ICS 35.240.40
A11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXXX—XXXX

中国金融移动支付 受理终端技术要求

China financial mobile payment--Point of interaction technical requirements

（报批稿）

（本稿完成日期：2012 年 10 月 22 日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国人民银行　　发 布

目　　次

前言 II
引言 3
1　范围 4
2　规范性引用文件 4
3　定义和术语 4
4　POS 终端 5
5　ATM 终端 7
6　SE 应用管理终端 7
7　PIN 输入设备 13
附录 A（规范性附录）　抗破坏能力 14

前　　言

本部分按照 GB/T 1.1-2009 给出的规则起草。

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/TC180）归口。

本部分负责起草单位：。

本部分参加起草单位：。

本部分主要起草人：。

引　　言

随着移动支付新业务、新产品、新管理模式的不断涌现，移动支付业务越来越多的应用到生活的方方面面，而良好的移动支付受理环境是移动支付业务发展的一个重要方面和前提条件。移动支付受理终端标准的统一可以有效的推进移动支付各环节的互联互通，降低产业成本，是移动支付受理环境建设的重要措施。

考虑到移动支付涉及面广、业务种类繁杂以及各商业银行和非金融支付机构的终端系统现状，为便于标准的推广，本标准仅对能够受理移动支付业务的终端进行描述，规定终端在受理移动支付业务时所需要的软、硬件要求，并对受理终端的安全性进行约束。对于仍存在不确定性、或未来可能会出现的新型受理终端，在标准后续的修订过程中逐步纳入。

JR/T ××××.×—××××

移动支付 受理终端技术要求

1 范围

本标准定义了移动支付受理终端的硬件、软件和安全等通用技术要求。受理终端包括POS终端、ATM和SE应用管理终端等。

本标准适用于从事移动支付受理终端设计、制造、开发等工作的各相关单位。

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 9254-1998 信息技术设备的无线电骚扰极限值和测量方法（GB 9254—1998，CISPR 22:1997，IDT）

GB/T 17618-1998 信息技术设备抗扰度限值和测量方法（GB/T 17618—1998，CISPR 24:1997，IDT）

GB 4943-2001 信息技术设备（包括电气事务设备）的安全（GB 4943—2001，IEC 60950:1999，EQV）

GB 18030-2005 信息技术 中文编码字符集

JR/T 0001-2009 银行卡销售点（POS）终端规范

JR/T 0002-2009 银行卡自动柜员机（ATM）终端规范

JR/T 0025.6-2010 中国金融集成电路（IC）卡规范 第6部分：借记贷记应用终端规范

JR/T 0025.7-2010 中国金融集成电路（IC）卡规范 第7部分：借记贷记应用安全规范

JR/T 0025.11-2010 中国金融集成电路（IC）卡规范 第11部分：非接触式IC卡通讯规范

GB 5199-2001 信息交换用汉字15X16点阵字模集

GB 17625.1 低压电气及电子设备发出的谐波电流限值（设备每项输入电流≤16A）

GA/T 73-1994 机械防盗锁

GB 13000.1-1993 信息技术 通用多八位编码字符集（UCS） 第1部分：体系结构与基本多文种平面（GB 13000.1—1993，ISO/IEC 10646-1:1993，IDT）

GB 5007.1-2010 信息技术 汉字编码字符集（基本集） 24点阵字型

3 定义和术语

3.1

钓现 fishing

将任何形式的带有一个或多个钩子或其它装置的绳索、金属线或类似物品作用于终端，以非法获取现金。

3.2

暴力取现 forcing

用撬棍、螺丝起子、扳手、或其它类似工具扩大缝隙，或通过打破一个部件或使一个部件变形以获取现金。

3.3

密钥管理 key management

整个密钥生命周期中对密钥和相关参数的操作，包括生成、存储、分发、注入、使用、删除、销毁和存档等。

3.4

攻击 tampering

对设备内部的探查或修改，或通过主动或被动的方法去探查或记录秘密数据的行为。

4 POS 终端

4.1 POS 终端硬件要求

4.1.1 概述

POS终端硬件及性能应符合JR/T 0001-2009第4章和JR/T 0025.6-2010第5章的要求。本标准有要求的，应满足本标准的要求。

4.1.2 POS 终端类型

POS终端按业务需求分为联机终端、脱机终端和联机/脱机终端，对各种POS终端类型的硬件配置要求见表1[1)]。

表1 终端类型的硬件要求

项目号	硬件模块	联机终端	联机/脱机终端	脱机终端
1	显示屏	√	√	√
2	键盘	√	√	Δ
3	密码键盘	√	√	Δ
4	打印机	√	√	Δ
5	非接触式读卡器	√	√	√
6	通信	√	√	Δ
7	存储器	√	√	√
8	计算器	Δ	Δ	Δ

4.1.3 非接触式读卡器

非接触式读卡器可以是与终端集成在一起的内置非接触式读卡器，也可以是与终端通过通讯线连接的外置非接触式读卡器。外置非接触式读卡器可以是独立非接触式读卡器，也可以是与密码键盘集成在一起的非接触式读卡器。

非接触式读卡器应满足JR/T 0025.11-2010的要求。

非接触式读卡器应具备明显的标识，标明非接触读卡区域。如果读卡区域在显示屏下方，可在交易时在显示屏上显示非接触读卡标识。

为保证较长时间的非接触通讯可以正常进行，读卡器应提供使移动支付终端平稳放置的支撑结构。

4.1.4 存储器

终端应当具有足够的存储容量来存放应用程序、密钥、交易数据和其它参数等，并确保在掉电后这些数据不会丢失。要求在保证完成交易功能的前提下，在单一批次内，具有联机能力的终端能够保存300笔以上的交易流水，仅脱机终端要求保存500笔以上。

4.1.5 计算器

内置计算器模块，复用键盘上的数字键和功能键实现加、减、乘、除等基本数学运算。

4.2 POS 终端软件要求

4.2.1 概述

POS终端软件应符合JR/T 0001-2009第5章的要求。本标准有要求的，应满足本标准的要求。

4.2.2 交易模型及流程

POS终端的交易模型和流程应符合JR/T XXXX《中国金融移动支付 近场支付应用 第2部分：交易模型及流程规范》的要求。

4.2.3 交易报文

1) 符号 “√” 表示必备，符号“Δ”表示可选

POS终端的交易报文应符合JR/T XXXX《中国金融移动支付 近场支付应用 第3部分：报文结构及要素》第5章的要求。

4.3 POS终端安全要求

4.3.1 概述

POS终端的安全应符合JR/T 0001-2009第6章和JR/T 0025.7-2010第9章的要求。本标准有要求的，应满足本标准的要求。

4.3.2 PIN输入安全

应符合第7章PIN输入设备要求。

5 ATM终端

5.1 ATM终端硬件要求

5.1.1 概述

ATM硬件及性能应符合JR/T 0002-2009第4章和JR/T 0025.6-2010第5章的要求。本标准有要求的，应满足本标准的要求。

5.1.2 非接触式读卡器

非接触式读卡模块应满足JR/T 0025.11-2010的要求，宜采用内嵌式模块。

非接触式读卡模块应具备明显的标识，标明非接触读卡区域。为保证较长时间的非接触通讯可以正常进行，非接触式读卡模块可提供使移动支付终端平稳放置的支撑结构。

5.1.3 密码键盘

ATM终端的密码键盘采用加密PIN键盘（EPP）来实现，PIN键盘包含一个内嵌的密码模块，该模块实施PIN加密和密钥管理的任务。EPP的密码模块（CM）通常还提供其他密码加密服务，比如报文加密和报文鉴别。应符合ISO 8731-1、ISO 13491-1、ISO 9564-2、ISO 11568、ANSI X9.8-1995等标准。

5.2 ATM终端软件要求

5.2.1 概述

ATM终端软件应符合JR/T 0002-2009第5章的要求。本标准有要求的，应满足本标准的要求。

5.2.2 交易模型及流程

ATM终端的交易模型和流程应符合JR/T XXXX《中国金融移动支付 近场支付应用 第2部分：交易模型及流程规范》的要求。

5.2.3 交易报文

ATM终端的交易报文应符合JR/T XXXX《中国金融移动支付 近场支付应用 第3部分：报文结构及要素》第5章的要求。

5.3 ATM终端安全要求

5.3.1 概述

ATM终端的安全应符合JR/T 0002-2009第6章和JR/T 0025.7-2010第9章的要求。本标准有要求的，应满足本标准的要求。

5.3.2 PIN输入安全

应符合第7章PIN输入设备要求。

6 SE应用管理终端

6.1 概述

SE应用管理终端是专门用于管理客户端SE应用的终端，一般布放在特定的场合，提供用户对客户端SE应用进行个人化、下载、查询、同步等功能。SE应用管理终端与TSM平台连接，在硬件上可以是POS终端形态、自助终端形态或其他类型设备形态。

6.2 SE 应用管理终端硬件要求

6.2.1 SE 应用管理终端（POS 形态）硬件要求

6.2.1.1 概述

SE应用管理终端（POS形态）硬件及性能应符合JR/T 0001-2009第4章和JR/T 0025.6-2010第5章的要求。本标准有要求的，应满足本标准的要求。

6.2.1.2 显示屏

应可显示ASCII可视字符，汉字应支持GB 5007.1-2010、GB 5199-2001、GB 13000.1-1993或GB 18030-2005的要求。应具有4行或4行以上英文和中文显示功能，其中每行显示不少于16个英文字母、数字和符号，或显示不少于8个汉字。终端的液晶显示屏对比度宜可调节或带背光功能。可具备图形显示能力。

6.2.1.3 键盘

应提供0～9的十进制数字型字符及若干功能键的输入，应能够输入字母。键盘使用寿命应达到每键可敲击300,000次以上。如果采用了带颜色的命令键，宜适用下面的颜色分配，命令键颜色：确认－绿色；取消－红色；清除－黄色。

6.2.1.4 密码键盘

SE应用管理终端（POS形态）应配有密码键盘，可以是与终端集成在一起的内置密码键盘，也可以是与终端通过通讯线连接的外置密码键盘。

密码键盘内部应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；独立密码键盘至少要具有一行数字/字母显示屏。键盘使用寿命应达到每键可敲击300,000次以上。

交易金额需显示在密码键盘的显示屏上。持卡人键入密码时，密码键盘的显示屏上不能显示明文，只能显示“*”。密码键盘与POS终端之间的关键数据传送应以密文的形式进行，如下载主密钥。

6.2.1.5 非接触式读卡器

非接触式读卡器可以是与终端集成在一起的内置非接触式读卡器，也可以是与终端通过通讯线连接的外置非接触式读卡器。外置非接触式读卡器可以是独立非接触式读卡器，也可以是与密码键盘集成在一起的非接触式读卡器。

非接触式读卡器应满足JR/T 0025.11-2010的要求。

非接触式读卡器应具备明显的标识，标明非接触读卡区域。如果读卡区域在显示屏下方，可在交易时在显示屏上显示非接触读卡标识。

为保证较长时间的非接触通讯可以正常进行，读卡器可提供使移动支付终端平稳放置的支撑结构。

6.2.1.6 打印机

打印机可选用点阵击打式或热敏纸记录式打印机，可内置或外接。打印应支持ASCII可视字符，汉字应支持GB5007.1-2010、GB 5199-2001、GB 13000.1-1993或GB 18030-2005的要求。无故障打印张数不少于50,000张凭证。打印机走纸定位应准确，点阵击打式打印机应至少能打印3联压感复写凭证。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。

6.2.1.7 存储器

终端应当具有足够的存储容量来存放应用程序、密钥、交易数据和其它参数等，并确保在掉电后这些数据不会丢失。要求在保证完成交易功能的前提下，在单一批次内，终端能够保存300笔以上的交易流水。

6.2.1.8 通讯端口

SE应用管理终端（POS形态）应以联机方式与TSM平台进行通讯，通讯端口应支持以下全部或部分类型的通讯方式：

—— 串口通讯；
—— MODEM 通讯；
—— 红外通讯；
—— 无线通讯；
—— 以太网通讯；
—— 其他。

6.2.2 SE 应用管理终端（自助终端形态）硬件要求

6.2.2.1 概述

SE应用管理终端（自助终端形态）硬件应符合GB/T 23647-2009第4章的要求。本规范有要求的，并符合本规范要求。

6.2.2.2 硬件设计原则

硬件设计应遵循以下原则：

——SE 应用管理终端（自助终端形态）应用在不同的场合时应分别具备防火、防盗、防尘、防淋、防震、防暴等要求，保证人身安全；
——配置的密封装置及门锁应耐久、安全、可靠，应符合 GA/T 73-1994 的要求，对异常情况有报警及日志记录功能；
——硬件系统和各模块单元的逻辑设计应尽量采用统一校验等技术，并留有适当的逻辑余量；
——硬件系统应具有一定的自检功能；
——框架和机柜应有一定的刚度和强度，以防止由于空间变动、部件变松或移位造成的全部或部分损坏，并应防止和减少部件发生火灾、电冲击和人身伤害的可能性；
——外形应具备人性化特点，客户操作应感到舒适方便，并应具备人文特征；
——安全模块需遵循严格的密钥机制，保证持卡人个人信息、PIN 等账户信息的安全。

6.2.2.3 外观和结构

SE应用管理终端（自助终端形态）的外观和结构应满足以下条件：

——SE 应用管理终端（自助终端形态）的外型结构尺寸由产品规范规定；
——SE 应用管理终端（自助终端形态）表面不应有明显的凹痕、划伤、裂缝、变形和污染等，表面涂镀层应均匀，不应起泡、龟裂、脱落和磨损，金属零部件不应有锈蚀及其他机械损伤；
——SE 应用管理终端（自助终端形态）的零部件应紧固无松动，键盘、开关及其他活动部件的动作应灵活可靠。

6.2.2.4 触摸屏输入

触摸反应时间≤20ms；透光率≥95%；单点触摸大于或等于3500万次的使用寿命（正常情况下使用）。

6.2.2.5 密码键盘

SE应用管理终端（自助终端形态）的密码键盘采用加密PIN键盘（EPP）来实现，PIN键盘包含一个内嵌的密码模块，该模块实施PIN加密和密钥管理的任务。为了便利期间，EPP的密码模块（CM）通常还提供其他密码加密服务，比如报文加密和报文鉴别。应符合ISO 8731-1、ISO 13491-1、ISO 9564-2、ISO 11568、ANSI X9.8-1995等标准。

6.2.2.6 非接触式读卡模块

非接触式读卡模块应满足JR/T 0025.11-2010的要求,宜采用内嵌式模块。

非接触式读卡模块应具备明显的标识，标明非接触读卡区域。为保证较长时间的非接触通讯可以正常进行，非接触式读卡模块可提供使移动支付终端平稳放置的支撑结构。

6.2.2.7 通讯端口

SE应用管理终端（自助终端形态）应以联机方式与TSM平台进行通讯，通讯端口应支持以下全部或部分类型的通讯方式：

—— 串口通讯；
—— MODEM 通讯；
—— 红外通讯；
—— 无线通讯；
—— 以太网通讯；
—— 其他。

6.2.2.8 电气安全

SE应用管理终端（自助终端形态）的电气安全要求应符合GB 4943-2001的有关规定。

6.2.2.9 抗破坏能力

SE 应用管理终端（自助终端形态）的抗破坏能力应满足附录 A 的有关要求。

6.2.2.10 抗破坏报警

SE应用管理终端（自助终端形态）遇到非操作员、非管理员开启机柜或遇到暴力攻击等非正常使用时，应能报警并有记录。

6.2.2.11 电磁兼容性

6.2.2.11.1 无线电骚扰限值

SE应用管理终端（自助终端形态）的无线电骚扰限值应符合GB 9254-1998的规定。在产品规范中应明确规定选用A级或B级所规定的无线电骚扰限值。

6.2.2.11.2 抗扰度限值

SE应用管理终端（自助终端形态）的抗扰度限值应符合GB/T 17618-1998的规定。

6.2.2.11.3 谐波电流限值

SE应用管理终端（自助终端形态）的谐波电流限值应符合GB 17625.1-2003的有关规定。

6.2.2.12 环境条件

气候环境适应性、盐雾环境、流动混合气体腐蚀、模拟地面上的太阳辐射等具体的要求由产品规范规定。

6.2.2.13 其他

SE应用管理终端（自助终端形态）其他部件的具体指标由产品规范规定，但性能应确保SE应用管理终端功能的实现。

6.3 SE 应用管理终端软件要求

6.3.1 系统软件要求

应具有系统初始化，对软件、硬件的自检及报警功能，具备断电保护功能，并方便应用程序的加载和参数设定。

6.3.2 二次开发平台

提供高级语言（如C语言）开发环境，提供二次开发专用接口，并提供应用模块，具备应用程序的调试和测试环境。

6.3.3 模块化结构

支持模块化结构设计，软件应封装成几个相对独立、性能稳定的模块，供应用开发者使用。

6.3.4 功能模块

6.3.4.1 概述

SE应用管理终端功能应包括以下全部或部分功能。

6.3.4.2 自检

SE应用管理终端开机后应对硬件状态进行检测和报警。

6.3.4.3 操作员签到

操作员开机后，键入操作员代码和密码，SE应用管理终端验证操作员的合法性。签到成功后操作员可对SE应用管理终端进行操作。

6.3.4.4 终端签到

SE应用管理终端与TSM平台签到采用联机方式，签到成功后才允许做其他交易。

6.3.4.5 终端签退

SE应用管理终端可以具备签退功能，签退后的终端应显示签到提示。

6.3.4.6 应用下载

通过TSM平台将应用程序通过SE应用管理终端发送并安装到移动支付终端SE内。

6.3.4.7 应用个人化

通过SE应用管理终端进行移动支付终端SE应用个人化。

6.3.4.8 应用列表查询

通过SE应用管理终端查询移动支付终端SE应用列表。

6.3.4.9 应用详细查询

通过SE应用管理终端查询移动支付终端SE应用信息。

6.3.4.10 应用同步

通过SE应用管理终端将移动支付终端上的SE应用和相关状态上送到系统。

6.3.4.11 应用删除

通过SE应用管理终端删除移动支付终端上的指定SE应用。

6.3.4.12 应用锁定

通过SE应用管理终端对移动支付终端的SE应用进行锁定。

6.3.4.13 应用解锁

通过SE应用管理终端对移动支付终端锁定的SE应用进行解锁。

6.3.4.14 应用远程管理同步

通过SE应用管理终端对移动支付终端远程设定的SE应用进行同步。

6.3.4.15 SE 激活

通过SE应用管理终端对移动支付终端的SE进行激活。

6.3.4.16 SE 锁定

通过SE应用管理终端对移动支付终端的SE进行锁定。

6.3.4.17 SE 终止

通过SE应用管理终端对移动支付终端的SE进行终止使用。

6.3.4.18 安全域锁定

通过SE应用管理终端对移动支付终端的安全域进行锁定。

6.3.4.19 安全域解锁

通过SE应用管理终端对移动支付终端锁定的安全域进行锁定。

6.3.4.20 安全域终止

通过SE应用管理终端对移动支付终端的安全域进行终止使用。

6.3.5 交易报文

SE应用管理终端的交易报文应符合JR/T XXXX《中国金融移动支付 近场支付应用 第3部分：报文结构及要素》第7章的要求。

6.4 SE 应用管理终端安全要求

6.4.1 SE 应用管理终端安全管理

6.4.1.1 自检

SE应用管理终端开机后应对硬件状态进行检测和报警。自检结束后自动进入工作状态。在工作状态中，操作员也可以通过选择功能设置对SE应用管理终端进行自检。自检完毕返回工作状态。

6.4.2 SE 应用管理终端（POS 形态）集成安全要求

6.4.2.1 配置管理

任何依据该规范对设备集成到密码输入终端进行安全性评估时，必须明确定义其物理和逻辑安全界定，如PIN输入和读卡器各自的功能。

6.4.2.2 PIN 输入功能集成

——应保证已经通过认证的安全器件在集成到 PIN 输入设备时，不降低整个设备的保护级别；
——对密码输入器的密码输入区域和其周围区域进行设计或改造时，应保证不会增加密码输入器受攻击的风险；
——终端在调用密码键盘执行 PIN 输入操作的时候，应遵循以下的要求：

- 终端上如果有消费金额的提示及输入 PIN 的提示，则这两个提示要明显区别；
- 终端在进入到输入 PIN 的界面之后不能再允许输入其它非 PIN 数据；
- 当终端进入到输入 PIN 的界面后，之前输入的金额部分不能再有修改的可能。以防止用户在输入 PIN 的过程中误操作到修改金额部分而泄露 PIN；
- 当终端进入到输入 PIN 操作阶段，终端上应该禁止进行其它和 PIN 输入无关的人机交互的操作（例如查看电话本），另外，如果此时发生应用切换操作，或者把显示屏的焦点从 PIN 输入界面移开，终端必须强制退出当前的 PIN 输入操作，并且该次 PIN 输入操作按失败处理；
- 当进行 PIN 输入提示的时候，终端只能接受诸如“Yes,‖－OK,‖－Cancel,‖or－No”这些控制字符。

6.4.2.3 SE 应用管理终端（POS 形态）的集成

——密码输入终端将已认证的安全设备进行物理和逻辑集成时，应确保不引入新的攻击途径；
——密码输入终端应具有防止偷取支付卡机制（Lebanese loop attack 黎巴嫩环攻击）；
——应保证在同一个设备中，安全器件与非安全组件之间要有比较清晰的逻辑和物理隔离；
——在应用执行过程中，显示给持卡人的动态信息和终端操作状态强制保持一致性。如果接收到来自外部设备更改持卡人动态显示信息和操作状态的命令，应保证该命令已被密码授权校验通过；
——PIN 输入设备应保证只具有一个支付卡密码输入接口，例如一个键盘等。如果有其他可用于 PIN 输入接口，应限制该端口密码输入的使用，例如无有效数字键、输入的数字不可用。

6.4.2.4 设备移除的安全要求

——终端应符合 7.2.10 的要求；
——供应商应对文档持续的维护更新，以保证终端集成使用者了解如何保护系统，对非法移除加以防止；
——对于嵌入式设备，应准确按照嵌入设备厂商提供的文档对系统加以保护，防止非法移除。

6.4.3 SE 应用管理终端（自助终端形态）逻辑安全

6.4.3.1 非 PIN 数据输入

如果SE应用管理终端的密码键盘需要输入非PIN数据，那么至少要满足以下条件的一个：

——提示信息由加密单元控制；

应满足7.2.9.1要求。

——改变用户界面提示攻击可能性分析；

在未授权情况下，改变非PIN数据输入时显示的提示内容危及PIN安全（例如：当输出信息不加密时提示输入PIN）应满足相关要求。

——安全模式。

SE应用管理终端必须确保持卡人可见信息与操作状态之间的关联关系。

6.4.3.2 多应用

如果SE应用管理终端支持多个应用程序，则它必须要能够将这些程序分离开来。一个应用程序不能干扰或篡改另外一个应用程序或SE应用管理终端的操作系统，包括修改属于另外一个程序的数据对象。

6.4.3.3 操作系统

SE应用管理终端操作系统只能包含设计应用用途所必需的零部件和服务。必须以最少的特权来配置和运行。

6.4.3.4 单一的 PIN 数据接口

SE应用管理终端只能通过一个单独的接口接收PIN数据，如果另外有一个键盘，必须阻止通过这个接口接收PIN数据。

6.4.4 传输报文加密

SE应用管理终端与TSM之间的报文应采用对称密钥进行加密传输或进行数字签名。

6.4.5 交易密钥管理

6.4.5.1 二级密钥体系

终端密钥分为二级：终端主密钥(TMK)和工作密钥(WK)。

6.4.5.2 终端主密钥(TMK)

用于对工作密钥(WK)进行加密保护，每台终端与 TSM 平台共享唯一的TMK。

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。

6.4.5.3 工作密钥（WK）

分为用于对个人标识码(PIN)加密的PIK以及进行报文鉴别(MAC)的MAK。

由TSM平台的加密机产生，在终端每次签到时从TSM平台利用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。

6.4.5.4 终端 MAC 的算法

当SE应用管理终端采用ISO8583报文格式时，从报文消息类型（MTI）到63域之间的部分构成MAC ELEMEMENT BLOCK （MAB），采用ECB工作方式，加密结果为128位的MAC。如采用XML报文格式，由TSM平台自行定义。

6.4.5.5 PIN 加密

PIN加密采用ANSI X9.8 Format（带主账号信息）。

加密算法采用双倍长密钥算法。

6.4.6 PIN 输入安全

应符合第7章PIN输入设备的要求。

7 PIN输入设备

本部分适用于所有移动支付的受理终端完成PIN输入的设备或模块（如：密码键盘）。

PIN输入设备应具备一定的物理、逻辑安全机制，如应具备入侵检测机制，防止PIN输入过程被监听，可安全地存储敏感信息，具备完整的密钥体系等。

在PIN输入设备和非接触式读卡器间传输PIN相关信息时，应有效地保护所传输的数据。

PIN输入设备应满足金融行业相关规范的要求。

附 录 A
（规范性附录）
抗破坏能力

A.1 目的

1) 试验的目的是检验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。
2) 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。
3) 除了设陷取现，成功的攻击应该在特定的时间内，移走自助终端内至少 10%的现金，或将现金暴露在外，以致它们都可以被移走。
4) 设陷取现必须成功地进行三次取现而不被发现或不打断自助终端的运行。设陷取现可以在操作中进行调节。
5) 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

1) 一次试验可选用多种攻击方式，每种攻击可进行 30min。
1) 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

1) 钓现、暴力取现、设陷取现是由自助终端的设计所决定的。
2) 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

1) 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。

2) 样机的门间隙应代表以后生产产品的最大门间隙。
3) 提供附有材料规格的完整结构图。
4) 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。
5) 如果所用材料不是钢，则不需提供这些样品。

A.3.2 工具

1) 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。
2) 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。
3) 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.2.3中所述的要求为准。

A.3.4 方法

1) 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。
2) 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。
3) 锁舌——通过门上的开口切断或移动主要锁舌使其脱离连接。
4) 切断锁舌——刺穿门的旁柱并切断主要锁舌。
5) 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。
6) 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。
7) 撬开或劈开门——用楔子、凿子和撬刺破或打开门以取走现金。
8) 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。
9) 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