇、张晓琪、高志民、高强裔、李超、高峰、周诗扬、孙茂增、马哲、尚可、胡盖、张俊江、蒋利兵、郭鑫、林眺、于海涛、白艳雷、李琴、宋铮、刘健、董晶晶。

银行卡受理终端安全规范
第1部分：销售点（POS）终端

1 范围

本部分定义了银行卡销售点（POS）终端的安全标准，主要内容包括银行卡特约销售点POS终端（包含智能POS终端）、mPOS终端等的安全要求。

本部分适用于所有对受理银行卡的各类POS终端（包含智能POS终端）、mPOS终端等设备开展的设计、制造、开发等方面。

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 4943.1 信息技术设备 安全 第1部分：通用要求

GB/T 21078.1 银行业务 个人识别码的管理与安全 第1部分：ATM终端和POS系统中联机PIN处理的基本原则和要求

JR/T 0001 银行卡销售点（POS）终端技术规范

JR/T 0002 银行卡自动柜员机（ATM）终端技术规范

JR/T 0025（所有部分） 中国金融集成电路（IC）卡规范

JR/T 0093.6 中国金融移动支付 远程支付应用 第6部分：基于安全单元（SE）的安全服务技术规范

JR/T 0120.5 银行卡受理终端安全规范 第5部分：PIN输入设备

GM/T 0002 SM4分组密码算法

GM/T 0003 SM2椭圆曲线公钥密码算法

GM/T 0004 SM3密码杂凑算法

GM/T 0009 SM2密码算法使用规范

ISO 9564—3 银行个人识别码（PIN）管理和安全 第3部分：在ATM和POS系统中对脱机PIN保护的原理与要求

3 术语和定义

JR/T 0001和JR/T 0002中界定的以及下列术语和定义适用于本文件。

3.1

终端主密钥 terminal master key（TMK）

用于加密终端工作密钥的密钥。

3.2

工作密钥 working key（WK）

PIN加密密钥、MAC计算的密钥和磁道加密密钥，也称为数据密钥。在联机更新的报文中，对工作密钥应用终端主密钥（TMK）加密，形成密文后进行传输，适用于有人值守的小区和便民点、单位办公室和无集中收银的商品批发市场的商用收单场景。

3.3

上位机 upper computer

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。

3.4

mPOS终端 mobile POS

具有银行卡相关信息采集、加密及交易报文处理能力，通过上位机进行商户收银操作并与后台处理系统交互完成交易的专用受理终端。

3.5

智能POS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。

4 符号和缩略语

下列符号和缩略语适用于本文件。

DoS　拒绝服务（Denial of Service）
DUKPT　每交易唯一密钥（Derived Unique Key Per Transaction）
IC　集成电路（Integrated Circuit）
IMEI　国际移动设备标识（International Mobile Equipment Identity）
IP　网络之间互连的协议（Internet Protocol）
MAC　报文鉴别码（Message Authentication Code）
MAK　MAC计算密钥（MAC Key）
PAN　主账号（Primary Account Number）
PIK　PIN加密密钥（PIN Key）
PIN　个人识别码（Personal Identification Number）
POS　销售点终端（Point Of Sale）
SSL　安全套接层（Secure Sockets Layer）
TDK　磁道数据加密密钥（Track Data Key）
TMK　终端主密钥（Terminal Master Key）
TLS　传输层安全（Transport Layer Security）
WK　工作密钥（Working Key）

5 终端硬件要求

终端硬件要求见JR/T 0001。

6 终端软件要求

终端软件要求见JR/T 0001。

7 POS终端安全要求

7.1 基本安全性

POS终端硬件的基本安全性应满足GB 4943.1。

7.2 操作员编号和密码

POS的每个操作员应有独立的编号和密码。操作员编号至少为2位数字或字母，密码至少为4位数字。POS终端应具备操作员密码校验功能，校验失败时禁止交易。

7.3 二级密钥体系

POS终端密钥分为二级：终端主密钥（TMK）和工作密钥（WK）。

7.3.1 终端主密钥

用于对工作密钥（WK）进行加密保护，POS中心为每台POS终端分配唯一的TMK。TMK应要有安全保护措施，只能写入并参与运算，不能被读取。

7.3.2 工作密钥

包括用于对个人标识码（PIN）加密的PIK、进行报文鉴别（MAC）的MAK、进行磁道加密的TDK。工作密钥（WK）由POS前置机的加密机产生，在POS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。POS终端工作密钥在下载时应以密文传送，严禁明文传送。

7.4 安全加密

POS终端应对上送的磁道信息进行加密，加密方式与POS中心约定。

采用安全可控的密码算法，保证POS交易数据的完整性和机密性，应支持SM2、SM3、SM4、RSA、SHA、3DES等。SM算法见GM/T 0002、GM/T 0003、GM/T 0004、GM/T 0009。联机PIN处理的原则和要求见GB/T 21078.1，脱机PIN的处理要求见ISO 9564—3。

PIN的采集加密、MAC计算、磁道加密等敏感信息的加解密应在密码键盘的安全模块中处理。

基于SM2、SM3、SM4、RSA、SHA、3DES算法应用的安全功能方面的要求详见JR/T 0025。

7.5 卡号屏蔽要求

POS终端打印的电子凭条应对卡号进行屏蔽保护（预授权交易卡号、转账交易的转入卡号或电子现金使用时除外），卡号的前六位和后四位正常显示，其余卡号位进行屏蔽，如6222 01** **** ***1 116。

7.6 IC卡的POS终端安全管理

IC卡POS终端安全管理要求参见JR/T 0025。

7.7 数据输入和传递安全

密码键盘等PIN输入设备应满足JR/T 0120.5的安全要求。

磁条阅读器、IC卡读卡器等数据输入和传递设备应满足JR/T 0120.5中相关部分的安全要求。

网络开放协议、IP 和链路层安全要求见 JR/T 0120.5。

7.8 终端防改装要求

POS终端应具备防拆开关、斑马条、mesh电路等软硬件电路防护机制，防止终端被加装非法电路或改造。

8 mPOS 安全要求

8.1 mPOS 安全要求概述

mPOS 应遵循第 7 章中相关安全要求，同时应遵循本章要求。

8.2 mPOS 受理终端安全要求

8.2.1 基础安全要求

受理终端宜实现DUKPT机制或等效的一次一密机制。

8.2.2 终端功能限制

受理终端不应向支付应用软件提供单独、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。

若受理终端向支付应用软件提供MAC计算功能，则应对交易金额、交易类型等交易信息进行强制填充和确认，防止交易信息被篡改后骗取合法MAC。

8.2.3 报文组包功能

受理终端应实现报文组包等关键交易处理逻辑。

8.2.4 传输安全要求

应采用SSL或TLS协议的相关要求，应支持SSL3.0或TLS 1.2及以上协议。如果使用蓝牙接口，应强制使用蓝牙的加密功能。

8.2.5 交易真实性要求

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，保证交易真实性，防止信息伪造和重放攻击。

8.2.6 账户数据保护要求

受理终端应对账户信息进行安全保护。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的加密和解密，在受理终端和后台系统的硬件加密模块之外不应以明文形式出现。终端输出主账号（卡号）信息应遵循卡号屏蔽要求，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应存储敏感数据（即使已经加密），账户信息只用于完成当前合法银行卡交易，不应用于任何其他用途。

8.2.7 交易信息安全要求

受理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。

8.2.8 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，受理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。

8.2.9 安全提示要求

受理终端应提供相关安全提示机制，确保交易过程中的关键环节（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。

8.3 mPOS 支付应用软件安全要求

8.3.1 基础安全要求

支付应用软件应符合JR/T 0093.6客户端软件相关安全要求。

8.3.2 辅助信息要求

支付应用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。

如支付应用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。

8.3.3 软件功能限制

IC卡应用处理内核不应部署于支付应用软件中。

报文组包等关键交易处理逻辑不应由支付应用软件实现。

8.4 mPOS 辅助安全要求

8.4.1 mPOS 使用管理要求

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

收单机构应采取必要的操作人员管理手段对上位机上的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上位机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Root等权限。

收单机构应将mPOS支付应用软件交易功能与对mPOS开放的交易权限保持一致，不应超限开放。支付应用软件支持的交易类型包括消费、消费撤销、退货、余额查询、预授权类交易。

8.4.2 后台处理系统

后台处理系统应配合受理终端、支付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。

后台处理系统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。

8.4.3 防切机转网

收单机构应具有受理终端防切机转网机制。