ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0120.4—2016

银行卡受理终端安全规范
第4部分:电话支付终端

Security specification for bank card terminals—

Part 4: Telephone payment 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4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、潘润红、邬向阳、杨倩、刘运、王炎方、单长胜、黄发国、李伟（中国银联）、张志波、邱俊、李春欢、夏庆凡、谭颖、严伟锋、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、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4部分：电话支付终端

1 范围

本部分规定了受理银行卡的电话支付终端在应遵循JR/T 0120.1要求基础上需额外遵循的安全标准，其中主要内容包括电话支付终端的硬件、软件及安全要求。

本部分适用于所有对受理银行卡（磁条卡或IC卡）的各类电话支付终端设备开展的设计、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/T 2312—1980 信息交换用汉字编码字符集 基本集

GB/T 16649（所有部分） 识别卡 带触点的集成电路卡

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 0120.1 银行卡受理终端安全规范 第1部分：销售点(POS)终端

JR/T 0120.5 银行卡受理终端安全规范 第5部分：PIN输入设备

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

电话支付终端 telephone payment terminal

在传统电话设备基础上，按照标准POS规范发展起来的一种新型终端设备，电话支付终端通过与电话支付中心进行信息交互、由后台定制交易完成基于银行卡的各种业务功能。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。

4 电话支付终端硬件要求

4.1 键盘

键盘应满足 JR/T 0001。其中，关于电话功能的相关键，可根据所提供的功能增加和复用其他键。

4.2 显示屏

显示屏应满足 JR/T 0001。其中，汉字字符集应至少符合国家标准 GB/T 2312 汉字。

4.3 磁条阅读器

磁条阅读器应满足 JR/T 0001。其中，刷卡速度范围为 10 毫米/秒-100 毫米/秒。

4.4 IC 卡阅读器

可选配一个大卡座，符合 GB/T 16649 关于 IC 卡读卡设备的相关规范要求，IC 卡阅读器寿命应达到 IC 卡插拔 100,000 次以上。终端在 IC 卡读卡器插槽附近有一明显标记指示如何插入 IC 卡。如果终端有锁卡功能，则应保证在掉电、设备异常或交易取消时能释放卡。IC 卡阅读器的安全要求见 JR/T 0120.5 的相应部分。

4.5 密码键盘

终端的加密模块应采用内置或外置的密码键盘。密码键盘应符合 JR/T 0120.5 相关要求，并且应具备防拆开关、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。

4.6 打印机（可选）

打印机应满足 JR/T 0001。

4.7 通讯

终端与中心间可采用 FSK（frequency shift keying，频移键控）、HDLC（high level data link control，高速数据链路控制）或 DTMF（dual tone multi-frequency，双音多频）三种有线通讯方式中一种或两种，也可选用无线通讯方式。

无线通讯方式通过 APN 专网接入，关闭漫游功能并具备锁定小区功能，终端在建链报文应上送 SIM 卡 IMSI 号码。

4.8 存储器

除应用程序外，需具备足够的存储空间存放应用信息。

4.9 外设通讯

至少具有一个外设通讯接入口，如 RS232、USB 等方式。若配备其他外设，终端应提供对应参数设置开关。

4.10 电源

电源应满足JR/T 0001。

4.11 对工作环境温湿度的要求

电话支付终端一般应能在温度为0℃～40℃，相对湿度为20%～93%（40℃）的环境下稳定工作，在特殊环境下工作的电话支付终端应能满足特殊环境的特殊要求。

4.12 抗跌落能力

抗跌落能力应满足JR/T 0001。

4.13 可靠性

可靠性应满足JR/T 0001。

5 电话支付终端软件要求

软件要求应满足JR/T 0001。

6 电话支付终端安全要求

6.1 基本安全性

电话支付终端硬件的基本安全性应满足JR/T 0120.5及JR/T 0120.1。

6.2 密钥体系

电话支付终端采用签到模式（见6.3签到模式）。

6.3 签到模式

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)。

6.3.1 密钥加密密钥(KEK)

密钥加密密钥(KEK)应满足JR/T 0120.5及JR/T 0120.1的安全要求。

6.3.2 工作密钥（WK）

工作密钥（WK）应满足JR/T 0120.5及JR/T 0120.1的安全要求。

6.4 MAC 加密

MAC加密应满足JR/T 0120.5的安全要求。

6.5 PIN 加密

PIN加密应满足JR/T 0120.5的安全要求。

6.6 磁道信息加密

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。

6.7 密钥管理与加密算法

密钥管理与加密算法应满足 JR/T 0120.5 的安全要求。

6.8 账户信息安全

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，不应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应满足 JR/T 0120.5 的安全要求，禁止通过重拨等功能获取相关资料。

6.9 终端关联

电话支付终端编号应与用户提供的电话号码（或 IMSI 号码）建立关联，对于关联不匹配的，电话支付中应拒绝该终端发起的所有交易请求。