ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0098.4—2012

中国金融移动支付 检测规范 第4部分：安全单元（SE）应用管理终端

China financial mobile payment—Test specifications—
Part 4: Secure element (SE) application manage terminal

2012-12-12 发布 2012-12-12 实施

中国人民银行 发布

目　　次

前　言

《中国金融移动支付 检测规范》标准由以下8部分构成：

——第1部分：移动终端非接触式接口；

——第2部分：安全芯片；

——第3部分：客户端软件；

——第4部分：安全单元（SE）应用管理终端；

——第5部分：安全单元（SE）嵌入式软件安全；

——第6部分：业务系统；

——第7部分：可信服务管理系统；

——第8部分：个人信息保护。

本部分为该标准的第4部分。

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：中国人民银行科技司、中国人民银行金融信息中心、中国金融电子化公司。

本部分参加起草单位：北京银联金卡科技有限公司（银行卡检测中心）、中金国盛认证中心、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）、上海市信息安全测评认证中心、信息产业信息安全测评中心、北京软件产品质量检测检验中心、中钞信用卡产业发展有限公司、上海华虹集成电路有限责任公司、上海复旦微电子股份有限公司、东信和平智能卡股份有限公司、大唐微电子技术有限公司、武汉天喻信息产业股份有限公司、恩智浦半导体有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、张雯华、刘力慷、刘志刚、聂丽琴、李晓、尚可、郭栋、熊文韬、宋铮、李宏达、王冠华、胡一鸣、张晓、平庆瑞、张志茂、陈君、彭美玲、李微、陈吉、程恒。

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。安全可靠的SE应用管理终端是移动支付业务发展的基础和保障。

本部分在收集、分析和评估SE应用管理终端风险的基础上，对其硬件、软件和安全要求的检测要求进行了规定。

中国金融移动支付　检测规范
第4部分：安全单元（SE）应用管理终端

1　范围

本部分定义了SE应用管理终端的硬件、软件和安全等的检测要求。SE应用管理终端的交易模型及流程、交易报文的检测不在本部分进行规定。

本部分适用于从事移动支付终端检测工作的各相关单位。

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 4943　信息技术设备（包括电气事务设备）的安全

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

GB 5199　信息交换用汉字15X16点阵字模集

GB 9254　信息技术设备的无线电骚扰极限值和测量方法

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 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）

GB 18030　信息技术 中文编码字符集

GB/T 17618　信息技术设备抗扰度限值和测量方法

JR/T 0025.11　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

GA/T 73　机械防盗锁

GB 228-1987　金属拉伸实验方法

3　术语和定义

下列术语和定义适用于本文件。

3.1

终端主密钥（TMK）　terminal master key（TMK）

用于加密终端工作密钥的密钥。

3.2

工作密钥（WK）　working key （WK）

通常指PIN加密密钥和MAC计算的密钥。工作密钥必须经常更新。在联机更新的报文中对工作密钥必须用密钥加密密钥（KEK）加密，形成密文后进行传输。

3.3

密钥加密密钥（KEK）　key encryption key（KEK）

终端工作时对工作密钥进行加密的密钥，由银行人员设置并直接保存在系统硬件中，只能使用，不能读取，该密钥必须与加密算法放在同一加密芯片里。

3.4

身份鉴别　authentication

用来验证身份或证实信息完整性的过程。

3.5

敏感数据（信息） sensitive data（information）

必须防止被非法泄露、修改或破坏的数据，特别是明文PIN和加密密钥以及包含设计特点、状态信息的数据。

3.6

密码键盘（EPP） encrypting PIN pad（EPP）

用于自动PIN受理装置中安全输入PIN码和加密的装置。EPP可以带有一个内置显示屏或读卡器，或者采用自动装置中安装的外部显示屏或读卡器。EPP具有明确的物理和逻辑界限以及一个防篡改功能或者能够显示篡改迹象的外壳。

3.7

物理安全性 physical security

设备在物理构造上抵御攻击的能力。

3.8

双重控制 dual control

通过两个以上的独立实体协同工作去保护敏感功能或信息的机制。

3.9

固件 firmware

在PIN输入设备内部与设备安全性相关所有程序代码称为固件，固件必须符合本规范的安全要求。

3.10

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。

3.11

知识分割 knowledge split

一种把消息分割成许多碎片的方法。分割后每一片所代表的信息足够小，但是把这些碎片重新组合在一起就能重现信息。

4 测试条件

默认环境条件（温度、湿度等）是指常温20±℃，相对湿度在20%-80%RH之间。如无特殊说明，后续案例均采用此环境条件。

5 SE 应用管理终端硬件要求检测

5.1 SE 应用管理终端（POS 形态）硬件要求测试

5.1.1 显示屏

检测目的：验证显示屏符合规范要求。

测试过程：检查厂商提供的资料并验证。

执行正常交易，观察显示屏。

调整无背光的显示屏的对比度。

通过标准：可显示 ASCII 可视字符，汉字支持 GB 5007.1-2010、GB 5199、GB 13000.1-1993 或 GB 18030 的要求。

具有 2 行或 2 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可调节或带背光功能。

5.1.2 键盘

检测目的：验证键盘符合规范要求。

测试过程：检查键盘是否具有 10 个数字键和清除、取消、确认键。

执行正常交易，检测按键的功能，观察按键的颜色。

通过标准：提供 0～9 的十进制数字型字符及若干功能键的输入，能够输入字母。按键颜色符合要求。

5.1.3 密码键盘

检测目的：验证密码键盘符合规范要求。

测试过程：检查密码键盘是否具有 10 个数字键和清除、确认键。

检查独立密码键盘的显示屏。

通过标准：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。

密码键盘能够安全地存储密钥。

可存储及选用多组密钥。

密码键盘至少具有 10 个数字键，若干功能键，功能键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。

交易金额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“*”。

密码键盘与终端之间的关键数据传送以密文的形式进行。

5.1.4 非接触式读卡器

检测目的：验证非接触式读卡器符合要求。

测试过程：检查非接触式读卡器是否具有通讯及电特性。

设计验证场景。

通过标准：非接触式读卡器满足 JR/T 0025.11 的相关要求。

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

读卡器可提供使移动支付终端平稳放置的支撑结构。

5.1.5 打印机

检测目的：验证打印机符合规范要求。

测试过程：检查打印机并进行打印操作。

通过标准：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。

打印支持 ASCII 可视字符，汉字支持 GB5007.1-2010、GB 5199、GB 13000.1-1993 或 GB 18030 的要求。

打印机走纸定位应准确，点阵击打式打印机至少能打印 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。

5.1.6 存储器

检测目的：验证存储器满足规范要求。

测试过程：设计场景，执行交易。

通过标准：终端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。

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。

5.1.7 通讯端口

检测目的：验证通讯接口符合规范要求。

测试过程：检查厂商提供的材料并实际验证终端采用的通讯接口。

验证通讯接口有效性。

通过标准：终端采用以下全部或部分通讯接口：串口通讯、MODEM 通讯、红外通讯、无线通讯、以太网通讯。

5.1.8 电源

检测项目：验证电源符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：交流供电的终端要求在输入交流电压 220V±22V，工作频率 50Hz±1Hz 的条件下能正常工作。

5.1.9 硬件安全性

检测项目：验证硬件安全性符合规范要求。
测试过程：检查厂商提供的材料。
按照 GB 4943 设计场景进行检测。
通过标准：终端硬件的安全性符合 GB 4943 的要求。

5.1.10 电磁兼容性

5.1.10.1 无线电干扰极限值

检测项目：验证无线电干扰极限值符合规范要求。
测试过程：检查厂商提供的材料。
按照 GB 9254 相关规定设计案例对产品进行检测。
通过标准：无线电干扰极限值符合 GB 9254 中的 B 级 ITE 规定。

5.1.10.2 抗扰度限值

检测项目：验证抗扰度限值符合规范要求。
测试过程：检查厂商提供的材料。
GB/T 17618 相关要求设计案例对产品进行检测。
通过标准：产品的抗扰度限值符合 GB/T 17618。

5.1.11 对工作环境温湿度的要求

检测项目：验证终端在规范的温湿度中能正常工作。
测试过程：检查厂商提供的材料。
在规定的温湿度范围中对产品进行检测。
通过标准：终端终端能在温度为 0°C～40°C，相对湿度为 20%～93%（40°C）的环境下稳定工作。

5.1.12 抗跌落能力

检测项目：验证抗跌落能力符合规范要求。
测试过程：检查厂商提供的材料。
进行跌落测试。
通过标准：在初速度为 0 的条件下，关机的终端从 250mm 高处以底面向下跌落方式做自由落体运动跌落到水泥地面 2 次，外壳无明显破损，开机后各部分可正常工作。

5.1.13 可靠性

检测项目：验证可靠性符合规范要求。
测试过程：检查厂商提供的材料。
通过标准：在常温（25°C）和稳定标称 220V 电压下的 m1 值（MTBF 的不可接受值）不得低于 10,000 小时。

5.2 SE 应用管理终端（自助终端形态）硬件要求检测

5.2.1 硬件设计原则

检测目的：验证终端硬件设计符合规范要求。
测试过程：检查厂商提供的材料。
通过标准：SE 应用管理终端（自助终端形态）应用在不同的场合时分别具备防火、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，符合 GA/T 73 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采用统一校验等技术，并留有适当的逻辑余量。
硬件系统具有一定的自检功能。
框架和机柜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。
安全单元需遵循严格的密钥机制，保证持卡人磁道信息、PIN 等账户信息的安全。

5.2.2 外观和结构

检测项目：验证外观和结构符合规范要求。
测试过程：检查厂商提供的材料。
检查设备的外观。
通过标准：SE 应用管理终端表面无明显的凹痕、划伤、裂缝、变形和污染等，表面涂镀层应均匀，无起泡、龟裂、脱落和磨损，金属零部件无锈蚀及其他机械损伤。
SE 应用管理终端的零部件紧固无松动，键盘、开关及其他活动部件的动作灵活可靠。

5.2.3 触摸屏输入

检测项目：验证触摸屏符合规范要求。
测试过程：检查厂商提供的材料。
通过标准：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。

5.2.4 密码键盘

检测项目：验证密码键盘符合规范要求。
测试过程：检查厂商提供的材料。
通过标准：符合第 8 章的要求。

5.2.5 非接触式读卡模块

检测目的：验证非接触式读卡器符合要求。
测试过程：检查非接触式读卡器是否具有通讯及电特性。
设计验证场景。
通过标准：非接触式读卡器应满足 JR/T 0025.11 的相关要求。
非接触式读卡器具备明显的标识，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。
读卡器可提供使移动支付终端平稳放置的支撑结构。

5.2.6 通讯端口

检测目的：验证通讯接口符合规范要求。
测试过程：检查厂商提供的材料并实际验证终端采用的通讯接口。
验证通讯接口有效性。
通过标准：终端采用以下全部或部分通讯接口：串口通讯、MODEM 通讯、红外通讯、无线通讯、以太网通讯。

5.2.7 抗破坏能力

检测目的：验证 SE 应用管理终端设备的抗破坏能力，保证在一定的成本下，设备不会被入侵。
测试过程：检查厂商提供的材料。
设计案例对设备进行检测。

通过标准：SE 应用管理终端的抗破坏能力满足附录 A 的有关要求。

5.2.8 抗破坏报警

检测目的：验证 SE 应用管理终端设备在遇见暴力攻击时，能够及时报警并有记录。
测试过程：检查厂商提供的材料。
设计案例对设备进行检测。
通过标准：SE 应用管理终端设备在遇见暴力攻击时，能够及时报警并有记录。

5.2.9 电磁兼容性

5.2.9.1 无线电骚扰限值

检测项目：验证无线电骚扰值符合规范要求。
测试过程：检查厂商提供的材料。
设计场景进行检测。
通过标准：SE 应用管理终端的无线电骚扰限值符合 GB 9254 的规定。

5.2.9.2 抗扰度限值

检测项目：验证抗扰度限值符合规范要求。
测试过程：检查厂商提供的材料。
设计场景进行检测。
通过标准：SE 应用管理终端的抗扰度限值符合 GB/T 17618 的规定。

5.2.9.3 谐波电流限值

检测项目：验证符合规范要求。
测试过程：检查厂商提供的材料。
通过标准：SE 应用管理终端的谐波电流限值符合 GB 17625.1-2003 的有关规定。

6 SE 应用管理终端软件要求检测

6.1 系统软件要求

检测目的：验证终端系统软件符合规范要求。
测试过程：进行系统软件测试，检查软件自检、报警和断电保护情况。
通过标准：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。

6.2 二次开发平台

检测目的：验证终端二次开发平台符合规范要求。
测试过程：进行二次开发测试，检查终端对二次开发的支持情况。
通过标准：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 模块化结构

检测目的：验证终端模块化结构符合规范要求。
测试过程：检查模块设计支持应用开发者的情况。
通过标准：支持模块化结构设计，软件应封装成几个功能相对独立、性能稳定的模块，供应用开发者使用。

6.4 功能模块

6.4.1 自检

检测目的：验证终端自检符合要求。
测试过程：检查厂商提供的资料并验证。
验证终端自检功能。

通过标准：开机后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。
工作状态中，操作员可通过选择功能设置对脱机终端进行自检。

6.4.2 操作员签到

检测项目：验证操作员签到功能符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

6.4.3 终端签到

检测项目：验证终端签到符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

6.4.4 终端签退

检测项目：验证终端签退符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

6.4.5 应用下载

检测项目：验证应用下载符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

6.4.6 应用个人化

检测项目：验证应用个人化符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端可进行移动支付终端 SE 应用个人化。

6.4.7 应用列表查询

检测项目：验证应用查询符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端可进行移动支付终端 SE 应用查询。

6.4.8 应用同步

检测项目：验证应用同步符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端可进行移动支付终端 SE 应用同步。

6.4.9 应用删除

检测项目：验证应用删除符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端可进行移动支付终端 SE 应用删除。

6.4.10 应用锁定

检测项目：验证应用锁定符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端 SE 应用可进行锁定。

6.4.11 应用解锁

检测项目：验证应用解锁符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端 SE 应用可进行解锁。

6.4.12 应用远程管理同步

检测项目：验证应用远程管理同步符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端 SE 应用可进行应用远程管理同步。

6.4.13 SE 激活

检测项目：验证 SE 激活符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端可进行 SE 激活。

6.4.14 SE 锁定

检测项目：验证 SE 锁定符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端可进行 SE 锁定。

6.4.15 SE 终止

检测项目：验证 SE 终止符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端可进行 SE 终止。

6.4.16 安全域锁定

检测项目：验证安全域锁定符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端可进行安全域锁定。

6.4.17 安全域解锁

检测项目：验证安全域解锁符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：通过 SE 应用管理终端对移动支付终端可进行安全域解锁。

6.4.18 安全域终止

检测项目：验证安全域终止符合规范要求。
测试过程：检查厂商提供的材料。

对产品进行实际检测。

通过标准：通过 SE 应用管理终端对移动支付终端可进行安全域终止。

7 SE 应用管理终端安全要求检测

7.1 SE 应用管理终端安全管理检测

7.1.1 自检

检测项目：验证终端自检符合规范要求。

测试过程：检查厂商提供的材料。

对产品进行实际检测。

通过标准：SE 应用管理终端开机后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。

7.2 SE 应用管理终端（POS 形态）集成安全要求

7.2.1 PIN 输入功能集成

检测目的：验证 PIN 输入功能集成符合规范要求。

测试过程：检查厂商提供的资料。

查看 PIN 输入设备的检测报告或证书。

通过标准：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，遵循以下的要求：

a) 终端上如果有消费金额的提示及输入 PIN 的提示，则这两个提示有明显区别；

b) 终端在进入到输入 PIN 的界面之后不能再输入其它非 PIN 数据；

c) 当终端进入到输入 PIN 的界面后，之前输入的金额部分不能被修改；

d) 当终端进入到输入 PIN 操作阶段，终端上禁止进行其它和 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；

e) 当进行 PIN 输入提示的时候，终端只接受诸如“Yes,‖—OK,‖—Cancel,‖or —No”这些控制字符。

7.2.2 SE 应用管理的集成

检测目的：验证 SE 应用管理的集成符合规范要求。

测试过程：检查厂商提供的资料并验证。

通过标准：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，不引入新的攻击途径。

密码输入终端具有防止偷取支付卡机制（Lebanese loop attack 黎巴嫩环攻击）。

在同一个设备中，安全器件与非安全组件之间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 输入设备只具有一个支付卡密码输入接口，例如一个键盘等。

7.2.3 设备移除的安全要求

检测目的：验证终端的集成符合规范要求。

测试过程：检查厂商提供的资料并验证。

通过标准：安全组件不能擅自被拆除。

供应商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，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。

7.3 SE 应用管理终端（自助终端形态）逻辑安全

7.3.1 非 PIN 数据输入

检测项目：验证非 PIN 数据输入符合规范要求。

测试过程：检查厂商提供的材料。

通过标准：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：

a) 提示信息由加密单元控制；

b) 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；

c) 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。

7.3.2 多应用

检测项目：验证多应用符合规范要求。

测试过程：检查厂商提供的材料。

对产品进行实际检测。

通过标准：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。

7.4 操作系统

检测项目：验证操作系统符合规范要求。

测试过程：检查厂商提供的材料。

对产品进行实际检测。

通过标准：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。必须要以最少的特权来配置和运行。

7.5 单一的 PIN 数据接口

检测项目：验证单一的 PIN 数据接口符合规范要求。

测试过程：检查厂商提供的材料。

对产品进行实际检测。

通过标准：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。

7.6 传输报文加密

检测项目：验证传输报文加密符合规范要求。

测试过程：检查厂商提供的材料。

对产品进行实际检测。

通过标准：针对所有连接 TSM 平台的 SE 应用管理终端，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。

7.7 终端联机交易密钥管理

7.7.1 二级密钥体系

检测项目：验证二级密钥体系符合规范要求。

测试过程：检查厂商提供的材料。

对产品进行实际检测。

通过标准：终端密钥分为二级：终端主密钥（TMK）和工作密钥（WK）。

7.7.2 终端主密钥(TMK)

检测项目：验证终端主密钥符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

7.7.3 工作密钥（WK）

检测项目：验证工作密钥符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

7.8 终端 MAC 的算法

检测项目：验证终端 MAC 的算法符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

7.9 PIN 加密

检测项目：验证 PIN 加密符合规范要求。
测试过程：检查厂商提供的材料。
对产品进行实际检测。
通过标准：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。

7.10 PIN 输入安全

检测项目：验证 PIN 输入安全符合规范要求。
测试过程：检查厂商提供的材料。
通过标准：PIN 输入设备应符合第 8 章 PIN 输入设备的要求。
PIN 输入设备应经过金融行业主管机构认可的权威检测机构的检测。

8 PIN 输入设备安全检测

8.1 物理安全性要求

8.1.1 入侵检测机制

检测目的：验证入侵检测机制符合要求。
测试过程：根据厂商提供资料，设计攻击场景使入侵检测机制失效，计算攻击分值。
通过标准：设计的攻击场景的攻击分值不低于 26（攻击分值的计算公式见附录 C，下同），其中实施攻击分最少 13 分。
PIN 输入设备应具备防攻击性和反攻击性的机制，保证设备在被攻击后立即处于不可操作状态，并自动立即擦除设备中存放的秘密信息。这些机制可以使设备抵抗如下物理攻击手段（包括但不限于）：钻孔、激光、化学溶剂、通过外壳和通风口的探查。并且要求绕过这些机制插入 PIN 窃取装置或者获取敏感信息的可行方法至少需要 26 分（不包括对非接触式读写器的攻击）的攻击分值，其中实施攻击分最少 13 分。

8.1.2 独立安全机制

检测目的：验证独立安全机制符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
检查是否至少具有两个安全机制。
设计攻击场景，检测每个安全机制是否独立。
通过标准：厂商提供的资料与安全要求一致。
设备的安全系统由至少两个以上的独立安全机制组成，设备的单个安全机制失效不会危及设备的安全。

8.1.3 内部访问响应

检测目的：符合内部访问响应符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
分析厂商文档和样品，看是否可访问 PIN 输入设备或非接触式读写器内部。对于可访问的通路是否有入侵检测机制。
通过标准：厂商提供的资料与安全要求一致。
如果可进行内部访问，入侵检测机制应符合安全要求。
若允许访问 PIN 输入设备或非接触式读写器内部区域（如服务或维护等），则通过该区域插入 PIN 窃取装置是不可能的。设备内部设计可以保证（例如将敏感数据所在的组件由防攻击性和反攻击性机制保护）禁止直接访问 PIN 或者密钥等敏感数据，或设备安全机制可以在非法访问其内部区域时立即擦除敏感数据。

8.1.4 环境和操作条件改变的适应性

检测目的：验证环境和操作条件改变的适应性符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
查看厂商相关资料，是否具有相应设备提供环境防护。
通过标准：厂商提供的资料与安全要求一致。
改变 PIN 输入设备的环境条件或操作条件不会影响其安全性（例如操作电压或环境温度超出 PIN 输入设备范围）。

8.1.5 敏感功能或信息保护

检测目的：验证敏感功能或信息保护符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
设计攻击场景尝试获取敏感信息，计算攻击分值。
通过标准：厂商提供的资料与安全要求一致。
敏感功能或敏感信息只能在 PIN 输入设备受保护的区域内使用。对敏感信息和敏感功能进行攻击和修改至少需要 26 分的攻击分值（不包括对非接触式读写器的攻击），其中实施攻击分最少 13 分。

8.1.6 PIN 输入过程中可听到的音调

检测目的：验证 PIN 输入过程中可听到的音调符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
分析数字键按键音。
通过标准：厂商提供的资料与安全要求一致。
PIN 输入时所产生的音调是不可分辨的。

8.1.7 PIN 输入过程中监控

检测目的：验证 PIN 输入过程中监控符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
对 PIN 输入过程中的声音进行分析。
对 PIN 输入过程中的电磁辐射进行分析。
设计一种攻击场景。
通过标准：厂商提供的资料与安全要求一致。

即使在收银员或店员的协助下，通过监听 PIN 输入设备的声音、电磁辐射、能量消耗或其他任何可以从外部监听到的特征来探查 PIN 都至少需要 26 分的攻击分值，其中实施攻击分最少 13 分。

8.1.8 密钥识别分析

检测目的：验证密钥识别分析符合要求。

测试过程：检查厂商提供的资料是否与安全要求一致。

进行 SPA/DPA 攻击试验。

通过标准：厂商提供的资料与安全要求一致。

通过入侵或渗透 PIN 输入设备或非接触式读写器、监测 PIN 输入设备或非接触式读写器的辐射（包括能量波动）的方法获取在 PIN 输入设备或非接触式读写器中存储的任何与 PIN 安全相关的密钥，要求至少需要 35 分攻击分值，其中实施攻击分至少 15 分。

8.1.9 PIN 输入设备输入非PIN 数据

8.1.9.1 提示信息由加密单元控制

检测目的：验证输入非 PIN 数据安全机制符合要求。

测试过程：检查厂商提供的资料是否与安全要求一致。

设计攻击场景。

通过标准：厂商提供的资料与安全要求一致。

输入非 PIN 数据时设备显示的提示内容应在安全单元的控制下，对非 PIN 数据的攻击至少需要 18 分攻击分值，其中实施攻击分至少 9 分。如果该提示内容是存储在安全单元内部，那么改变该提示内容会导致安全单元内密钥的擦除。如果该提示内容是存储在安全单元外部，那么设备安全机制要保证提示内容的完整性、正确使用和不被非法修改或使用（由厂商满足实现）。

8.1.10 移除检测

检测目的：验证移除检测符合要求。

测试过程：检查厂商提供的资料是否与安全要求一致。

设计攻击场景。

通过标准：厂商提供的资料与安全要求一致。

安全组件不能擅自被拆除。如果要破坏或绕过该安全保护功能至少需要攻击分 18 分，其中实施攻击分最少 9 分。

8.1.11 防偷窥保护（仅用于POS PED）

检测目的：验证防偷窥保护符合要求。

测试过程：检查厂商提供的资料是否与安全要求一致。

厂商的声明中要明确指出 PIN 输入设备采取了措施防止持卡者在输入 PIN 时被偷窥。

实际检查和评估 PIN 输入设备。

通过标准：厂商提供的资料与安全要求一致。

PIN 输入设备防偷窥设计符合安全要求。测试方法见附录 B。

8.1.12 独特外观（仅用于POS PED）

检测目的：验证独特外观符合要求。

测试过程：检查厂商提供的资料是否与安全要求一致。厂商的声明中要明确指出 PIN 输入设备或非接触式读卡器应该设计成无法通过从市场上购买组件来复制。

通过标准：厂商提供的资料与安全要求一致。

PIN 输入设备或非接触式读写器应经过合理设计，以保证无法利用在零售市场上可买到的商品组件来组装 PIN 输入设备或非接触式读写器。例如，特有的设备外壳。

8.2 逻辑安全要求

8.2.1 自检测试

检测目的：验证自检测试符合要求。
测试过程：检查厂商提供的材料。
设计验证场景
通过标准：自检在设备启动时进行并至少每天进行一次。
固件完整性符合安全要求。
固件真实性符合安全要求。
PIN 输入设备应具备自检功能，能够检查设备的固件、安全机制以及安全状态，自检在设备启动时进行并至少每天进行一次。自检的目标是检查固件、针对篡改迹象的安全机制以及 PED 是否处于被攻破状态。一旦出现故障，PED 及其功能会以安全的方式失去效用。

8.2.2 逻辑异常

检测目的：验证逻辑异常保护机制符合要求。
测试过程：检查厂商提供的材料。
执行测试验证设备属性。
通过标准：PIN 输入设备不应受异常数据的影响而泄露 PIN 的明文或其他敏感数据，这些异常数据包括（但不限于）：错误顺序的命令、未知命令、错误模式下的命令和错误的参数。

8.2.3 固件认证

检测目的：验证固件认证机制符合要求。
测试过程：检查厂商提供的材料。
检查任何厂商提供的附加相关文档。
验证场景设计。
通过标准：设备固件及对固件的任何改动都必须经过严格的流程控制，以保证固件中不含隐藏的非法功能。

8.2.4 固件更新

检测目的：验证固件更新符合要求。
测试过程：检查厂商提供的材料。
确定固件更新符合安全要求。
通过标准：如果 PIN 输入设备固件能够进行更新，那么设备必须通过加密机制验证更新固件的完整性和真实性。如果未确认其完整性和真实性，那么设备应拒绝进行固件更新或清除设备中所有的密钥。

8.2.5 输入 PIN 区别

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
验证环境设计。
通过标准：设备不能显示或者泄漏输入的 PIN 数字。所有与输入 PIN 相关的字符应显示为无意义的字符（例如星号）或者输出无区别的信号等。

8.2.6 内存清除

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
通过标准：PIN 输入设备应严格控制敏感信息的存在时间和使用次数。设备在下面任一情况必须自动清空其内部保存得敏感信息：
交易已经完成；
f） PIN 输入设备等待持卡人或商户的响应超时。

8.2.7 敏感服务保护

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
验证敏感服务保护。
通过标准：设备的敏感服务用于访问敏感功能，敏感功能处理设备中如密钥、PIN 和口令等敏感数据，使用设备的敏感服务必须通过身份验证。进入或退出敏感服务不应泄露或改变设备中的敏感信息。

8.2.8 敏感服务限制

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
验证敏感服务限制。
通过标准：为保证设备的敏感服务不被非法使用，必须对设备敏感服务的范围和使用时间进行限制，若超出服务范围和使用时间则 PIN 输入设备应退出敏感服务并返回到正常模式。

8.2.9 随机数

检测目的：验证设备的保护机制符合要求。
测试过程：对随机数随机性进行测试。
通过标准：随机数具有足够的随机性。

8.2.10 PIN 防穷举

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
检查厂商提交的相关的附加文件。
通过标准：设备应具有防止利用盗取的设备穷举探测获得 PIN 值的特性。

8.2.11 密钥管理

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
通过标准：设备执行密钥管理技术需要同时遵守 ISO 11568 和 ANSI X9.24，或者符合两者之一。密钥管理技术必须支持 ANSI TR-31 或者一个等价的方法用于维持 TDEA 密钥组。

8.2.12 加密算法测试

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
检查厂商提交的文档。
验证 PIN 加密算法符合要求。
通过标准：设备中执行的 PIN 加密技术是 ISO 9564 中规定的技术。

8.2.13 对设备中任意数据加解密

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
验证对设备中任意数据加解密。
通过标准：不能利用 PIN 输入设备内的工作密钥（WK）或密钥加密密钥（KEK）去加密或解密其他任意的数据。PIN 输入设备必须强制使数据密钥，密钥加密密钥和 PIN 加密密钥有不同的值。

8.2.14 明文密钥安全

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
检查厂商提交的任何相关的附加文件。
通过标准：不允许输出私钥或密钥以及 PIN 的明文；不允许用可能已经泄密的密钥去加密其他密钥或 PIN；不允许把密钥明文从高安全的组件传送至低安全的组件中去。

8.2.15 交易控制

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
检查厂商提交的任何相关的附加文件。
验证交易控制。
通过标准：任何其他交易数据的入口必须与 PIN 输入过程分离，避免在设备屏幕意外的显示持卡人 PIN。如果其他数据与 PIN 通过同一个键盘输入，那么其他数据输入与 PIN 输入应该是清晰分离的操作。

8.2.16 PIN 输入设备输入非 PIN 数据

8.2.16.1 改变用户界面提示攻击可能性分析

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
设计攻击场景。
通过标准：厂商提供的资料与安全要求一致。
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）的攻击至少需要 18 分的攻击分值，其中实施攻击分至少 9 分（由厂商满足实现）。

8.2.16.2 基于加密的控制

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
设计攻击场景。
通过标准：厂商提供的资料与安全要求一致。
对于具有可变显示功能的 PIN 输入设备，设备的显示必须在安全单元控制下进行，设备的控制机制应保证不能通过改变设备的显示内容来获得明文 PIN，并且提供特有的认证机制和合适长度的密钥。在设计设备密钥管理方式或其他安全控制机制时应采用双重控制和知识分割的原则（允许第三方控制认证方法）。

8.2.17 设备多应用

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
评估设备支持的应用是都独立。
验证应用的独立性。
通过标准：厂商提供的资料与安全要求一致。
如果设备支持多应用，必须保证各应用间的相互独立，其中任何应用不能干扰其它应用和操作系统，包括不能修改属于其它应用的数据对象。

8.2.18 操作系统

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
验证权限配置。
通过标准：厂商提供的资料与安全要求一致。
设备的操作系统中只能包含设备内部操作及服务应用软件，操作系统必须进行安全配置，开通尽量少的权限设置。

8.2.19 集成指南

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商是否具有集成指南。
验证集成指南的可操作性。

通过标准：供应商应提供完整详细的安全引导指南，方便集成商将安全设备集成到终端中去。

8.3 联机终端安全要求

8.3.1 密钥替换（仅用于POS PED）

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
检查厂商提交的任何相关的附加文件。
通过标准：验证如果设备能保存多个加密密钥并且用于加密 PIN 的密钥能从外部选择，那么设备禁止未经授权的密钥替换和密钥滥用。

8.4 脱机终端安全要求（仅用于POS PED）

8.4.1 防穿透保护

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
查看其它相关文档。
设计攻击场景。
通过标准：厂商提供的资料与安全要求一致。
在要求攻击分值小于 16 的情况下，任何渗透非接触式读卡器从而附加、替换和修改非接触式读卡器的软件或硬件，以获取或修改任何敏感数据的攻击都是不可行的。注意事项：读卡器可以有不同安全级别区域，例如 SE 接口自身的区域和容纳退卡的区域。

8.4.2 PIN 输入设备和非接触式读卡器间 PIN 传输保护

8.4.2.1 PIN 输入设备和非接触式读卡器间 PIN 传输保护

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
通过标准：如果 PIN 输入设备和非接触式读写器不是集成在一起，且验证持卡人方式为加密 PIN 验证，PIN 输入设备和非接触式读写器之间传送的 PIN BLOCK 必须通过 SE 上的加密密钥进行加密，或与 ISO 9564 加密要求保持一致。

8.4.2.2 PIN 输入设备和非接触式读卡器间 PIN 传输保护

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
通过标准：如果 PIN 输入设备和非接触式读写器不是集成在一起，且验证持卡人方式为明文 PIN 验证，那么从 PIN 输入设备向非接触式读写器传送的 PIN BLOCK 必须按照 ISO 9564 要求进行加密。

8.4.2.3 PIN 输入设备和非接触式读卡器间 PIN 传输保护

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
通过标准：如果 PIN 输入设备和非接触式读写器集成在一起，且验证持卡人方式为加密 PIN 验证，那么 PIN BLOCK 必须通过 SE 上的加密密钥进行加密。

8.4.2.4 PIN 输入设备和非接触式读卡器间 PIN 传输保护

检测目的：验证设备的保护机制符合要求。
测试过程：检查厂商提供的材料。
通过标准：如果 PIN 输入设备和非接触式读写器集成在一起，且验证持卡人方式为明文 PIN 验证，那么 PIN BLOCK 在受保护环境（ISO 9564）中传输时不需加密。如果明文 PIN 在未受保护环境中从 PIN 输入设备传输至非接触式读写器，则 PIN BLOCK 应按照 ISO 9564 要求进行加密。

8.5 设备安全管理

8.5.1 生产期间的设备安全管理要求

检测目的：验证设备的保护机制符合要求。

测试过程：检查厂商提供的资料，验证生产安全管理符合规范要求。

设计测试案例，验证生产安全管理措施的有效性。

通过标准：设备生产期间的安全管理符合要求。

在设备生产过程中必须采取变更控制机制，该机制可以保证当设备的任何物理或逻辑特性发生改变时，设备都应按照本规范的物理安全性要求或逻辑安全性要求进行重新评估。

对通过评估的固件要合理地保护和存储，以防止被非法修改。对固件的保护应采用双重控制或密码验证方式进行。

在生产过程中，用于组装 PIN 输入设备的组件必须通过物理安全性要求的评估，并且这些组件没有被非法替换。

设备所安装的软件在运送、存储和使用时，必须遵循双重控制的原则，以防止在未授权情况下的对软件的修改或替换。

在产品生产完成后且在出厂前，PIN 输入设备和其任何组件都应存放在受保护的、进行访问控制的区域内，或将设备封装在具有防攻击特性的包装中，以防止非法接触设备或其组件。

如果 PIN 输入设备在装载密钥时要对设备进行验证，且验证要素为生产过程中装入设备的秘密信息，那么该秘密信息的设置应对每台 PIN 输入设备唯一，任何人都不可知和不可预测该信息，并且该秘密信息在装入 PIN 输入设备时应在双重控制之下，以保证在装入期间不会泄露。如果 PIN 输入设备和非接触式读写器集成在一起，且验证持卡人方式为明文 PIN 验证，那么 PIN BLOCK 在受保护环境（ISO 9564）中传输时不需加密。如果明文 PIN 在未受保护环境中从 PIN 输入设备传输至非接触式读写器，则 PIN BLOCK 应按照 ISO 9564 要求进行加密。

8.5.2 初始密钥注入前的设备安全管理要求

检测目的：验证设备的保护机制符合要求。

测试过程：检查厂商提供的资料，验证初始密钥注入前的设备安全管理符合规范要求。

设计测试案例，验证初始密钥注入前的设备安全管理措施的有效性。

通过标准：初始密钥注入前的设备安全管理符合要求。

PIN 输入设备从生产厂家至初始密钥注入方的运送途中的存储过程都要受到控制和审计，以便及时确定设备在途中的地点。

必须设计合理的流程将对设备的安全责任从厂家递交给设备初始密钥注入方。

在设备从生产厂家向初始密钥注入方运送的过程中，应该具备下列条件：在具有防攻击特性的包装中存放并运送设备；如果设备在存放和运送时存有秘密信息，那么当试图对设备做任何物理或功能上的改变时，该秘密信息应立即自动销毁。初始密钥注入方能验证该秘密信息完整性，但是未授权的个人无法获取该秘密信息。

附 录 A
（规范性附录）
抗破坏能力

A.1 目的

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。

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。

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。

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。

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

a) 一次试验可选用多种攻击方式，每种攻击可进行 30min。
b) 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

a) 钓现、暴力取现、设陷取现是由自助终端的设计所决定的。
b) 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

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

A.3.2 工具

a) 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。
b) 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。
c) 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.1中所述的要求为准。

A.3.4 方法

a) 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。
b) 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。
c) 锁舌——通过门上的开口切断或移动主要锁舌使其脱离连接。
d) 切断锁舌——刺穿门的旁柱并切断主要锁舌。
e) 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。
f) 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。
g) 撬开或劈开门——用楔子、凿子和撬刺破或打开门以取走现金。
h) 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。
i) 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。

附 录 B
（规范性附录）
挡板设计标准

B.1 满足PIN输入设备设计的挡板设计标准

下面的例子，是一个符合安全要求的PIN输入设备设计的主体部分，其中就包含挡板的设计，设备样品如图B.1、B.1、B.3。其他设计也可以达到要求。

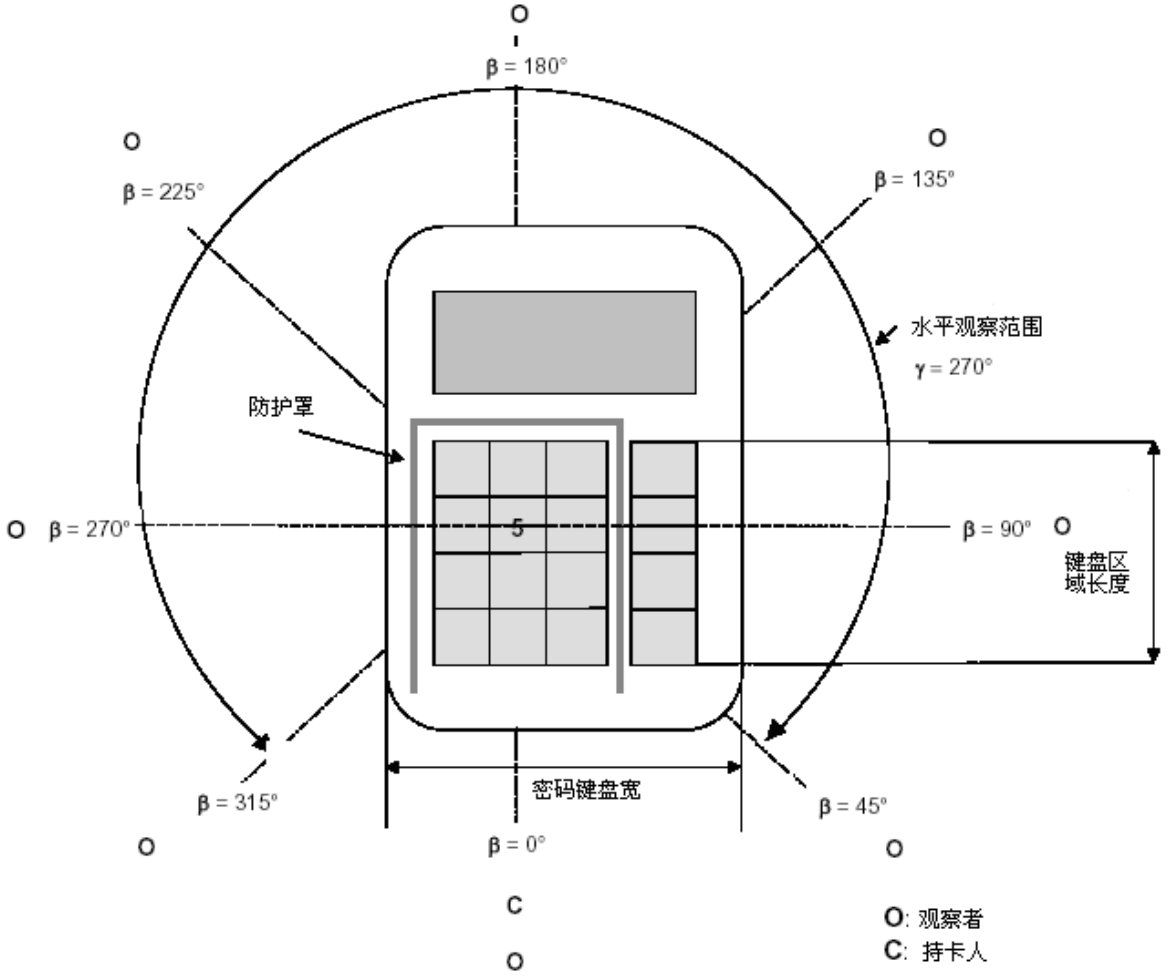

图 B. 1 含有挡板设计的 PIN 输入设备样品，俯视图

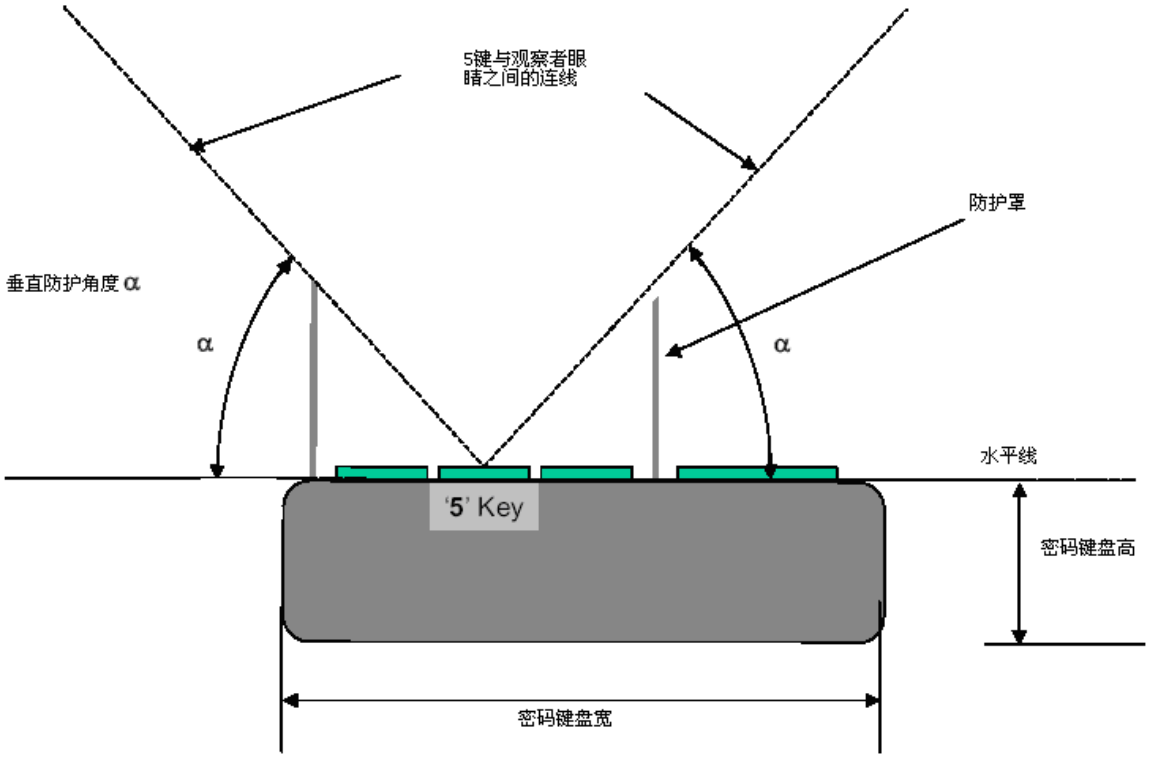

图 B.2　PIN 输入设备样品，正视图

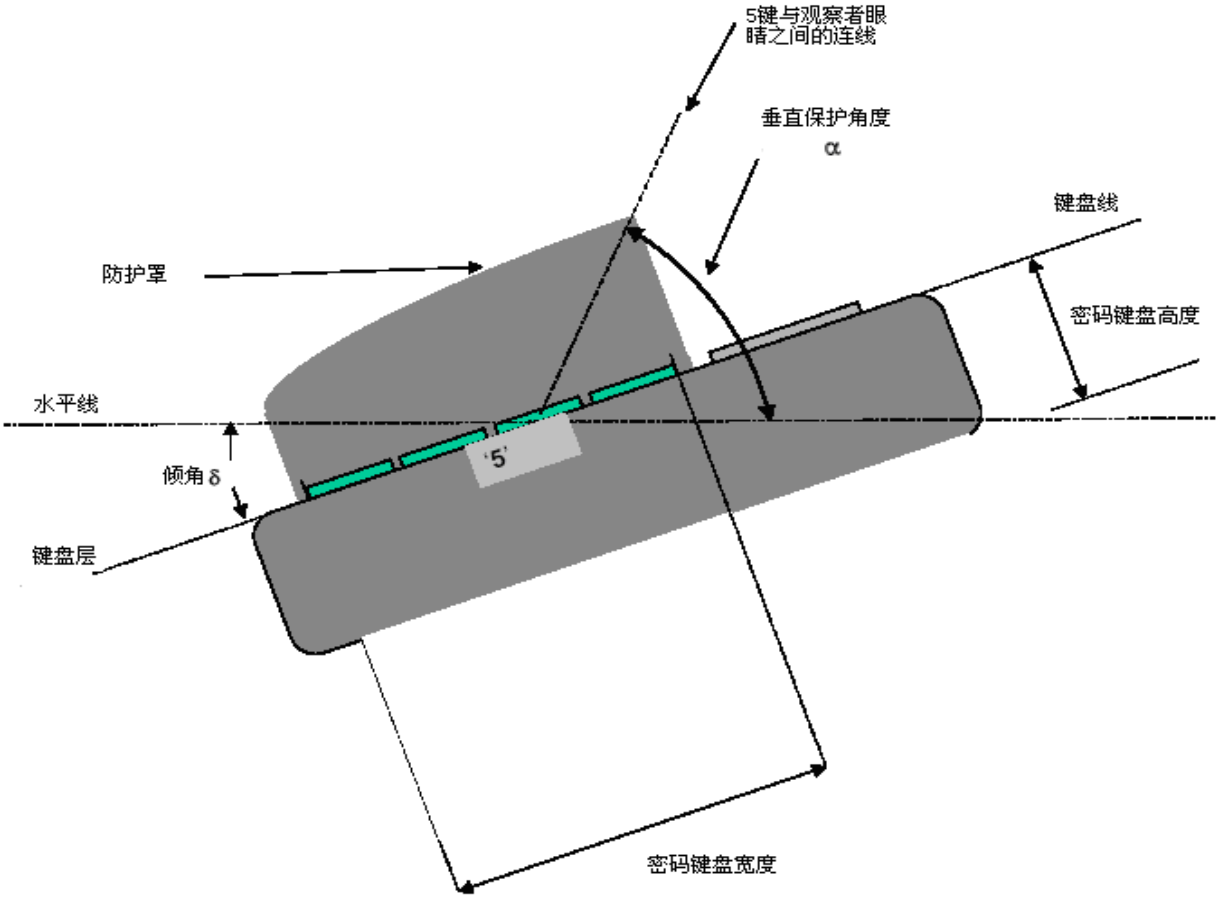

图 B.3　PIN 输入设备样品，侧视图

以上图中的角度定义如下：

α：此角度是5键所在平面与连接5键与观测者视角的虚线之间的角度。

β：观测者位置相对于操作员的位置之间的水平角度。

γ：挡板存在的水平角度。

δ：键盘区平面与水平面之间的角度。

设计原则

手持设备，有人职守设备以及无人职守设备有不同的设计要求。所以一定要明确待评估设备的预期使用方式。

手持设备必须由重量，尺寸以及外形来支持其手持操作。标准如下：

重量应不超过 500g；

5 键处的宽度不得超过 3inches 或者 7.62cm；

5 键处宽度与高度的总和应不得超过 4inches 或者 10.16cm；

键盘区的长度应不得超过 4inches 或者 10.16cm。

如果设备的模型明显的超出了这些范围，那么作为手持设备它就不适合进行此项评估。因为手持设备必须由其尺寸以及外形来支持其手持操作。设计的小巧并不意味着满足要求。即使设备外观的很小，如果其常备支撑或者设备支架明显的表明PIN输入设备被装在一个旋转的支架上或者类似工具上，它将被认定为桌上设备而不是手持设备。

设备的挡板应放置水平位置或者稍稍有一角度（$0 \le \delta \le 45^o$），并且要求提供以下的保护角度，测试角度要求如表B.1：

表 B.1　测试角度要求

水平角度 β	注释	垂直角度 α
$315^o \le \beta \le 45^o$	在这个 β 角度范围内，持卡人使用身体能将观测者的视角所遮挡。	N/A
$45^o \le \beta \le 90^o$ $270^o \le \beta \le 315^o$	在这个 β 角度范围内，观测键盘区的视线一部分被持卡人所遮挡。此时，保护角度 α 必须不小于 35^o。注意：如果 PIN 输入设备倾斜放置，前面的挡板应该更高。	$\alpha \ge 35^o$
$90^o \le \beta \le 270^o$	保护角度 α 至少为 40^o。如果键盘平面向下倾斜，则前挡板则可以适当的降低。	$\alpha \ge 40^o$

表B.1中的垂直角度α的要求范围，与水平面的位置有着相应的关系（见表B.1）。如果PIN输入设备设计中键盘区向持卡人方向倾斜，则挡板后面的高度则可以适当降低。

如果PIN输入设备垂直放置或者放置角度大于45^o，那么第三步将做适当的改变。使用垂直面代替水平面作为α的参考平面。

此项保护只是针对于观测的视角，并不意味着必须使用特别的技术手段，比如说物理防护。如果PIN输入设备实际中是一个触摸屏，那么一定要使用偏光器（例如触摸屏表面的模糊处理）制造视觉障碍，这样就能阻止从旁边进行观测。店员一边必须使用物理防护。

B.2　满足PIN输入设备放置环境的挡板设计标准

以下的技术可以在PIN输入时，对键盘区进行有效的遮挡。尽管这些技术在某些案例中可以单独使用，但是通常情况下，会同时使用这些技术。

注意：此选项并不是不使用A1中定义的防护机制，而是对物理防护机制降低一些要求，比如$\alpha \ge 20^o$。

设备放置位置的检测目的是使得对PIN输入过程的观测是不可实现的。比如包括以下各点：

a) 在验货台上要设计视觉挡板。这个挡板可以独立的作为挡板使用，或者作为一般通用验货台的一部分，比如说是验货台的销售部位。

b) 将 PIN 输入设备成一定的角度放置，使得 PIN 输入时难以进行偷窥。

c) 将 PIN 输入设备安装一个可调节的支架，这种支架可以便于消费者将设备向旁边旋转、向前或向后倾斜一定位置，使得 PIN 输入时难以进行偷窥。

d) 在店内的安全摄像头的放置位置处，应不得看到 PIN 输入。

e) 提醒持卡人关于 PIN 输入的安全事项，可以用以下几种方式进行：

　　1) 在 PIN 输入设备上标注；

2) 在显示时进行提示，尽可能使用一个“单击确认”画面；
3) 印在终端上；
4) 安全 PIN 输入过程的一个标识。

除此之外还有其他的可行方法。以上只是一些厂商在PIN输入过程中保护PIN的一些例子。厂商必须在PIN输入设备文档中提供恰当的技术，并且要包含一个针对不同观察区域安全所实施技术的矩阵。表B.2是一个矩阵的例子：

表 B.2 观察区域以及 PIN 保护方法的矩阵样本

	观测途径				
方法	**收银员**	**排队的顾客**	**非排队的顾客**	**现场的摄像机**	**远程摄像机**
A 类 PED 支架	M	H	L	L	L
B 类 PED 支架	H	H	H	L	M
A 类收银台	L	M	M	L	H
B 类收银台	H	H	M	H	H
客户使用说明	H*	H*	H*	H*	H*

[a] *客户使用说明的方法可重复性低，因此应该与其他方法共同使用。

[b] L：低等防护水平，M：中等防护水平，H：高等防护水平

矩阵中必须明示PIN输入设备的购买方如何保护持卡人PIN的方法。应该根据所有的观察区域选择一个恰当的方法，以便于保持一个适当的保护级别。

附 录 C
（规范性附录）
攻击分值计算公式

C.1 计算攻击分值

本章节分析决定攻击分值的因素，并给出评估过程中如何避免一些主观因素的指导意见。评估人员应根据实际情况，采纳该规范要求。

C.2 识别分析和实施攻击

攻击者在准备实施攻击已存在的漏洞时必须首先识别分析出漏洞。所以将其分为两个步骤：识别分析和实施攻击。

C.3 需要考虑的因素

C.3.1 考虑因素概述

在分析漏洞攻击分值时，应当考虑下列因素：

——识别分析

- 使用各种级别的专业技术，进行攻击所需的时间；
- 获取 PIN 输入设备的设计及操作原理知识的分值；
- 访问 PIN 输入设备的分值；
- 需要的设备，如进行分析所需的工具，组件，IT 硬件和软件；
- PIN 输入设备特定的零配件。

——实施攻击

- 使用各种级别的专业技术，进行攻击所需的时间；
- 获取 PIN 输入设备的设计及操作原理知识的分值；
- 访问 PIN 输入设备的分值；
- 需要的设备，如进行分析所需的工具，组件，IT 硬件和软件；
- PIN 输入设备特定的备用组件。这些因素并不互相依赖，但是在某种程度上却是可互相替代的。例如，专业技术或者软/硬件工具在某些情况下可以减少攻击所需的时间。

C.3.2 具体因素描述

C.3.2.1 攻击时间

攻击时间指攻击者识别分析或者实施攻击所需的时间（以小时为单位）。如果攻击由多步组成，则攻击时间累加起来从而获得攻击所需的总时间。应当统计实际的工作时间，而不是整个过程所耗费的时间，因为对采用的方法来说，没有一个最小的攻击时间(例如进行旁路分析所需时间或者环氧变硬所需的时间)。在那些无需人员职守的某攻击阶段，攻击时间应当以整个耗费时间的1/3来计算。

为了更好地计算实际工作时间，这里使用的转换关系为：1天=8个小时，1周=40小时，1月=180小时。

C.3.2.2 专业技术

专业技术指在应用领域或者产品类型等方面的通用知识等级。(例如，Unix操作系统，网络协议）分为以下等级：

——专家，对所采用的安全机制规则和理念非常熟悉，并对产品或系统类型相关的底层算法、协议、硬件、组织等方面也相当熟悉；

——精通，熟悉产品的安全特性的人，为了进行攻击，精通人员应具有使得攻击成功所需技能的资质；

——外行，和专家、精通的人相比是外行，没有专门技术，为了实施攻击，外行人员可以依据一个脚本或者既定流程，不需要特殊的技能。

如果某个攻击需要精通多个领域的技术,例如电子工程或者密码学,则可以假定需要专家级别的专门技术。

复合专家等级是指在多个技术领域达到专家等级的知识储备。这些领域都是为攻击技术所必须的。而复合专家所关心的领域必须是不相同的,比如硬件操作和密码学。复合专家等级适用于那些需要培训等级的相关领域,而不是针对一次攻击所需要的实际个体数。在使用复合专家等级的时候必须要提供非常充分的理由。

C.3.2.3 PIN输入设备相关知识

PIN 输入设备相关的知识指具有特定的和 PIN 输入设备相关的专门技术。可分为以下等级：

——与 PIN 输入设备有关的公开信息（或者没有任何信息），每个人都很容易获取到（如从互联网获取）的信息，或者可由厂商提供给任何客户的信息，这些都被认为是公开的。

——与 PIN 输入设备有关受限制的信息（从厂商技术规格说明书中获取的信息），如果设备是先申请后发放，并且发放需要注册，则此类信息也被认为是受限制的信息。

——与 PIN 输入设备有关的敏感信息（内部设计的知识），需要利用“社交工程”或者彻底的逆向工程才能获取的信息。

应必须仔细区分用来分析漏洞和用来攻击的信息，特别是敏感信息更需要进行严格区分。实施攻击一般不需要敏感信息。

专家技术以及PIN输入设备的知识影响着有能力攻击PIN输入设备的攻击者所需信息的多少。攻击者的技术水平和在攻击中熟练使用设备的能力间有一些内在关系。攻击者的技术水平越低,它熟练使用设备的能力越弱。同样的，技术水平越高，在攻击中使用设备的能力越强，具体关系不是唯一，须根据实际情况而定，如当环境因素限制专家级的攻击者使用设备,或者使用他人已开发并免费发布(通过互联网）的“傻瓜式”攻击工具。

C.3.2.4 访问PIN输入设备

机械样本是非功能性仅用来学习或者提供备份部件使用。没有工作密钥的功能性样本可用来测试设备的逻辑或者电气特性，不能用于网络支付和真正的支付卡支付。此种设备攻击者可购买到。注意，安装了测试密钥或者伪密钥的样本属于此类。带有工作密钥的功能性样本是全功能的设备,可用来验证一种攻击手段或实施攻击。如果在某个类别中需要超过1个样本，不可采用样本的数量乘以分数，而应当使用表C.1的因子：

表 C.1 多个样本因子

设备的数量	因子
1	1
2	1.5
3-4	2
5-10	4
>10	5

C.3.2.5 分析设备工具

分析设备工具指用来分析或攻击漏洞的设备。可分成以下类别：

——标准设备：攻击者可快速使用分析漏洞或进行攻击的设备。这类设备较容易获取，如已在附近的仓库或从互联网下载的。可包含简单的攻击脚本、个人计算机、读卡器、模式发生器、简单光学显微镜、供电电源或者简单的机械装备；

——专门设备，攻击者不能马上获取，但可经过正当途径获得的设备。包括购买中等数量的设备，如专门的电子卡片、专用的测试平台、协议分析器、示波器、微探针工作站、化学工作台、精确铣床设备等等，或者开发更多的攻击脚本或程序；

——定制设备，指对公众还没有，需要专门定制的设备，如非常专业的软件，或设备太专业，控制发放甚至是严格限制。也可以是设备非常昂贵，如离子聚焦光束、扫描式电子显微镜，激光打磨器。可

以租用到的定制设备可以视为专门设备，在分析阶段开发的软件也可认为是定制设备，在攻击阶段开发的则不算。

——芯片级别攻击设备，有必要时需进行芯片级攻击，其在市场上非广泛应用并且受到限制。该攻击使用的设备价格非常昂贵，因此将其单独进行分类。仅以下设备属于此类范畴：

- 聚焦离子束
- 电子扫描显微镜
- 激光研磨设备如果某个阶段（识别阶段或攻击阶段）需要使用不同级别的设备，应只保留其中最高等级即可。如果在识别阶段使用的设备，在攻击阶段也会重复利用，不能对同一设备进行两次评分。这种情况下，设备的分值应平均后分别用于识别阶段和攻击阶段中。

分析阶段使用多个设备能够保证在攻击阶段的成功率，但是在攻击阶段很少会使用多个设备。

C.3.2.6 隐藏攻击痕迹的组件

组件用来隐藏攻击痕迹、替换数据监控或安装通讯装置。如果同样的零件在识别分析或者实施攻击过程中都使用，则只可以被统计一次。PIN获取bug属于此类范畴。

——标准组件，攻击者较容易得到的部件，可通过市场购买或从同类型设备样本中拆来的部件；

——专用组件，不是攻击者已有，但可通过正当途径获得的部件。如通过市场订购且需要很长的运送时间，或需要按批购买的组件；

——定制组件，需要专门制造的部件。如果攻击需要专门定制部件，则这种攻击方式不大可行。

C.3.2.7 攻击成功率

攻击成功率仅在攻击的初始阶段使用，是一个用于对攻击的后续阶段可以重复利用设备、知识进行优化，通过实验室评估的手段很难进行判定。在后续攻击阶段重复使用并用于计算的典型因素包括设备和知识两种。

在某些攻击场景中会导致总分以及攻击分值一致，但是其中之一会使得攻击阶段的耗费较低，除上面两个因素外的其他因素在评分时都要被考虑。

攻击成功率如果实施一个攻击的难度相当的大，导致成功的数量较少，此时需要依据限制条件应用多个设备。

为了应对这类情况的出现，目标设备（例如攻击阶段使用带有工作密钥的功能性样本）的数量，应使用表C.2中的因子进行乘法运算：

表 C.2 成功率乘法因子

成功率	因子
P≥0.5	1
0.5＞P≥0.25	1.5
P＞0.25	2

一旦确认了攻击存在可能的因素，攻击的每一个步骤必须分成独立的阶段，其中每个阶段都必须具有其自己的可能性。总体的可能性是所有因子乘和得到。

一旦总体的可能性降低到 0.5 以下，需要出具一个恰当的文档。确定可能性的工作是基于终端实际攻击的基础上得到的，并行可能使用恰当的样本制作统计数据图表。

C.4 攻击分值计算方法

针对一个既定的攻击，须提出多种攻击场景计算分值。如替换专业人员的攻击时间和设备。当分析出一个漏洞且在公用域中，则识别分值应该选用攻击者在公用域中提出攻击方案的分值，而不采用最初的识别分值，攻击分值因素分值见表 C.3。

表 C.3 攻击分值因素分值

分值	范围	分析阶段	攻击阶段
攻击时间	<1 小时	0	0
	<=8 小时	2	2

分值	范围	分析阶段	攻击阶段
	<=24 小时	3	3
	<=40 小时	3.5	3.5
	<=80 小时	4	4
	<=160 小时	5	5
	>160 小时	5.5	5.5
技术水平	外行	0	0
	精通	1.5	1.5
	专家	4	4
PIN 输入设备的知识	公开知识	0	0
	限制知识	2	2
	私有知识	3	3
攻击时需要获得 PIN 输入设备每个部件，如果需要多个部件，分值应当乘上上面的因子	设备样本	1	1
	没有工作密钥的功能性样本	2	2
	带有工作密钥和软件的功能性样本	4	4
攻击需要的设备	无	0	0
	标准的	1	1
	专用的	3	3
	定做的	5	5
	芯片级攻击	7	7
特殊零件需求	无	0	0
	标准的	1	1
	专用的	3	3
	定做的	5	5

这种方法并不适用于所有的情况或因素，但是它给出了计算攻击分值的一个比较好的思路。其它因素，例如依靠攻击结束前的偶然性或者运气等，则不包含在基本模型之中。但可以由评估人员而不应该由基本模型来界定。

确定适当的时间和等级对于每个阶段而言，测试实验室应记录所有的必须的步骤。应包括所使用的技术水平，设备，特殊零件需求，以及操作所需的时间（按小时计算）如果涉及到成功率，也要予以明确。

表C.3中描述的所有项目是一个很好的汇总，能够帮助对于上述因素进行合理的选择。

C.5 攻击实例一

本攻击的目标是向 PIN 输入设备中插入一个 PIN 探测装置。这个装置被放置在设备外壳下方的键盘板 PCB 附近，其目的在于监测键盘信号并且记录 PIN 的输入：

识别阶段：

对设备进行逆向工程以熟悉其设计原理，包括入侵检测信号以及传感器信号。电子专业的专家进行安全信号的走线的解析，也对键盘信号的扫描方式进行确认。随后，定位入侵检测机制，并且设计攻破或绕过这些机制的方法。因此，这个过程需要 60 个工作时，专家技能，标准的设备，以及一个机械样本。

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	公开	无	1 个机械样本	60 小时

定制用于监控键盘信号以及记录PIN输入的bug。在此示例中，使用了简单的扫描技术，因此作出以下级别判定：专家，30工作时，标准部件，标准设备，重复使用了机械样本。

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	公开	标准	无	30 小时

使用带有测试密钥的工作样本进行验证实验注入测试密钥的操作以及对入侵响应的恢复工作需要有权使用密钥下载软件或者相关的说明，因此涉及到了限制知识。

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	受限	标准	1 个带测试密钥的功能样本	40 小时

对整个识别阶段进行总结，得到以下结果：

技术水平	设备	知识	部件	样本	攻击时间
专家	标准	受限	标准	1 个机械样本； 1 个带测试密钥的功能样本	130 小时

攻击阶段：

攻击者使用带有密钥的功能样本进行实际的攻击，需要以下几个步骤：

攻击入侵检测机制后，进入到终端内部。可以认为外壳能够被多余的部件替换，攻击每个检测机制的成功率可以达到0.9，并且每个机制需要用时1小时。在这个示例中，总共有八个入侵检测机制，但是只有其中四个需要进行攻击。需要额外的1小时用于攻击的稳定性。

尽管攻击方案被制定，仍然需要较好的机械技能以及保障成功的技巧。因此人员等级定为为“精通”。

技术水平	设备	知识	部件	样本	攻击时间
精通	标准（重复利用）	公开	无	1 个带工作密钥的功能样本； P=0.94≈0.66	5 小时

一旦进入到终端内部，攻击需要对终端较深层的敏感信号（例如，键盘扫描信号）进行定位，

这些信号由更为难攻破的，其他的入侵检测机制进行保护。

技术水平	设备	知识	部件	样本	攻击时间
专家	标准（重复利用）	公开	无	1 个带测试密钥的功能样本； P=0.8	12 小时

一旦成功完成上述步骤，攻击者能够在键盘线上进行bug的安装，替换外壳，并对终端进行测。

试。恢复后的终端可以还回到原商户或商店。专用设备需要用来植入 bug，取决于前面步骤中的受限制的访问。

技术水平	设备	知识	部件	样本	攻击时间
精通	专用	公开	标准（bug）	1 个带测试密钥的功能样本；P=1	6 小时

对攻击阶段进行总结，得到以下结论：

技术水平	设备	知识	部件	样本	攻击时间
专家	专用	公开	标准	1 个带测试密钥的功能样本；P≈0.52；因子为 1	23 小时

攻击分值见表 C.4：

表 C.4　插入一个 PIN 探测装置的攻击分值

相关方面	识别分析值		实施攻击值	
攻击时间	<=160 小时	5	<=24 小时	3
技术水平	专家	4	专家	4
对设备的知识	限制	2	公开	0
对 PIN 输入设备的访问	1 个机械样本；一个没有工作密钥的功能样本	4	有工作密钥的功能性样本 P≈0.52	4
设备	标准	1	专用	3
专用零件	标准	1	标准	1
每个阶段攻击分值		17		15
总共攻击分值		32		

C.6　攻击实例二

这个攻击的目标在于使用 DPA 确定 3DES 加密密钥，假定如下：

需要使用 PIN 输入设备的某个功能，这个功能提供 PIN 以供加密，此加密处理的密钥就是攻击目标。DPA 用到的数据，可从 PIN 输入设备外部接口获取。例如，没有对 PIN 输入设备执行进一步的物理攻击来获取需要的测试数据，并且 PIN 输入设备没有有效的防 DPA 的功能。攻击包含以下步骤：

a）　确定在 PIN 输入设备上运行 DPA 的方法。一般包含分析电子和逻辑接口。这个步骤需要专业的电子计算机知识。

b）　建立攻击方案，包含以一个自动控制的方式来操作 PIN 输入设备。由于需要大量的 PIN 输入，而这些输入很难手动进行，因此采用一种专门的机制来进行 PIN 的输入。该设备为定制设备，专门为这个攻击定做的，在分析阶段也会使用。

c）　得到一个 PIN 输入设备，并测试。需要观察至少 20000 个 PIN 输入以及随后的加密过程。在分析阶段可能会重复多次。由于需要穷举 PIN，所以 20000 个 PIN 输入至少需要 7 天。

由于这么大量的交易不可能在真实的交易环境中出现，因此极有可能和一个模拟主机运行离线交易。

d) 分析采样数据，得到 PIN 加密密钥。使用与第一个示例类似的手段，攻击分值的计算方法如表 C.5：

表C.5　DPA分析攻击分值

相关方面	识别值		攻击值	
攻击时间	＞160 小时	5.5	<80 小时	4
技术水平	专家	4	专家	4
对设备的知识	限制	2	公开	0
对 PIN 输入设备的访问	使用试验密钥的功能性样本	2	有工作密钥的功能性样本	4
设备	定做	5	专用	3
专用零件	标准	1	不需要其他的零件	0
每个阶段攻击分值		19.5		15
总共攻击分值		34.5		