ICS 35.240.15
L63

T/PCAC

中 国 支 付 清 算 协 会 标 准

T/PCAC 0004—2018

银行卡自动柜员机（ATM）终端检测规范

Testing specification on automatic teller machine （ATM） terminal for bank card

2018－03－01 发布　　2018－03－01 实施

中国支付清算协会安全与技术标准专业委员会 发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国支付清算协会提出。

本标准由中国支付清算协会安全与技术标准专业委员会归口。

本标准指导单位：中国人民银行。

本标准起草单位：：中国支付清算协会、北京中金国盛认证有限公司、中国金融电子化公司、北京银联金卡科技有限公司、易宝支付有限公司、广州广电运通金融电子股份有限公司等单位。

本标准主要起草人：蔡洪波、马国光、邢桂伟、于沛、欧阳明、聂丽琴、王翠、付小康、陈兰朋、郭栋、陈龙、孟飞宇、张永峰、侯晓晨、李瑞、孙嵩奇、刘成伟、林冠辰、陈占良、侯玉华等。

银行卡自动柜员机（ATM）终端检测规范

1 范围

本标准规定了银行卡自动柜员机终端的基本硬件、软件和安全的检测流程及通过标准。

本标准适用于中华人民共和国境内各种类型的银行卡自动柜员机终端设备。

2 规范性引用文件

下列文件对于本标准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标准。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。

JR/T 0025 《中国金融集成电路（IC）卡规范》

JR/T 0002 《银行卡自动柜员机（ATM）终端技术规范》

JR/T 0120.3 《银行卡受理终端安全规范 第3部分：自助终端》

JR/T 0120.5 《银行卡受理终端安全规范 第5部分：PIN输入设备》

中国人民银行.中国人民银行关于进一步加强银行卡风险管理的通知（银发〔2016〕170号）.2016年6月15日

中国人民银行.中国人民银行关于强化银行卡受理终端安全管理的通知（银发〔2017〕21号）.2017年1月23日

3 ATM终端硬件要求

3.1 硬件设计与结构设计

检测目的：硬件设计与结构设计应符合国家标准GB/T 18789的要求。

测试过程：查看厂商提交的硬件设计说明或相关报告等材料，检查厂商提供的资料是否与要求一致。

通过标准：硬件设计与结构设计应符合国家标准GB/T 18789的要求。

3.2 模块配置要求

检测目的：检测模块配置是否包含：电源模块、通讯模块、终端控制模块、显示模块、现金模块（存款机必备存款模块，取款机必备出钞模块）、卡处理模块、凭证打印模块、客户输入模块、数据安全模块（包括硬件加密模块）。可根据需要加装其他功能模块。

卡处理模块应支持受理符合JR/T 0025的接触式IC卡，应支持非接触式IC卡和移动支付设备的受理；

密码键盘应有防窥机体设计或者加装防窥罩；

ATM终端验钞功能、钞票冠字号码记录功能等应符合金融行业主管部门相关规定。

如自动柜员机不具备打印模块，应采取其他形式储存有效、关键的交易数据，并宜具有防篡改等保护措施。

各模块配置应符合 GB/T 18789 的要求。

测试过程：终端应依照实际的模块配置进行验证

通过标准：各模块配置符合 GB/T 18789 的要求。

卡处理模块支持受理符合 JR/T 0025 的接触式 IC 卡，应支持非接触式 IC 卡和移动支付设备的受理。

密码键盘有防窥机体设计或者加装防窥罩

ATM 终端验钞功能、钞票冠字号码记录功能等应符合金融行业主管部门相关规定。

不具备打印模块的自动柜员机具备其他形式存储有效、关键的交易数据，宜具有防篡改保护措施。

4 ATM 终端软件要求

4.1 软件设计和软件功能

检测目的：ATM 终端的软件设计、软件功能和产品的字符集及字型等应符合国家标准 GB/T 18789 的要求。

测试过程：查看厂商提交的软件设计说明或相关代码等材料，检查厂商提供的资料是否与要求一致。

通过标准：软件设计、软件功能和产品的字符集及字型等应符合国家标准 GB/T 18789 的要求。

4.2 软件配置

检测目的：ATM终端的软件配置要求如下：

a) 操作系统软件；

b) 硬件驱动和控制软件；

c) ATM 终端系统软件：

1) ATM 终端控制软件；

2) ATM 终端故障诊断软件（或具备故障诊断能力）。

d) ATM 安全控制软件（或具备安全控制能力）；

e) ATM 软件中间件（可选）；

f) ATM 终端辅助工具软件（可选）；

g) ATM 终端软件自动更新模块（可选）。

测试过程：检查 ATM 终端的软件配置。

通过标准：软件配置功能符合要求。

4.3 其他要求

4.3.1 卡号和磁条信息格式要求

检测目的：ATM 终端接受的银行卡卡号应按 JR/T 0008 的有关规定，磁条信息格式应按 GB/T 19584 的有关规定。

测试过程：对银行卡卡号及磁条信息进行有效性验证。

通过标准：ATM 终端接受的银行卡卡号应按 JR/T 0008 的有关规定。

银行卡磁条信息格式应按 GB/T 19584 的有关规定。

4.3.2 磁道处理要求

检测目的：ATM 终端应能正确地按顺序读取第二、三磁道并能根据 GB/T 19584 的相关规定准确地识别主账号，跨行操作不应对银行卡磁道内容进行任何更改。

测试过程：对 ATM 读取磁道信息功能进行有效性验证。

通过标准：ATM 根据 GB/T 19584 的相关规定准确地识别主账号，跨行操作不应对银行卡磁道内容进行任何更改。

4.3.3 IC 卡处理要求

检测目的：ATM 终端应按 JR/T 0025、JR/T 0091 的规定正确处理接触式、非接触式金融 IC 卡和移动支付设备。

测试过程：根据厂商提供资料和应用对 ATM 处理接触式、非接触式金融 IC 卡和移动支付设备功能进行有效性验证。

通过标准：ATM 根据 JR/T 0025、JR/T 0091 的规定正确处理接触式、非接触式金融 IC 卡和移动支付设备。

4.3.4 自检要求

检测目的：当 ATM 终端接受银行卡后，交易选择时，发现有关部件不能正常工作时，应有所提示或屏蔽相应功能，不应提供相应的操作选择。

测试过程：根据厂商提供资料和应用对 ATM 自检功能进行有效性验证。

通过标准：当 ATM 终端接受银行卡后，交易选择时，发现有关部件不能正常工作时，应有所提示或屏蔽相应功能，不应提供相应的操作选择。

5 ATM 终端安全要求

5.1 ATM 基本安全

5.1.1 终端硬件安全检测

5.1.1.1 硬件设计原则检测

检测目的：终端硬件设计应符合 JR/T 0120.3 中 4.1 的要求。

测试目的:查看厂商提交的硬件设计说明或相关报告等材料,检查厂商提供的资料是否与安全要求一致。

通过标准：厂商提供的资料与安全要求一致。

终端硬件设计符合 JR/T 0120.3 中 4.1 的要求。

5.1.1.2 电气安全检测

检测目的：终端的电气安全性应符合 GB 4943.1 的有关规定。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

终端的电气安全性符合 GB 4943.1 的有关规定。

5.1.1.3 抗破坏能力检测

检测目的：终端的抗破坏能力应满足 JR/T 0120.3 中附录 C 的有关要求。

测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料进行有效性验证。
通过标准：厂商提供的资料与安全要求一致。
终端的抗破坏能力应满足 JR/T 0120.3 中附录 C 的有关要求。

5.1.1.4 抗破坏报警检测

检测目的：终端遇到非操作员、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。
测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料进行有效性验证。
通过标准：厂商提供的资料与安全要求一致。
终端遇到非操作员、非管理员开启机柜或遇到暴力攻击等非正常使用时，必须能报警并有记录。

5.1.1.5 一机一钥检测

检测目的：自助终端的机柜钥匙应当实现一机柜一钥匙，不能多机柜共用一把钥匙，简称“一机一钥”的要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料进行有效性验证。
通过标准：厂商提供的资料与安全要求一致。
终端的保险柜钥匙须一保险柜一钥匙，不能多机共用一把保险柜钥匙。

5.1.1.6 读卡器等安全设备防移除检测

检测目的：终端的读卡器等安全设备要防止恶意拆除，攻击和绕开该保护功能的机制至少需要 18 分，实施攻击分值至少 9 分。分值计算方式应符合 JR/T 0120.5 的要求。
测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料，设计攻击场景使读卡器等安全设备移除，计算攻击分值。
通过标准：厂商提供的资料与安全要求一致。
终端的读卡器等安全设备能防止恶意拆除，攻击和绕开该保护功能的机制。
设计的攻击场景的攻击分值不低于 18 分，其中实施攻击分值最少 9 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.1.7 防恶意窃卡机制检测

检测目的：终端应具备安全机制，防止有目的地保留或偷取持卡人卡片（比如循环攻击）。
测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料进行有效性验证。
通过标准：厂商提供的资料与安全要求一致。
终端具备防止有目的地保留或偷取持卡人卡片的安全机制，可以有效抵抗循环攻击等攻击方式。

5.1.1.8 防渗透替换机制检测

检测目的：不允许通过条件改变、替换或修改磁条卡读写器、终端的硬件软件，达到替换或者修改磁道数据的目的，至少需要 16 分值，实施攻击分至少 8 分。分值计算方式应符合 JR/T 0120.5 的要求。

测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料，设计攻击场景使磁条卡读写器、终端的硬件软件达到替换或修改的目的，计算攻击分值。
通过标准：厂商提供的资料与安全要求一致。
设计的攻击场景的攻击总分至少 20 分，其中攻击阶段至少 10 分，攻击时间至少 10 个小时。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.1.9 其他硬件检测

检测目的：终端硬件设计应符合 JR/T 0120.3 中附录 A 的要求。
测试过程：查看厂商提交的硬件设计说明或相关报告等材料，检查厂商提供的资料是否与安全要求一致。
通过标准：厂商提供的资料与安全要求一致。
终端硬件设计符合 JR/T 0120.3 中附录 A 的要求。

5.1.2 软件安全性

5.1.2.1 软件设计原则检测

检测目的：终端软件设计应符合 JR/T 0120.3 中 5.1 的要求。
测试过程：查看厂商提交的软件设计说明或相关代码等材料，检查厂商提供的资料是否与安全要求一致。
通过标准：厂商提供的资料与安全要求一致。
终端软件设计符合 JR/T 0120.3 中 5.1 的要求。

5.1.2.2 系统软件检测

检测目的：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。
测试条件：适用时
测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料进行有效性验证。
通过标准：厂商提供的资料与安全要求一致。
软件具有系统初始化，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。

5.1.2.3 二次开发平台检测

检测目的：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。
测试条件：适用时
测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料进行有效性验证。
通过标准：厂商提供的资料与安全要求一致。
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。

5.1.2.4 模块化结构

检测目的：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。

测试条件：适用时

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

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

5.1.2.5 其他软件检测

检测目的：终端软件设计应符合 JR/T 0120.3 中附录 B 要求。

测试过程：查看厂商提交的软件设计说明或相关代码等材料，检查厂商提供的资料是否与安全要求一致。

通过标准：厂商提供的资料与安全要求一致。

终端软件设计符合 JR/T 0120.3 中附录 B 的要求。

5.1.3 逻辑安全性

5.1.3.1 非 PIN 数据输入检测

检测目的：验证终端的密码键盘需要输入非PIN数据，至少满足以下条件的一个：

a) 提示信息由加密单元控制： 输入非 PIN 数据时设备显示的提示内容应在安全模块的控制下，对非 PIN 数据的攻击至少需要 18 分攻击分值，实施攻击分至少 9 分。 如果该提示内容是存储在安全模块内部，那么改变该提示内容会导致安全模块内密钥的擦除。如果该提示内容是存储在安全模块外部，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；

b) 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）的攻击至少需要 16 分的攻击分值；

c) 安全模式：终端应确保持卡人可见信息与操作状态之间的关联关系。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查提示的控制是否安全。

设计攻击场景。

通过标准：厂商提供的资料与安全要求一致。

终端需要输入非PIN数据(包括但不限于通过密码键盘、触摸屏等模块输入)时，满足检测目的a)、b)、c)中的任意一条。

5.1.3.2 多应用隔离检测

检测目的：验证如果终端支持多个应用程序，则应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终端的操作系统，包括修改属于另外一个程序的数据对象。

测试过程：检查厂商提供的资料是否与安全要求是否一致。

评估设备支持的应用是否独立。

执行模拟交易或操作，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。

各应用间应相互独立。

一个应用程序不能干扰或篡改另外一个应用程序或终端的操作系统，包括修改属于另外一个程序的数据对象。

5.1.3.3 操作系统最小配置检测

检测目的: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。应以最少的特权来配置和运行。
测试过程：检查厂商提供的资料是否与安全要求一致。
确定设备的操作系统。
检查操作系统配置。
通过标准：厂商提供的资料与安全要求一致。
操作系统必须进行安全配置，须开通最小的权限设置。

5.1.3.4 单一的 PIN 数据接口检测

检测目的：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，应阻止通过这个接口接收 PIN 数据。
测试过程：检查厂商提供的资料是否与安全要求一致。
检查终端是否只具有一个支付密码输入接口。
检查终端如果有其他可用于输入的键盘接口，是否禁止该键盘作为支付密码输入使用。
通过标准：厂商提供的资料与安全要求一致。
终端只具有一个单独的接口接收 PIN 数据，例如一个键盘等。
如果另外有一个键盘，应阻止通过这个接口接收 PIN 数据。

5.1.4 PIN 输入设备

5.1.4.1 物理安全性要求

5.1.4.1.1 入侵检测机制

检测目的：PIN 输入设备应具备防攻击性机制，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 IC 卡读写器的攻击）的攻击分值，其中实施攻击分至少 13 分。
测试过程：检查厂商提供的资料是否与安全要求一致。
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：厂商提供的资料与安全要求一致。
设计的攻击场景的攻击分值不低于 26 分，其中实施攻击分值最少 13 分。攻击时间至少 10 个小时。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.1.2 独立安全机制

检测目的：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。
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。
检查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。
具有至少两个独立的安全机制。

5.1.4.1.3 内部访问响应

检测目的：若允许访问 PIN 输入设备或 IC 卡读写器内部区域（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。

测试过程：检查厂商提供的资料是否与安全要求一致。
实际查看终端内部访问响应区域有无敏感走线。

通过标准：若允许访问 PIN 输入设备或 IC 卡读写器内部区域（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。

5.1.4.1.4 环境和操作条件改变的适应性

检测目的：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）。

测试条件：操作电压或环境温度等超出设备正常应用范围。

测试过程：检查厂商提供的资料是否与安全要求一致。
查看厂商提供的相关资料，是否具有相应环境防护措施。

通过标准：厂商提供的资料与安全要求一致。
设备的安全性不能因环境条件或操作条件发生变化而降低。

5.1.4.1.5 敏感功能或信息保护

检测目的：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 IC 卡读写器的攻击），其中实施攻击分至少 13 分。

测试过程：检查厂商提供的资料是否与安全要求一致。
根据厂商提供资料，设计攻击场景获得敏感功能，计算攻击分值。

通过标准：厂商提供的资料与安全要求一致。
获得敏感信息需要 26 分的攻击分值，其中实施攻击分值最少 13 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.1.6 PIN 输入过程中可听到的音调

检测目的：如果 PIN 输入时有声音提示，那么输入每一位 PIN 所发出的声音和输入其他位 PIN 所发出的声音应保持一致或声音随机，无法辨别。

测试过程：检查厂商提供的资料是否与安全要求一致。
采集输入 PIN 时数字键按键音，使用分析工具进行分析。

通过标准：厂商提供的资料与安全要求一致。
无法根据提示音区别数字按键。

5.1.4.1.7 PIN 输入过程中监控

检测目的：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，其中实施攻击分至少 13 分。

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。
设计攻击场景获得 PIN，计算攻击分值。

通过标准：厂商提供的资料与安全要求一致。
攻击场景至少需要 26 分的攻击分值，其中实施攻击分值最少 13 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.1.8 密钥识别分析

检测目的：通过入侵或渗透 PIN 输入设备或 IC 卡读写器、监测 PIN 输入设备或 IC 卡读写器的辐射（包括能量波动）的方法获取在 PIN 输入设备或 IC 卡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。

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，对能量进行分析。

通过标准：厂商提供的资料与安全要求一致。
获取密钥至少需要 35 分攻击分值，其中实施攻击分值至少 15 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.1.9 非 PIN 数据输入提示信息物理安全

检测目的：输入非 PIN 数据时设备显示的提示内容应在安全模块的控制下，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模块内部，那么改变该提示内容会导致安全模块内密钥的擦除。如果该提示内容是存储在安全模块外部，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。

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，计算攻击分值。

通过标准：厂商提供的资料与安全要求一致。
访问到存储提示信息的攻击场景，至少需要 18 分攻击分值，其中实施攻击分值至少 9 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.1.10 移除检测（仅适用于 EPP）

检测目的：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，其中实施攻击分至少 9 分。

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，计算攻击分值。

通过标准：厂商提供的资料与安全要求一致。
攻击场景至少需要攻击分 18 分，其中实施攻击分值最少 9 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.1.11 防偷窥保护

检测目的：PIN 输入设备的设计应防止其他人对 PIN 输入的窥视，具体要求参考 JR/T 0120.5 附录 A。

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。测试方法参见 JR/T 0120.5 附录 A。

5.1.4.1.12 磁条读卡器（适用于任何带有集成式磁条读卡器的有人值守式 POS-PED，EPP 可选）

检测目的：在攻击分值低于 16 分（实施攻击分 8 分）的条件下，通过入侵 PIN 输入设备安装附加物、替代或修改磁条阅读器的磁头和相关软硬件的方式，从而获取或修改磁道数据都是不可行的。

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，计算攻击分值。

通过标准：厂商提供的资料与安全要求一致。
攻击场景的攻击分值不低于 16 分，实施攻击总分不低于 8 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.2 逻辑安全性要求

5.1.4.2.1 自检测试

检测目的：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，设备每 24 小时内至少重新初始化内存。自检包括检查固件、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。

测试过程：检查厂商提供的资料是否与安全要求一致。
执行任何需要的测试验证。

通过标准：厂商提供的资料与安全要求一致。
设备每 24 小时内要至少重新初始化内存一次。
一旦设备处于被攻击状态，本身及其功能会以安全的方式失去效用。
设备在启动时自检，并且至少每天进行一次自检。

5.1.4.2.2 逻辑异常

检测目的：PIN 输入设备不应受异常逻辑的影响而泄露 PIN 的明文或其他敏感数据，这些异常逻辑包括但不限于：错误的命令序列、未知命令、错误模式下的命令和错误的参数。

测试过程：检查厂商提供的资料是否与安全要求一致。
执行任何需要的测试验证。

通过标准：厂商提供的资料与安全要求一致。
终端不受逻辑异常的影响。

5.1.4.2.3 固件认证

检测目的：设备固件及对固件的任何改动都应经过严格的流程控制，以保证固件中不含隐藏的非法功能。

测试过程：检查厂商提供的资料是否与安全要求一致。
检查任何厂商提供的附加相关文档，验证机制与厂商声明的一致。

通过标准：厂商提供的资料与安全要求一致。
固件和应用及后续的任何改动应该被严格控制，并保证固件中不含隐藏的、非法功能。

5.1.4.2.4 固件更新

检测目的：如果 PIN 输入设备固件能够进行更新，那么设备应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。

测试过程：检查厂商提供的资料是否与安全要求一致。
检查任何厂商提供的附加相关文档，验证机制与厂商声明的一致。
通过标准：厂商提供的资料与安全要求一致。
验证如果设备允许固件更新，设备应加密验证固件的完整性和真实性，如果验证未通过，固件更新应被拒绝并删除。
验证如果设备允许应用更新，设备应加密验证应用的完整性和真实性，如果验证未通过，应用更新应被拒绝并删除。

5.1.4.2.5 输入 PIN 区别

检测目的：PIN 输入设备在任何情况下都不显示或者泄漏 PIN 的明文。任何和 PIN 相关的数据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。同时应保证这些密码的输出只能输出至显示设备接口上，其他接口连接屏无法显示。对于加密密码键盘，加密密码键盘从不向另外一个部件输出信息（比如，显示屏或设备控制器），从而能够对输入的 PIN 数字进行区分。
测试过程：检查厂商提供的资料是否与安全要求一致。
执行模拟交易进行验证。
通过标准：厂商提供的资料与安全要求一致。
PIN 输入设备不能显示或者泄漏输入的 PIN 数字。任何与输入 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。同时这些密码的输出只能输出至显示设备接口上，其他接口连接屏无法显示。加密密码键盘从不向另外一个部件输出信息（比如，显示屏或设备控制器），能够对输入的 PIN 数字进行区分。

5.1.4.2.6 内存清除

检测目的：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应自动清空其内部保存的敏感信息：
a) 交易已经完成；
b) PIN 输入设备等待持卡人或商户的响应超时。
测试过程：检查厂商提供的资料是否与安全要求一致。
检查其它的相关文档，来验证机制与厂商声明的一致。
通过标准：厂商提供的资料与安全要求一致。
在交易完成或设备等待持卡人或商户响应超时时，设备必须自动清除内部缓存。

5.1.4.2.7 敏感服务保护

检测目的：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应通过身份验证。进入或退出敏感服务不应泄露或改变设备中的敏感信息。
测试过程：检查厂商提供的资料是否与安全要求一致。
检查使用敏感服务是否泄露或改变设备中的敏感信息。
通过标准：厂商提供的资料与安全要求一致。
使用敏感服务不泄露或改变设备中的敏感信息。

5.1.4.2.8 敏感服务限制

检测目的：为保证设备的敏感服务不被非法使用，应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。

测试过程：检查厂商提供的资料是否与安全要求一致。
检查是否对敏感服务的操作次数和时间进行强制限制。
通过标准：厂商提供的资料与安全要求一致。
对敏感服务的操作次数和时间进行强制限制。

5.1.4.2.9 随机数

检测目的：如果PIN输入设备产生的随机数与敏感数据有关系，则设备中的随机数产生器应经过评估，以保证其产生的随机数无法被预测。
测试过程：检查厂商提供的资料是否与安全要求一致。
使用随机数测试工具对随机数随机性进行测试。
通过标准：厂商提供的资料与安全要求一致。
随机数具有足够的随机性。

5.1.4.2.10 PIN 防穷举

检测目的：PIN 输入设备应具有防止利用穷举探测 PIN 值的特性。
测试过程：检查厂商提供的资料是否与安全要求一致。
检查设备是否具有防止利用穷举探测 PIN 值的能力。
通过标准：厂商提供的资料与安全要求一致。
设备应能防止利用盗取的设备穷举探测获得 PIN 值。

5.1.4.2.11 密钥管理

检测目的：PIN 输入设备中执行密钥管理技术需要符合 ISO 11568 和/或 ANSI X9.24。有关 TDES 密钥组的密钥管理技术符合 ANSI TR-31。
测试过程：检查厂商提供的资料是否与安全要求一致。
检查密钥管理技术是否满足 ISO 11568 和/或 ANSI X9.24 的密钥管理规则的要求。
通过标准：厂商提供的资料与安全要求一致。
设备执行密钥管理技术需要同时遵守 ISO 11568 和 ANSI X9.24。密钥管理技术必须支持 ANSI TR-31 或者一个等价的方法。

5.1.4.2.12 加密算法测试

检测目的：PIN 输入设备采用的 PIN 加密技术应遵循 ISO 9564。
测试过程：检查厂商提供的资料是否与安全要求一致。
执行模拟交易，验证 PIN 加密算法符合要求。
通过标准：厂商提供的资料与安全要求一致。
设备中执行的 PIN 加密技术是 ISO 9564 中规定的技术。

5.1.4.2.13 对设备中任意数据加解密

检测目的：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 输入设备应强制使数据密钥（指 MAC 密钥和磁道加密密钥），密钥加密密钥和 PIN 加密密钥有不同的值。
测试过程：检查厂商提供的资料是否与安全要求一致。
检查是否能利用设备内的工作密钥或密钥加密密钥去加密或解密不应由其加解密的其他任意数据。

检查数据密钥、PIN 加密密钥、密钥加密密钥是否具有不同的值。

通过标准：厂商提供的资料与安全要求一致。

不能利用设备内的工作密钥或密钥加密密钥去加密或解密不应由其加解密的其他任意数据。

数据密钥、PIN 加密密钥、密钥加密密钥应具有不同的值。

5.1.4.2.14 明文密钥安全

检测目的：PIN 输入设备的机制应保证：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。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查设备是否允许输出私钥或密钥以及 PIN 的明文。

检查设备是否允许用已经泄密或存在已经泄露可能性的密钥去加密其他密钥或 PIN。

检查设备是否允许把密钥明文从高安全性的组件传送至低安全性的组件中去。

通过标准：厂商提供的资料与安全要求一致。

不允许输出私钥或密钥以及 PIN 的明文。

不允许用已经泄密或存在已经泄露可能性的密钥去加密其他密钥或 PIN。

不允许把密钥明文从高安全性的组件传送至低安全性的组件中去。

5.1.4.2.15 交易控制

检测目的：输入其他交易数据的过程应和输入 PIN 的过程分开，以避免 PIN 的明文意外显示。如果其他交易数据和 PIN 是通过同一个键盘输入，那么输入其他交易数据和 PIN 时设备应有明显提示进行区别。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查输入其他交易数据的过程是否和输入 PIN 的过程分开。

如果其他交易数据和 PIN 是通过同一个键盘输入，检查输入交易金额和 PIN 时设备是否有明显提示进行区别。

通过标准：厂商提供的资料与安全要求一致。

输入其他交易数据的过程必须和输入 PIN 的过程分开。

如果其他交易数据和 PIN 是通过同一个键盘输入，那么输入交易金额和 PIN 时设备应有明显提示进行区别。

5.1.4.2.16 非 PIN 数据输入提示信息逻辑安全

5.1.4.2.16.1 改变用户界面提示攻击可能性分析

检测目的：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）。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查提示的控制是否安全。

设计攻击场景。

通过标准：厂商提供的资料与安全要求一致。

改变非 PIN 数据输入时显示的提示内容至少需要 18 分攻击分值，其中实施攻击分值至少 9 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.2.16.2 基于加密的控制

检测目的：对于具有可变显示功能的PIN输入设备，设备的显示应在安全模块控制下进行，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，并且提供有效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）。

测试过程：检查厂商提供的资料是否与安全要求一致。
检查提示的控制是否安全。
设计攻击场景。

通过标准：厂商提供的资料与安全要求一致。
改变非PIN数据输入时显示的提示内容至少需要18分攻击分值，其中实施攻击分值至少9分。攻击分值计算公式参见JR/T 0120.5附录B。

5.1.4.2.16.3 设备多应用

检测目的：如果设备支持多应用，应保证各应用间的相互独立，其中任何应用不能干扰其他应用和操作系统，包括不能修改属于其他应用的数据对象。

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否独立。
执行模拟交易或操作，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。
各应用间应相互独立。
一个应用不能干扰或损害另一个应用或者操作系统，包括修改属于其他应用的数据或者操作系统。

5.1.4.2.17 操作系统

检测目的：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，操作系统应进行安全配置，开通尽量少的权限设置。

测试过程：检查厂商提供的资料是否与安全要求一致。
确定设备的操作系统。
检查操作系统配置。

通过标准：厂商提供的资料与安全要求一致。
操作系统必须进行安全配置，须开通最小的权限设置。

5.1.4.2.18 集成指南

检测目的：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。

测试过程：检查厂商提供的资料是否与安全要求一致。
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：厂商提供的资料与安全要求一致。
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。

5.1.4.2.19 安全策略

检测目的：终端生产厂商提供给用户一个关于终端正确使用的安全策略，需包括：密钥管理责任、行政责任、设备功能、规格书、以及环境要求。该安全策略应定义终端支持的规则，并以确定的表格形式明确给出每个规则的可接受服务。

终端仅可执行它确定的功能，例如：不能有隐藏的功能。经过认证的功能属于安全策略许可的范围之内。

测试过程：检查厂商提供的资料是否与安全要求一致。

设计测试案例，验证生产安全管理措施的有效性。

检查厂商提交的文件，是否具有正确使用终端的安全策略，检查包含的内容及安全策略的规则，并以确定的表格形式明确给出每个规则的可接受服务。

检查设计测试案例终端是否仅可执行它确定的功能，例如：不能有隐藏的功能。经过认证的功能属于安全策略许可的范围之内。

通过标准：厂商提供的资料与安全要求一致。

设备安全管理策略符合要求。

设备安全管理措施有效。

5.1.4.2.20 远程密钥发布

检测目的：如果使用了远程密钥发布技术，需支持发送方与接受方之间的双向认证。破坏密钥发布过程不能导致密钥被泄露。

测试过程：厂商提供的资料与安全要求一致。

设计测试案例，验证远程密钥更新的安全性。

通过标准：检查厂商提供的资料是否与安全要求一致。

设备如果使用远程密钥发布技术，则应支持发送发与接收方之间的双向认证。

5.1.4.3 联机终端的安全要求

检测目的：如果 PIN 输入设备能够保存多个 PIN 加密密钥而且能够在外部选择，那么设备安全机制应防止密钥被非法替换和使用。

测试过程：检查厂商提供的资料是否与安全要求一致。

通过标准：厂商提供的资料与安全要求一致。

设备禁止未经授权的密钥替换和密钥滥用。

5.1.4.4 脱机终端安全要求

5.1.4.4.1 防穿透保护

检测目的：在要求攻击分值小于 20 分（实施攻击分 10 分）的情况下，任何渗透 IC 卡读写器从而附加、替换和修改 IC 卡读写器的软件或硬件，以获取或修改任何敏感数据的攻击都是不可行的。

测试过程：检查厂商提供的资料是否与安全要求一致。

验证声明的保护措施存在并且和厂商在文档中描述的一致。

通过标准：厂商提供的资料与安全要求一致。

设计的攻击场景的攻击总分至少 20 分，其中攻击阶段至少 10 分，攻击时间至少 10 个小时。

攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.4.2 IC 卡读写器卡槽结构

检测目的：在插入 IC 卡时，IC 卡读写器插槽应没有空间被装入 PIN 窃取装置，要增大设备空间来容纳

这种窃取装置也是不可行的。IC 卡和其他任何外物不可能同时驻留在 IC 卡读卡器插槽内。
在卡插入过程中，IC 卡插槽的入口处可完全处于持卡人的监控下，这样在插槽入口处的任何可疑物都可以被发觉。

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，执行测试确定其可行性。

通过标准：厂商提供的资料与安全要求一致。
在插入 IC 卡时，IC 卡读写器插槽没有空间被装入 PIN 窃取装置，IC 卡和其他任何外物不可能同时驻留在 IC 卡读卡器插槽内。
在卡插入过程中，IC 卡插槽的入口处可完全处于持卡人的监控下，在插槽入口处的任何可疑物都可以被发觉。

5.1.4.4.3 IC 卡读卡器构造（连线）

检测目的：IC 卡读写器的构造可以保证任何从 IC 卡读写槽到外部记录器或发射机（外部窃取装置）的连接线都可以被持卡人观察到。

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，执行测试确定其可行性。

通过标准：厂商提供的资料与安全要求一致。
IC 卡读写器的构造可以保证任何从 IC 卡读写槽到外部记录器或发射机（外部窃取装置）的连接线都可以被持卡人观察到。

5.1.4.4.4 PIN 输入设备和 IC 卡读卡器间 PIN 传输保护

检测目的：在PIN输入设备中传输时PIN的保护（至少满足下列的一条）：

a) 如果 PIN 输入设备和 IC 卡读写器没有集成在一起，且验证持卡人方式为加密 PIN 验证，那么在 PIN 输入设备和 IC 卡读写器之间传送的 PIN BLOCK 应通过 IC 卡上的加密密钥进行加密，或与 ISO 9564 加密要求保持一致；
b) 如果 PIN 输入设备和 IC 卡读写器没有集成在一起，且验证持卡人方式为明文 PIN 验证，那么从 PIN 输入设备向 IC 卡读写器传送的 PIN BLOCK 应按照 ISO 9564 要求进行加密；
c) 如果 PIN 输入设备和 IC 卡读写器集成在一起，且验证持卡人方式为加密 PIN 验证，那么 PIN BLOCK 应通过 IC 卡上的加密密钥进行加密；
d) 如果 PIN 输入设备和 IC 卡读写器集成在一起，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。
e) 如果明文 PIN 在未受保护环境中从 PIN 输入设备传输至 IC 卡读写器，则 PIN BLOCK 应按照 ISO 9564 要求进行加密。

测试过程：检查厂商提供的资料,必须明显的表明PIN BLOCK 在PIN输入设备和IC卡读写器之间传送时通过IC卡上的加密密钥进行加密，或与ISO9564加密要求保持一致。
检查所有相关的文件，比如图纸等这些由厂商提交的证明自身符合安全的要求的文件。

通过标准：厂商提供的资料与安全要求一致。
如果 PIN 输入设备和 IC 卡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 IC 卡读写器之间传送的 PIN BLOCK 必须通过 IC 卡上的加密密钥进行加密，或与 ISO9564 加密要求保持一致。
如果 PIN 输入设备和 IC 卡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 IC 卡读写器传送的 PIN BLOCK 必须按照 ISO9564 要求进行加密。
如果 PIN 输入设备和 IC 卡读写器集成在一起，且验证持卡人方式为明文 PIN 验证，那么 PIN

BLOCK 在受保护环境（ISO9564）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 IC 卡读写器，则 PIN BLOCK 应按照 ISO9564 要求进行加密。

如果 PIN 输入设备和 IC 卡读写器集成在一起，且验证持卡人方式为加密 PIN 验证，那么 PIN BLOCK 必须通过 IC 卡上的加密密钥进行加密。

5.1.4.5 集成安全要求

5.1.4.5.1 配置管理

检测目的：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，应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。

测试过程：检查厂商提供的资料是否与安全要求一致。

分析终端内的安全组件，检查是否明确定义其物理和逻辑安全边界。

通过标准：厂商提供的资料与安全要求一致。

集成到终端内的任何安全组件明确定义其物理和逻辑安全边界。

5.1.4.5.2 PIN 输入功能集成

检测目的：PIN输入功能集成安全要求：

a) 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；

b) 对 PIN 输入设备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 PIN 输入设备受攻击的风险。如对 PIN 输入设备的攻击至少需要攻击总分 18 分，其中实施攻击分 9 分。

测试过程：检查厂商提供的资料是否与安全要求一致。

分析终端内的已通过认证的安全组件，是否影响整个设备保护级别。

根据厂商提供资料，设计攻击场景获取 PIN，计算攻击分值。

通过标准：厂商提供的资料与安全要求一致。

终端内的已通过认证的安全组件，不影响整个设备保护级别。

设计的攻击场景的攻击分值不低于 18 分，其中攻击阶段最少 9 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.5.3 终端集成

5.1.4.5.3.1 全等级保持

检测目的：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。

测试过程：检查厂商提供的资料是否与安全要求一致。

分析终端内的已通过认证的安全组件，是否会引入新的攻击PIN或其他敏感数据的方式。

通过标准：厂商提供的资料与安全要求一致。

终端内的已通过认证的安全组件，不会引入新的攻击PIN或其他敏感数据的方式。

5.1.4.5.3.2 防卡片盗取

检测目的：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）。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查终端是否能够防止银行卡被恶意保存或盗取（如 Lebanese Loop attack）。

通过标准：厂商提供的资料与安全要求一致。

终端能够防止银行卡被恶意保存或盗取（如 Lebanese Loop attack）。

5.1.4.5.3.3 组件隔离

检测目的：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。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查设备的安全组件和非安全组件之间是否有明显的逻辑和/或物理隔离。

通过标准：厂商提供的资料与安全要求一致。

设备的安全组件和非安全组件之间要有明显的逻辑和/或物理隔离。

5.1.4.5.3.4 设备显示安全

检测目的：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。对持卡人操作动态显示信息和系统操作状态之间修改的攻击，攻击总分至少 18 分，其中实施攻击分 9 分。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查终端在应用执行过程中，持卡人可见的显示信息和终端操作状态是否保持一致性。

针对外部设备更改显示信息和操作状态的命令，检查该命令是否已被密码授权校验通过。

根据厂商提供资料，设计攻击场景尝试对持卡人操作动态显示信息和系统操作状态修改。

通过标准：厂商提供的资料与安全要求一致。

在应用执行过程中，持卡人可见的显示信息和终端操作状态保持一致性。

如果接收到来自外部设备更改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。

设计的攻击场景的攻击分值不低于 18 分，其中攻击阶段最少 9 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

5.1.4.5.3.5 密码输入接口控制

检测目的：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，例如可采取无有效数字键、对输入的数字不可用。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查终端是否只具有一个支付密码输入接口。

检查终端如果有其他可用于输入的键盘接口，是否禁止该键盘作为支付密码输入使用。

通过标准：厂商提供的资料与安全要求一致。

终端只具有一个支付密码输入接口，例如一个键盘等。

如果终端有其他可用于输入的键盘接口，应禁止该键盘作为支付密码输入使用。

5.1.4.5.3.6 设备移除要求

检测目的：终端应具有防止未授权移除组件机制。攻击这种防止移除机制需要攻击总分 18 分，其中实施攻击分 9 分；供应商应对文档持续地维护更新，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。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查终端是否具有防止未授权移除组件的机制。

根据厂商提供资料，设计攻击场景尝试未授权移除组件。

检查终端厂商是否具有相应文档并进行持续的维护更新，以保证集成使用者了解如何保护系统、防止未授权的移除。

对于嵌入式设备，检查是否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。

通过标准：厂商提供的资料与安全要求一致。

终端具有防止未授权移除组件的机制。

设计的攻击场景的攻击分值不低于 18 分，其中攻击阶段最少 9 分。攻击分值计算公式参见 JR/T 0120.5 附录 B。

终端厂商具有相应文档并进行持续的维护更新。

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。

5.1.5 网络开放协议的安全要求

5.1.5.1 IP 和链路层要求

检测目的：为保证计算机网络相互连接通信安全，厂商应保证IP和链路层整体满足下列安全要求：

a) 应准确识别出系统平台中开放协议定义的所有链路层选项；

b) 对 IP 层和链路层进行受攻击脆弱性评估，以保证 IP 层和链路层没有受攻击弱点。通过以下方式实现：

1) 根据安全文档进行评估；

2) 根据公共域的信息反馈进行评估；

3) 通过一些测试进行评估。

c) 供应商应不断更新维护安全指南，描述 IP 层和链路层如何被使用。安全指南提供给应用开发者、系统集成者以及终端用户如何使用的引导。安全指南应保证 IP 层和链路层使用的安全性；

d) IP 协议的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权形式进行更新，一旦认证不通过，应禁止更新。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查设备是否能识别出系统平台中开放协议定义的所有链路层选项。

检查是否具备针对 IP 层和链路层的受攻击脆弱性评估文档。

检查设备是否经过受攻击脆弱性评估并且确保 IP 层和链路层不存在受攻击弱点。

检查是否具有对如何使用 IP 层和链路层进行了描述的安全指南，安全指南是否不断更新。

检查安全指南是否提供了给应用开发者、系统集成者以及终端用户如何使用的引导，并保证 IP 层和链路层使用的安全性。

检查 IP 协议的默认配置是否与安全指南一致。

检查如果设备进行配置更新，是否采用密码授权形式进行更新，认证不通过时，是否禁止更新。

通过标准：厂商提供的资料与安全要求一致。

设备能识别出系统平台中开放协议定义的所有链路层选项。

具备针对 IP 层和链路层的受攻击脆弱性评估文档。

设备经过受攻击脆弱性评估并且确保 IP 层和链路层不存在受攻击弱点。

具有对如何使用 IP 层和链路层进行了描述的安全指南，安全指南不断更新。

安全指南提供给应用开发者、系统集成者以及终端用户如何使用的引导，并能保证 IP 层和链路层使用的安全性。

IP 协议的默认配置与安全指南一致。

设备进行配置更新时，采用密码授权形式进行更新，认证不通过时，禁止更新。

5.1.5.2 IP 协议要求

检测目的：为保证计算机网络相互连接通信安全，IP协议应满足以下安全：

a) 应清楚地识别出系统平台中定义的所有 IP 协议项；

b) 对 IP 协议执行脆弱性评估，保证使用 IP 协议无明显容易受攻击的弱点。评估通过以下几种方式：

1) 根据 IP 协议安全文档进行评估；

2) 根据公共域信息反馈进行评估；

3) 通过一些测试进行评估。

c) 供应商应维护安全指南，描述 IP 协议如何被使用。安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作的引导，应保证使用 IP 协议的安全性；

d) IP 协议的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权方式的更新，一旦认证不通过，应禁止更新。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查设备是否能清楚地识别出系统平台中定义的所有 IP 协议项。

检查是否进行了 IP 协议执行脆弱性评估，使用 IP 协议无明显容易受攻击的弱点。

检查是否具备由供应商维护的描述 IP 协议如何被使用的安全指南。

检查安全指南是否能为应用开发者、系统集成者和系统平台使用者提供安全处理操作的引导，并保证使用 IP 协议的安全性。

检查 IP 协议的默认配置是否与安全指南一致。

检查如果设备进行配置更新，是否采用密码授权形式进行更新，认证不通过时，是否禁止更新。

通过标准：厂商提供的资料与安全要求一致。

设备能清楚地识别出系统平台中定义的所有 IP 协议项。

进行了 IP 协议执行脆弱性评估，使用 IP 协议无明显容易受攻击的弱点。

具备由供应商维护的安全指南，描述了 IP 协议如何被使用。

安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作的引导，并保证使用 IP 协议的安全性。

IP 协议的默认配置与安全指南一致。

如果设备进行配置更新，采用密码授权形式进行更新，认证不通过时，是否禁止更新。

5.1.5.3 安全协议要求

检测目的：为保证计算机网络相互连接通信安全，厂商应实现满足安全协议的功能要求，如 SSL/TLS，IPSec 协议等，同时作为一个整体满足下列安全要求：

a) 应保证可以完全识别系统平台上开放协议定义的所有安全协议项；

b) 对安全协议进行脆弱性评估，以保证安全协议的使用不具有明显易受攻击弱点。评估采用以下方式实现：

1) 根据安全协议文档进行评估；

2) 根据公共域信息反馈进行评估；

3) 通过一些测试进行评估。

c) 系统平台供应商应维护安全指南，描述安全协议如何被使用：

1) 安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作引导；
2) 应保证使用安全协议的安全性；
3) 安全指南应明确提出相关的安全协议是否能够作为金融应用或系统平台管理应用；
4) 安全指南应明确指出安全协议相关配置是否能应用于金融应用或系统平台管理应用。

d) 协议的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权更新，一旦认证不通过，应禁止更新；

e) 系统平台供应商应进行密钥管理安全指南的管理和维护，描述密钥和证书应如何被使用：
1) 密钥管理指南为系统平台中的内部使用者、应用开发者、系统集成者和终端使用者提供密钥管理的安全引导；
2) 密钥管理安全指南要描述系统平台上所有密钥和证书的属性；
3) 密钥管理安全指南保证密钥和证书使用的安全。

f) 安全协议应保证网络传输数据的保密性，加密机制采用适合相关算法的密钥长度，在安全模式下使用合理的密钥管理程序加密，如NIST SP800-21；

g) 安全协议为网络传输连接提供完整数据，采用MAC协议或数字签名实现数据完整性一致性，哈希算法采用SHA-224、SHA-256、SHA-384、SHA-512中的一种，杂凑算法采用SM3；

h) 安全协议对服务进行授权：
1) 服务授权应使用对应相关算法合适的密钥长度；
2) 系统平台能够验证接收到公钥的有效性；
3) 系统平台能够验证接收到公钥的权限。

i) 安全协议能够监控信息反馈，并对异常进行处理；

j) 安全协议利用随机发生器校验NIST SP 800-22等。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查设备是否可以完全识别系统平台上开放协议定义的所有安全协议项。

检查是否对安全协议进行脆弱性评估，以保证安全协议的使用不具有明显易受攻击弱点。

检查系统平台供应商是否维护了描述安全协议如何被使用的安全指南。

检查协议的默认配置是否与安全指南一致,如果设备进行配置更新,是否采用密码授权更新，认证不通过时，是否禁止更新。

检查系统平台供应商是否进行密钥管理安全指南的管理和维护,是否描述了密钥和证书应如何被使用。

检查安全协议能否保证网络传输数据的保密性。

检查安全协议能否为网络传输连接提供完整数据。

检查安全协议是否对服务进行授权。

检查安全协议是否能够监控信息反馈，并对异常进行处理。

检查安全协议是否利用随机发生器校验NIST SP 800-22等。

通过标准：厂商提供的资料是否与安全要求一致。

设备可以完全识别系统平台上开放协议定义的所有安全协议项。

对安全协议进行了脆弱性评估，安全协议的使用不具有明显易受攻击弱点。

系统平台供应商维护安全指南，安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作引导；保证使用安全协议的安全性；明确提出相关的安全协议是否能够作为金融应用或系统平台管理应用;明确指出安全协议相关配置是否能应用于金融应用或系统平台管理应用。

协议的默认配置与安全指南一致，如果设备进行配置更新，采用密码授权更新，认证不通过时，禁止更新。

密钥管理指南为系统平台中的内部使用者、应用开发者、系统集成者和终端使用者提供密钥管理的安全引导；描述了系统平台上所有密钥和证书的属性；保证密钥和证书使用的安全。

安全协议可保证网络传输数据的保密性，加密机制采用适合相关算法的密钥长度，在安全模式下使用合理的密钥管理程序加密，如NIST SP800-21。

安全协议可为网络传输连接提供完整数据，采用MAC协议或数字签名实现数据完整性一致性，哈希算法采用SHA-224、SHA-256、SHA-384、SHA-512中的一种，杂凑算法采用SM3。

服务授权使用对应相关算法合适的密钥长度；系统平台能够验证接收到公钥的有效性；系统平台能够验证接收到公钥的权限。

安全协议能够监控信息反馈，并对异常进行处理。

安全协议利用随机发生器校验NIST SP 800-22等。

5.1.5.4 IP服务要求

检测目的：为保证计算机网络相互连接通信安全，厂商应实现IP服务的要求，如DNS、DHCP、HTTP、FTP等。

a) 应完全识别系统平台中开放协议定义的 IP 服务项；

b) 对 IP 服务进行脆弱性评估，以保证 IP 服务中不包含明显的易受攻击弱点。通过以下方式实现：

1) 通过文档分析对服务安全性进行评估；
2) 根据公共域信息反馈进行评估；
3) 通过一些测试进行评估。

c) 供应商应维护安全指南，描述 IP 服务如何被使用：

1) 安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作引导；
2) 应保证使用 IP 服务的安全性；
3) 安全指南应明确提出相关的 IP 服务是否能够作为金融应用或系统平台管理应用；
4) 安全指南应明确指出 IP 服务相关配置是否适用于金融应用或系统平台管理应用。

d) IP 服务的默认配置应与安全指南一致，如果设备进行配置更新，应采用密码授权形式的更新，一旦认证不通过，应禁止更新；

e) 系统平台实现会话层管理：

1) 系统平台保持对所有连接的跟踪，将活动的会话数量约束在最小必要范围值内；
2) 系统平台对会话设置时间限制，保证会话开放时间限制在一定范围内。

f) 使用合理的安全协议保证 IP 服务的机密性和完整性，并实现对 IP 服务的密码授权和防止重复使用。

测试过程：检查厂商提供的资料是否与安全要求一致。

对IP服务进行脆弱性评估，检查IP服务中是否包含明显的易受攻击弱点。

检查供应商是否维护了描述IP服务如何被使用的安全指南。

检查IP服务的默认配置是否与安全指南一致，如果设备进行配置更新，是否采用密码授权更新，认证不通过时，是否禁止更新。

检查系统平台是否实现了会话层管理。

检查是否使用合理的安全协议保证IP服务的机密性和完整性，并实现对IP服务的密码授权和防止重复使用。

通过标准：厂商提供的资料与安全要求一致。

对IP服务进行脆弱性评估，IP服务中不包含明显的易受攻击弱点。
供应商维护安全指南，安全指南为应用开发者、系统集成者和系统平台使用者提供安全处理操作引导；保证使用IP服务的安全性；明确提出相关的IP服务是否能够作为金融应用或系统平台管理应用；明确指出IP服务相关配置是否适用于金融应用或系统平台管理应用。
IP服务的默认配置与安全指南一致，如果设备进行配置更新，采用密码授权形式的更新，认证不通过时，禁止更新。
系统平台实现会话层管理：系统平台保持对所有连接的跟踪，将活动的会话数量约束在最小必要范围值内；系统平台对会话设置时间限制，保证会话开放时间限制在一定范围内。
使用合理的安全协议保证IP服务的机密性和完整性，并实现对IP服务的密码授权和防止重复使用。

5.1.5.5 安全管理要求

检测目的：安全管理要求如下：

a) 供应商应维护安全指南，对系统平台的配置管理作相关描述：
   1) 安全指南为系统平台提供内部使用者、应用开发者、系统集成者和终端使用者提供安全使用引导；
   2) 安全指南应覆盖整个系统平台，包括固件、应用软件、密钥和证书；
   3) 安全指南应覆盖整个系统平台的生命周期，从设计开发、出厂、交付使用及操作过程
   4) 安全指南应保证禁止未授权修改行为；
   5) 安全指南应保证任何对已通过认证系统平台做影响安全性能修改，会导致系统平台标识符改变。

b) 供应商推出安全维护的措施：
   1) 形成安全维护策略文档；
   2) 通过周期执行易受攻击脆弱性评估，保证及时检测易受攻击的弱点，例如报告分析、公共域信息反馈和测试；
   3) 应保证及时评估和分类最新发现的易受攻击弱点；
   4) 应保证及时建立缓解最新发现漏洞影响的机制。

c) 系统平台供应商对易受攻击的漏洞进行公开批露：
   1) 以文档形式保存相关漏洞信息；
   2) 保证及时公布最新发现易受攻击漏洞的信息，包括标识符、标识信息和漏洞相关的评估；
   3) 提供及时缓解漏洞危害的方法。

d) 系统平台可以被更新，供应商应维护更新机制描述，提供更新是如何实现：
   1) 更新机制采用恰当的、被认证的安全协议保证系统平台信息的机密性和完整性，对服务进行授权并防止重复使用。如果设备允许进行软件和配置更新，设备应采用加密授权，一旦授权不成功，则更新失败中止；
   2) 系统平台供应商为应用开发者、系统集成者和终端使用者提供更新最新系统平台的安全指南；
   3) 安全指南应覆盖固件、应用、密钥和证书的更新；

测试过程：检查厂商提供的资料是否与安全要求一致。
检查供应商是否维护了安全指南，安全指南是否对系统平台的配置管理作相关描述。
检查供应商是否推出安全维护的措施。

检查系统平台供应商是否对易受攻击的漏洞进行公开批露。

检查系统平台是否可以被更新，供应商是否对维护更新机制进行描述，是否说明更新是如何实现。

通过标准：厂商提供的资料与安全要求一致。

供应商维护安全指南，安全指南对系统平台的配置管理作相关描述。

供应商推出安全维护的措施，包括：形成安全维护策略文档；通过周期执行易受攻击脆弱性评估，保证及时检测易受攻击的弱点，例如报告分析、公共域信息反馈和测试；保证及时评估和分类最新发现的易受攻击弱点；保证及时建立缓解最新发现漏洞影响的机制。

系统平台供应商对易受攻击的漏洞进行公开批露，包括：以文档形式保存相关漏洞信息；保证及时公布最新发现易受攻击漏洞的信息，包括标识符、标识信息和漏洞相关的评估；提供及时缓解漏洞危害的方法。

系统平台可以被更新，供应商对维护更新机制进行描述，提供更新是如何实现，包括：

a) 更新机制采用恰当的、被认证的安全协议保证系统平台信息的机密性和完整性，对服务进行授权并防止重复使用。如果设备允许进行软件和配置更新，设备应采用加密授权，一旦授权不成功，则更新失败中止；
b) 系统平台供应商为应用开发者、系统集成者和终端使用者提供更新最新系统平台的安全指南；
c) 安全指南应覆盖固件、应用、密钥和证书的更新；

5.1.5.6 服务器身份鉴别

检测目的：所使用的安全协议应能鉴别后台服务器身份，基本要求包括：

a) 服务器身份验证采用合适的协议，采用合适的算法和密钥长度；
b) 采用 SM3 杂凑算法或 SHA-224、SHA-256、SHA-384、SHA-512 中的一种哈希算法；
c) 能够验证接收到的公钥的有效性；
d) 能够验证接收到的公钥的真实性；
e) 使用 WIFI 方式传输时，应使用 WAP 或 WAP2 或更高安全性的加密方式,同时使用安全协议；
f) 使用蓝牙方式传输时，不应使用安全模式 1 与 2 以及安全模式 4 的“Just Works”安全配对选项或者在用户指导文档中指导用户不使用这些模式。

测试过程：检查厂商提供的资料是否与安全要求一致。

检查服务器身份验证是否采用合适的协议，采用合适的算法和密钥长度；

检查是否采用 SM3 杂凑算法或 SHA-224、SHA-256、SHA-384、SHA-512 中的一种哈希算法；

检查是否能够验证接收到的公钥的有效性；

检查是否能够验证接收到的公钥的真实性；

使用 WIFI 方式传输时，检查是否使用 WAP 或 WAP2 或更高安全性的加密方式,同时使用安全协议；

使用蓝牙方式传输时，检查是否使用安全模式 1 与 2 以及安全模式 4 的“Just Works”安全配对选项或者是否在用户指导文档中指导用户不使用这些模式。

通过标准：厂商提供的资料与安全要求一致。

服务器身份验证采用了合适的协议，采用了合适的算法和密钥长度；

采用 SM3 杂凑算法或 SHA-224、SHA-256、SHA-384、SHA-512 中的一种哈希算法；

能够验证接收到的公钥的有效性；

能够验证接收到的公钥的真实性；

使用 WIFI 方式传输时，使用 WPA 或 WPA2 或更高安全性的加密方式,同时使用安全协议；

使用蓝牙方式传输时，不使用安全模式 1 与 2 以及安全模式 4 的“Just Works”安全配对选项或者在用户指导文档中指导用户不使用这些模式。

5.2 加密要求

检测目的：应采取措施保障从 ATM 终端到所连 ATMP 的数据传输不泄漏银行卡信息。 采用安全可控的密码算法，保证 ATM 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；密码算法应保证 ATM 终端交易数据的安全性。PIN 要求用硬加密，PIN 处理的原则和要求见 GB/T 21078.1。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

从 ATM 终端到所连 ATMP 的数据传输不泄漏银行卡信息，采用安全可控的密码算法，保证 ATM 交易数据的完整性和机密性。

终端支持的国密算法符合 GM/T 0002、GM/T 0003、GM/T 0004、GM/T 0009 的要求。

密码算法应保证 ATM 终端交易数据的安全性。

PIN 为硬加密，PIN 处理的原则和要求见 GB/T 21078.1。

5.3 密钥管理

5.3.1 二级密钥体系

检测目的：密钥体系应不少于二级，ATM 终端密钥分为二级：密钥加密密钥（KEK）和工作密钥（WK）。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

密钥体系不少于二级，具备密钥加密密钥（KEK）和工作密钥（WK）。

5.3.2 密钥加密密钥

检测目的：KEK 用于对工作密钥（WK）进行加密保护，每台 ATM 终端有唯一的 KEK。

KEK 应有安全保护措施（如采用分量输入方式、远程密钥加载方式等）。只能写入并参与运算，不能被读取。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

KEK 用于对工作密钥（WK）进行加密保护，每台 ATM 终端有唯一的 KEK。

KEK 具有安全保护措施（如采用分量输入方式、远程密钥加载方式等），只能写入并参与运算，不能被读取。

5.3.3 工作密钥

检测目的：ATM 终端采用三种工作密钥用于数据的加解密，即对个人识别码（PIN）加解密的 PIN 密钥（PIK），计算报文鉴别码（MAC）的 MAC 密钥（MAK）和对磁道信息加解密的磁道加密密钥（TDK）。

ATM 终端工作密钥在下载时和传输时都应以密文方式出现，不应明文传送。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

ATM 终端采用三种工作密钥用于数据的加解密，即对个人识别码（PIN）加解密的 PIN 密钥（PIK），计算报文鉴别码（MAC）的 MAC 密钥（MAK）和对磁道信息加解密的磁道加密密钥（TDK）。

终端工作密钥在下载时和传输时以密文方式出现，不采用明文传送。

5.4 通讯要求

检测目的：ATM 终端内部各关键模块间通讯时，应采取严格的双向验证机制，防止伪造请求。吐钞模块应当对请求指令的来源和合法性进行严格验证。

ATM 终端的外设接口应严格限制使用，对 USB、串口等通讯接口应采取严格的控制措施，防止通过外设接口植入木马等恶意程序。

ATM 终端与后台服务器信息交互时，应使用强壮的加密算法和安全协议保护敏感数据在网络上的传输安全，并且应采取双向认证等方式，对交易报文进行合法性验证，防范中间人攻击。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

ATM 终端内部各关键模块间通讯时，采取严格的双向验证机制，防止伪造请求。吐钞模块对请求指令的来源和合法性进行严格验证。

ATM 终端的外设接口严格限制使用，对 USB、串口等通讯接口采取严格的控制措施，无法通过外设接口植入木马等恶意程序。

ATM 终端与后台服务器信息交互时，使用强壮的加密算法和安全协议保护敏感数据在网络上的传输安全，并且采取双向认证等方式，对交易报文进行合法性验证，防范中间人攻击。

5.5 操作系统要求

检测目的：ATM 终端操作系统应定期维护更新，及时安装系统补丁，部署防病毒程序，并采取白名单等方式，禁止非法程序执行。定期对操作系统安全性进行测试。操作系统应最小化安装，关闭不安全、不必要的服务。ATM 终端在进入维护模式时应采取多因素验证等方式。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：厂商提供的资料与安全要求一致。

ATM 终端操作系统定期维护更新，及时安装系统补丁，部署防病毒程序，并采取白名单等方式，禁止非法程序执行。

定期对操作系统安全性进行测试。

操作系统为最小化安装，已关闭不安全、不必要的服务。

ATM 终端在进入维护模式时采取多因素验证等方式。

5.6 其他要求

5.6.1 敏感信息存储

检测目的：银行卡敏感数据信息（如完整的磁道信息、PIN、卡片验证码及卡片有效期等）不能在 ATM 终端中保存。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：ATM 终端中未保存银行卡敏感数据信息（如完整的磁道信息、PIN、卡片验证码及卡片有效期等）。

5.6.2 非接读卡器要求

检测目的：对银行卡操作（特别是非接触操作）进行蜂鸣、指示灯、语音、文字、画面等提示。例如，在非接读卡器放卡或移卡操作时进行提示。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：非接触银行卡读取操作具备蜂鸣、指示灯、语音、文字、画面等提示。例如，在非接读卡器放卡或移卡操作时终端具备提示。

5.6.3 吞卡要求

检测目的：对于接触式受理情况，如果交易处理失败且响应码要求吞卡，则 ATM 终端应执行吞卡操作，同时打印客户凭证。交易环节中应有相应的安全提示和安全警示（例如：个人密码输入界面宜增加密码防窥提示，交易结束宜增加客户取卡提示）。如果在交易进行过程中，持卡人在限定时间内没有任何操作，则应将银行卡退回至入卡口，同时提示持卡人取卡。如果在限定时间内持卡人未将银行卡从入卡口取走，则应执行吞卡操作，并给予客户相应提示信息。对于非指令性的吞卡，银行可经过客户信息验证后，即时通过设备端返还吞卡。

对于非接触式受理情况，由于机具无法执行吞卡操作，为避免引起持卡人误解，发卡机构不应对非接触式受理的情况返回吞卡指令。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：对于接触式受理情况，如果交易处理失败且响应码要求吞卡，ATM 终端执行吞卡操作，同时打印客户凭证。

交易环节具有相应的安全提示和安全警示（例如：个人密码输入界面宜增加密码防窥提示，交易结束宜增加客户取卡提示）。

如果在交易进行过程中，持卡人在限定时间内没有任何操作，则将银行卡退回至入卡口，同时提示持卡人取卡。如果在限定时间内持卡人未将银行卡从入卡口取走，则执行吞卡操作，并给予客户相应提示信息。对于非指令性的吞卡，银行具备经过客户信息验证后，即时通过设备端返还吞卡的流程。

对于非接触式受理情况，由于机具无法执行吞卡操作，为避免引起持卡人误解，发卡机构不对非接触式受理的情况返回吞卡指令。

5.6.4 电子日志保护管理

检测目的：电子日志类信息应具备保护机制。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：电子日志类信息具备保护机制，且真实有效。

5.6.5 生物特征识别技术（可选）

检测目的：银行卡信息可采用人体生物特征识别技术增强其安全性。

测试过程：检查厂商提供的资料是否与安全要求一致。

根据厂商提供资料进行有效性验证。

通过标准：银行卡信息采用有效的人体生物特征识别技术，安全性得到了增强。