Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.3.1—2014

银联卡受理终端安全规范
第 3 卷：检测卷
第 1 部分：基础安全检测要求

Security Specifications for Terminal Accepting UnionPay Card
Volume 3: Testing Requirements
Part 1: Testing Requirements for Fundamental Security

2014-11-30 发布　　2014-12-01 实施

中国银联股份有限公司 发布

目　　次

前　言

本标准对受理银联卡（包括磁条卡和IC卡）终端的硬件和安全做具体规定。

本标准由以下部分组成：

——第1卷：基础卷

——第1部分：术语

——第2部分：设备安全

——第3部分：管理安全

——第4部分：硬件要求

——第2卷：产品卷

——第1部分：销售点（POS）终端

——第2部分：无人值守（自助）终端

——第3部分：个人支付终端

——第4部分：独立部件

——第5部分：电话终端

——第6部分：智能销售点终端

——第7部分：mPOS通用技术安全

——第3卷：检测卷

——第1部分：基础安全检测要求

——第2部分：产品分类安全检测要求

——第3部分：硬件技术检测要求

——第4卷：辅助卷

——第1部分：终端防切转网技术安全指南

——第2部分：航空机上支付技术安全指南

——第3部分：POS互联网接入系统部署方案

——第4部分：基于地理位置定位的终端非法移机监控技术方案

本部分为《银联卡受理终端安全规范》第3卷第1部分。

本部分由中国银联提出。

本部分由中国银联技术部组织制定和修订。

本部分的主要起草单位：银行卡检测中心、中国银联。

本部分的主要起草人：刘志刚、杜磊、彭乾、李海冰、王建新、安焘、蒋利兵、吴水炯、汪毅、周思捷。

银联卡受理终端安全规范
第 3 卷：检测卷
第 1 部分：基础安全检测要求

1 范围

本部分对受理终端基础安全的检测进行说明，与《受理终端安全规范-第1卷：基础卷-第2部分： 设备安全》（007.1.2-2014）的安全要求相对应。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡标注日期的引用文件，对于标注日期之后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，但是，鼓励根据本标准达成协议的各方研究是否可使用这些引用文件的最新版本。凡不标注日期的引用文件，其最新版本均适用于本标准。

Q/CUP 007.1 银联卡受理终端安全规范-第1卷：基础卷

ISO 11568 Banking-Key Management (Retail) 银行业务密钥管理（零售）

ANSI X9.24 Retail Financial Services-Symmetric Key Management 零售金融业务对称密钥管理

ANSI TR-31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms 通用对称算法密钥安全交换和密钥包规范

Q/CUP 058 银联卡密码算法使用与管理规范

ISO 9564 Financial Services – Personal Identification Number（PIN） Management and Security 金融服务个人识别码的管理与安全

NIST SP800-21 Guideline for Implementing Cryptography 密码实施指南

NIST SP 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications 密码应用中随机和伪随机数生成器的统计测试

PCI PIN Transaction Security Point of Interaction-Modular Security Requirement 交互点个人识别码交易安全-模块安全要求

3 物理安全

3.1 入侵检测机制

检测目的：设备使用攻击监测和响应机制，一旦触发事件，设备立刻不可操作，并且立即自动清除保存的敏感数据，并且保证这些敏感数据不易恢复。

所具备的机制保证能够抵御物理方式的侵入，包括但不限于：钻孔、激光、化学腐蚀、打开盖子等。没有任何可以关闭或者使这个机制失效的方法，也不能通过植入一个 PIN-disclosing bug 来获取敏感信息，攻击总分至少 26 分，攻击阶段分值至少 13 分，攻击时间至少 10 个小时。

检测范围：IC 卡读卡器不适用本项。

测试条件：N/A。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。

- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.2 独立安全机制

检测目的：单一的安全机制失效不会对设备的安全性造成损害，保护机制至少应具有2个独立安全机制。

检测范围：全部终端。

测试条件：N/A。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 具有至少两个独立的安全机制。

3.3 环境和操作条件改变适应性

检测目的：环境条件或操作条件发生变化时，设备的安全性不能因此降低。

检测范围：全部终端。

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《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.4 敏感功能或信息保护

检测目的：敏感函数或者数据只存在于设备的受保护区域。敏感数据和函数能够受保护防止被修改，攻击总分至少26分 ，其中攻击阶段至少13分。

检测范围：IC卡读卡器不适用本项。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.5 PIN 输入过程监控

检测目的：通过检测声音，电磁辐射、能量消耗或者其他外部特性检测等（即使是在设备操作员或销售员提供的协助下）不能侦测到内部传输的PIN。攻击总分至少26分，攻击阶段分值至少13分。

检测范围：IC卡读卡器不适用本项。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。

- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.6 密钥识别分析

检测目的：通过侵入设备或者检测设备泄露的信息（包括能量消耗）侦测设备内任何PIN安全相关的密钥的攻击总分至少35分，攻击阶段分值至少15分。

检测范围：全部终端。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 进行 SPA/DPA 攻击试验，对能量进行分析。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.7 设备显示的物理安全

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，攻击总分至少18分，攻击阶段分值至少9分。

检测范围：若支持PIN输入的设备同时支持非PIN数据输入，则应至少满足3.7、4.14、或7.3.4中的任意一项。本节要求适用于在加密处理器与显示单元间包含明文显示信号的任意单元或路径。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 设计攻击场景，计算攻击分值。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.8 防偷窥保护

检测目的：设备提供防止持卡人在输入PIN时被窥视的方法，具体要求参考附录A。

检测范围：非手持设备。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答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。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 实际检查和评估 PIN 输入设备。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- PIN 输入设备防偷窥设计符合安全要求。测试方法参见附录 A。

3.9 磁条读卡器保护

检测目的：应防止通过入侵设备、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以获取或修改磁道数据。攻击总分值至少16分，同时攻击阶段分值至少8分。

检测范围：具备磁条阅读器的终端。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 设计攻击场景，计算攻击分值。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.10 无人值守（自助）支付终端设备防移除

检测目的：无人值守（自助）支付终端 设备的安全组件，应保证未经许可不会被拆除或者重新安装。攻击总分至少18分，同时攻击阶段分值至少9分。

检测范围：无人值守设备。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 设计攻击场景，计算攻击分值。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

3.11 PIN 输入音调

检测目的：如果PIN输入过程中有声音提示，应保证每个PIN数字键提示音一致。

检测范围：全部终端。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 无法根据提示音区别数字按键。

3.12 IC 卡读写器结构

检测目的：IC卡读写器应具有安全的卡槽结构，插卡处应可以被持卡人清楚的看到，以便任何可能的可疑物都能被发现。

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。

检测范围：支持脱机安全的终端。

测试条件：厂商提供设计文档。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 设计攻击场景，执行测试确定其可行性。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 在卡插入过程中，IC 卡插槽的入口处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。
- 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。

- 手持设备综合使用场合、外形尺寸，进行合理判断。

4 逻辑安全

4.1 自检测试

检测目的：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。自检包括完整性和真实性，其目标是检查固件、针对篡改迹象的安全机制以及设备是否处于被攻破状态。 一旦出现故障，设备及其功能会以安全的方式失去效用。设备每24小时内要至少重新初始化内存一次。

自检在设备启动时进行并且至少每天进行一次。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查其它的相关文档，以验证支持厂商的回答。
- 执行任何需要的测试验证。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.2 逻辑异常

检测目的：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；

——错误的参数。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 执行任何需要的测试验证。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 终端不受逻辑异常的影响。

4.3 固件和应用软件的认证及更新

检测目的：设备应对固件进行有效保护，包括但不限于：

——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。

——如果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并删除验证失败的固件。

——设备固件必须验证下载到设备的应用程序，如果设备支持更新应用软件和/或配置，设备必须通过加密机制验证更新应用软件和/或配置的完整性和真实性，如果未确认其完整性和真实性，那么设备应拒绝进行软件更新并删除验证失败的软件。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 固件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。
- 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，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和/或配置更新，设备应加密验证应用和/或配置的完整性，如果验证未通过，应用和/或配置更新应被拒绝并删除。

4.4 输入 PIN 区别

检测目的：设备在任何情况下都不显示或者泄漏PIN的明文。任何和PIN相关的数据必须显示为无意义的字符（例如星号）或者输出无区别的信号等。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 执行模拟交易。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.5 内存清除

检测目的：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的敏感信息：

——交易已经完成；

——设备等待持卡人或商户的响应超时。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.6 敏感服务

检测目的：设备敏感服务用于访问敏感功能，敏感功能涉及设备中密钥、PIN 和口令等敏感数据的处理。应对敏感服务进行有效保护并进行使用限制：

——设备的敏感服务应充分保护，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。

——必须对设备敏感服务的范围和使用时间进行限制，保证设备敏感服务不被非法使用，若超出服务范围和使用时间则设备应退出敏感服务并返回到正常模式。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查使用敏感服务是否泄露或改变设备中的敏感信息。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 使用敏感服务不泄露或改变设备中的敏感信息。
- 对敏感服务的操作次数和时间进行强制限制。

4.7 随机数

检测目的：如果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必须经过评估，以保证其产生的随机数无法被预测。

检测范围：全部终端。

测试条件：厂商提供随机数文件。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 使用随机数测试工具对随机数随机性进行测试。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 随机数具有足够的随机性。

4.8 PIN 防穷举

检测目的：设备应具有防止利用穷举探测PIN值的能力。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备应能防止利用盗取的设备穷举探测获得 PIN 值。

4.9 密钥管理技术

检测目的：设备涉及的密钥管理技术应满足以下规范要求：

——应满足《银联卡密码算法使用与管理规范》（Q/CUP 058-2013）要求；

——应符合ISO 11568和/或ANSI X9.24要求；

——应支持ANSI TR-31或等效的密钥管理规则；如密码键盘同时提供了支持ANSI TR-31（或者等同）的密钥衍生方法和非等同于ANSI TR-31的密钥衍生方法，则这两种方法衍生（例如下载）的密钥不能混用（例如先用ANSI TR-31的方式下载主密钥，然后又用非TR-31的方式下载该主密钥下属的工作密钥）。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查密钥管理技术是否满足《银联卡密码算法使用与管理规范》（Q/CUP 058-2013）、ISO 11568 和/或 ANSI X9.24、ANSI TR-31 或等效的密钥管理规则的要求。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备执行密钥管理技术需要同时遵守 ISO11568 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。

4.10 PIN 加密算法

检测目的：设备采用的PIN加密技术必须遵循ISO 9564。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 执行模拟交易，验证 PIN 加密算法符合要求。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备中执行的 PIN 加密技术是 IS09564 中规定的技术。

4.11 数据加解密

检测目的：不能利用设备内的工作密钥（WK）或密钥加密密钥（KEK）去加密或解密不应由其加解密的其他任意数据。数据密钥（包括MAC密钥（MAK）和磁道加密密钥（TDK））、PIN加密密钥（PIK）、密钥加密密钥（KEK）应具有不同的值。如果密钥通过联机方式获取，由平台决定不同密钥的取值。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.12 明文密钥安全

检测目的：设备应具备密钥和PIN的保护机制，实现以下功能：

——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。

检测范围：全部终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。

- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.13 交易控制

检测目的：输入其他交易数据的过程必须和输入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，那么输入交易金额和PIN时设备应有明显提示进行区别。

检测范围：具备交易应用的终端。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.14 设备显示的逻辑安全

检测目的：非PIN输入的提示信息需要在加密单元的控制下。攻击总分至少18分，同时攻击阶段分值至少9分。如果提示符存放在加密单元中，它们在不擦除密钥的情况下不能轻易地被修改。如果提示符是存储在密码单元之外的，必须有密码机制保证认证和提示符的正当使用，防止修改提示符或者对提示符的非法使用。

检测范围：若支持PIN输入的设备同时支持非PIN数据输入，则应至少满足3.7、4.14、或7.3.4中的任意一项。本节要求适用于设备允许更新显示或基于加密机制与显示单元通讯（不论该操作由厂商或收单行控制）。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查提示的控制是否安全。
- 设计攻击场景。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.15 应用隔离

检测目的：如果设备支持多应用，应用间必须强制隔离。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。

检测范围：具备交易应用的终端。

测试条件：N/A

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.16 操作系统最小配置

检测目的：设备的操作系统需要仅包含必须的组件和服务。操作系统必须被安全的配置并运行于最小的特权。

检测范围：全部终端。

测试条件：厂商提供设计文档。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 确定设备的操作系统。
- 检查操作系统配置。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 操作系统必须进行安全配置，须开通最小的权限设置。

4.17 组建集成文档

检测目的：终端生产厂商必须提供足够的文档，以指导如何将其他安全组件以安全的方式集成到终端。

检测范围：全部终端。

测试条件：厂商提供设计文档。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

4.18 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。

检测范围：全部终端。

测试条件：厂商提供设计文档。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 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：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备安全管理策略符合要求。
• 设备安全管理措施有效。

4.19 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。

检测范围：全部终端。

测试条件：厂商提供设计文档。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 设计测试案例，验证远程密钥更新的安全性。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 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 联机 PIN 安全

5.1 密钥替换

检测目的：如设备能够保存多个工作密钥而且能够在外部选择，则设备应具备防止密钥被非法替换和使用的安全机制。

检测范围：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的终端。

测试条件：厂商提供设计文档。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备禁止未经授权的密钥替换和密钥滥用。

6 脱机 PIN 安全

6.1 防渗透保护

检测目的：任何渗透IC卡读卡器，从而附加、替换或修改IC卡读卡器的硬件或者软件，以获取或修改任何敏感数据的攻击总分至少20分，其中攻击阶段至少10分，攻击时间至少10个小时，不能容许IC卡和其他物品可以同时驻留读卡器的卡槽中。

检测范围：支持脱机安全的终端。

测试条件：厂商提供设计文档。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 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：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 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，不能容许 IC 卡和其他物品可以同时塞进读卡器的卡槽中。

6.2 IC 卡读写器结构

检测目的：IC卡读写器应具有安全的卡槽结构，插卡处应可以被持卡人清楚的看到，以便任何可能的可疑物都能被发现。

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。

检测范围：支持脱机安全的终端。

测试条件：厂商提供设计文档。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 设计攻击场景，执行测试确定其可行性。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 在卡插入过程中，IC 卡插槽的入口处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。
• 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。
• 手持设备综合使用场合、外形尺寸，进行合理判断。

6.3 PIN 传输保护

检测目的：在设备中传输PIN时，如果PIN加密设备和IC卡读卡器不是一体的安全模块，应满足以下安全要求：

——密文PIN验证时，PIN加密设备和IC卡读卡器间传输的PIN必须是由IC卡的密钥加密的或者按照ISO 9564要求加密；

——明文PIN验证时，PINBLOCK必须是按照ISO 9564格式加密后从PIN加密设备传送到IC卡读卡器（IC卡读卡器再解密后送到IC卡）；

如果PIN加密设备和IC卡读卡器是一体的安全模块，应满足以下安全要求：

——密文密码验证时，PINBLOCK必须是用IC卡认证后的密钥加密；

——明文密码验证时，如果传输线路在保护区域，可以是明文的；如果传输线路不在保护区域，则PINBLOCK需要根据ISO9564格式加密。

检测范围：支持脱机安全的终端。

测试条件：厂商提供设计文档。

测试过程：• 检查《厂商评估调查问卷》中的回答, 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：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 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。

7 集成安全

7.1 配置管理

检测目的：集成到终端内的任何安全组件必须明确定义其物理和逻辑安全边界，主要适用于PIN输入功能组件和读卡器功能组件。

检测范围：集成到终端内的安全组件

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

7.2 PIN 输入功能集成

检测目的：一个通过认证的安全组件集成到终端，应不影响整个设备保护级别。密码键盘（PIN输入区域）及其周边区域应具有防overlay攻击的设计，攻击总分至少18分，同时攻击阶段分值至少9分。

检测范围：集成到终端内的安全组件

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

7.3 终端集成

7.3.1 安全等级保持

检测目的：终端通过逻辑及物理方式集成了通过认证的安全组件，将不会引入新的攻击PIN或其他敏感数据的方式。

检测范围：集成到终端内的安全组件

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 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。

7.3.2 防卡片盗取

检测目的：终端应防止银行卡被恶意保存或盗取（如Lebanese Loop attack）。
检测范围：全部终端
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 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：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 终端能够防止银行卡被恶意保存或盗取（如Lebanese Loop attack）。

7.3.3 组件隔离

检测目的：一个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。
检测范围：集成到终端内的安全组件
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 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：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 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。

7.3.4 设备显示安全

检测目的：若支持PIN输入的设备同时支持非PIN数据输入，则应至少满足3.7、4.14、或7.3.4中的任意一项。本节要求适用于不满足4.7和5.14项要求的无人值守（自助）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保持一致性，如通过加密认证方式。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。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，其中攻击阶段9分。
检测范围：支持非PIN数据输入的终端和不满足3.7和4.14项要求的无人值守（自助）终端。
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 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：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 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。

7.3.5 密码输入接口控制

检测目的：应保证只具有一个支付密码输入接口，例如一个键盘等。如果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，例如：键盘无数字键，或按键无法用于数字输入，或采用与4.14相一致的控制方式。

检测范围：全部终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

7.3.6 设备移除要求

检测目的：终端应具有防止未授权移除组件的机制，其攻击总分至少18分，其中攻击阶段至少9分。终端厂商应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，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。

检测范围：全部终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 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：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。
- 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。

8 开放协议

8.1 协议和接口声明和定义

检测目的：设备使用的所有有效的公共域协议和接口必须明确声明和定义。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备使用的所有有效的公共域协议和接口是否明确声明和定义。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。

• 设备使用的所有有效的公共域协议和接口已经明确声明和定义。

8.2 漏洞评估

检测目的：设备已具备针对每个协议和接口的漏洞评估过程与漏洞评估文档。

设备已经过一个漏洞评估并且确保协议和接口不存在可利用的漏洞。评估通过以下几种方式进行：

——以文档形式描述对协议和接口的安全性的分析；

——根据公共域信息调查；

——通过一些测试。

设备厂商有适当的漏洞发布措施，包括：

——以文档形式描述；

——确保周期性地发布新发现的漏洞，漏洞信息包括标识符、描述和漏洞评估；

——确保周期性地发布漏洞补救措施。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备是否具备针对每个协议和接口的漏洞评估过程与漏洞评估文档。
- 检查设备是否经过一个漏洞评估并且确保协议和接口不存在可利用的漏洞。
- 检查设备厂商是否有适当的漏洞发布措施。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备已具备针对每个协议和接口的漏洞评估过程与漏洞评估文档。
- 设备已经过一个漏洞评估并且确保协议和接口不存在可利用的漏洞。评估通过以下几种方式进行：

——以文档形式描述对协议和接口的安全性的分析；

——根据公共域信息调查；

——通过一些测试。

- 设备厂商有适当的漏洞发布措施，包括：

——以文档形式描述；

——确保周期性地发布新发现的漏洞，漏洞信息包括标识符、描述和漏洞评估；

——确保周期性地发布漏洞补救措施。

8.3 厂商指南

检测目的：应具有对所有有效接口的协议和服务如何使用进行描述的安全指南。

应具有对每一个接口上的每一种协议和服务的默认配置进行描述的指南。

应具有对关于私钥和证书如何使用的密钥管理机制进行描述的指南，包括：

——为应用开发者、系统集成者和平台终端使用者提供安全处理操作引导；

——描述所有平台上使用的私钥和证书的属性；

——描述平台相关的厂商、应用开发者、系统集成商和终端用户的职责；

——确保安全地使用私钥和证书。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查是否具有对所有有效接口的协议和服务如何使用进行描述的安全指南。

• 检查是否具有对每一个接口上的每一种协议和服务的默认配置进行描述的指南。
• 检查是否具有对关于私钥和证书如何使用的密钥管理机制进行描述的指南。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 具有对所有有效接口的协议和服务如何使用进行描述的安全指南。
• 具有对每一个接口上的每一种协议和服务的默认配置进行描述的指南。
• 具有对关于私钥和证书如何使用的密钥管理机制进行描述的指南，包括：
——为应用开发者、系统集成者和平台终端使用者提供安全处理操作引导；
——描述所有平台上使用的私钥和证书的属性；
——描述平台相关的厂商、应用开发者、系统集成商和终端用户的职责；
——确保安全地使用私钥和证书。

8.4 运行测试

8.4.1 安全协议声明

检测目的：设备清晰地声明了所有使用的安全协议。
检测范围：使用公共协议的终端
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查设备是否清晰地声明了所有使用的安全协议。
通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备清晰地声明了所有使用的安全协议。

8.4.2 数据机密性保护

检测目的：所使用的安全协议应能确保在网络上发送数据的机密性，基本要求包括：
——采用合适的算法和密钥长度；
——在安全模式下使用合理的密钥管理程序加密，如NIST SP800-21。
检测范围：使用公共协议的终端
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查设备所使用的安全协议是否能确保在网络上发送数据的机密性。
通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备所使用的安全协议能确保在网络上发送数据的机密性，满足下列基本要求：
——采用合适的算法和密钥长度；
——在安全模式下使用合理的密钥管理程序加密，如NIST SP800-21。

8.4.3 数据完整性保护

检测目的：所使用的安全协议应能确保在网络上发送数据的完整性，基本要求包括：
——采用MAC或数字签名；
——采用SHA-224、SHA-256、SHA-384、SHA-512中的一种hash算法；
——采用合适的算法和密钥长度。
检测范围：使用公共协议的终端
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。

• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查设备所使用的安全协议是否能确保在网络上发送数据的完整性。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备所使用的安全协议应能确保在网络上发送数据的完整性，满足下列基本要求：
——采用MAC或数字签名；
——采用SHA-224、SHA-256、SHA-384、SHA-512中的一种hash算法；
——采用合适的算法和密钥长度。

8.4.4 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：
——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；
——采用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，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；
——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。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查设备所使用的安全协议应能鉴别后台服务器身份。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备所使用的安全协议应能鉴别后台服务器身份，满足下列基本要求：
——服务器身份验证采用合适的协议，如TLS 1.2及以上版本，采用合适的算法和密钥长度；
——采用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，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；
——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。

8.4.5 异常监测

检测目的：设备能够监测信息重放，并对异常进行处理。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查设备是否能够监测信息重放，并对异常进行处理。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备能够监测信息重放，并对异常进行处理。

8.4.6 随机数

检测目的：设备使用经NIST SP 800-22验证或与其等效的随机数发生器进行随机数的生成。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备是否使用经NIST SP 800-22验证或与其等效的随机数发生器进行随机数的生成。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备使用经NIST SP 800-22验证或与其等效的随机数发生器进行随机数的生成。

8.4.7 会话管理

检测目的：设备实现了会话管理，包括以下要求：

——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；

——对会话设置时间进行限制，保证会话开放时间限制在一定范围内。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备是否实现了会话管理。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备实现了会话管理，满足以下要求：

——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；

——对会话设置时间进行限制，保证会话开放时间限制在一定范围内。

8.5 管理和维护

8.5.1 配置管理安全指南

检测目的：应提供并维护终端系统平台配置管理指南，包括但不限于以下要求：

——针对内部使用者、应用开发者、系统集成者和终端系统平台使用者提供维护处理的操作引导；

——应覆盖整个终端系统平台，包含固件、应用程序、证书及密钥；

——应覆盖终端系统平台的整个生命周期，包括开发、生产、派送及操作；

——应确保未经认证的修改不可实施；

——应保证对经过检测认证的终端系统平台进行设计安全性的改动，应会导致平台标识的改变。

检测范围：使用公共协议的终端

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备是否提供并维护终端系统平台配置管理指南。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备提供并维护终端系统平台配置管理指南，包括但不限于以下要求：

——针对内部使用者、应用开发者、系统集成者和终端系统平台使用者提供维护处理的操作引导；

——应覆盖整个终端系统平台，包含固件、应用程序、证书及密钥；
——应覆盖终端系统平台的整个生命周期，包括开发、生产、派送及操作；
——应确保未经认证的修改不可实施；
——应保证对经过检测认证的终端系统平台进行设计安全性的改动，应会导致平台标识的改变。

8.5.2 安全维护指南

检测目的：应具备安全维护指南，包括但不限于以下要求：
——维护方法应以文档形式明确给出；
——维护方法应通过周期性的漏洞评估来确保对设备漏洞的及时监测，评估和监测方法包括：分析、调查公开发布的信息以及执行测试等；
——维护方法应能确保对新发现的漏洞进行及时的评估和分类处理；
——维护方法应能确保对可能影响终端系统平台安全的新发现漏洞及时生成缓解措施。
检测范围：使用公共协议的终端
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查设备是否具备安全维护指南。
通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 设备具备安全维护指南，包括但不限于以下要求：
——维护方法应以文档形式明确给出；
——维护方法应通过周期性的漏洞评估来确保对设备漏洞的及时监测，评估和监测方法包括：分析、调查公开发布的信息以及执行测试等；
——维护方法应能确保对新发现的漏洞进行及时的评估和分类处理；
——维护方法应能确保对可能影响终端系统平台安全的新发现漏洞及时生成缓解措施。

8.5.3 更新机制

检测目的：终端系统平台如可以被更新，应提供说明更新机制的指导文档。
所采用的更新机制应确保安全，包括但不限于以下要求：
——通过使用适当、已声明的安全协议来确保保密性、完整性、服务真实性和保护防止重放；
——如设备可进行更新，设备必须通过加密机制验证更新内容的完整性和真实性；
——如未确认更新内容的完整性和真实性，则设备应拒绝进行更新，并删除更新的内容。
检测范围：使用公共协议的终端
测试条件：厂商提供设计文档、源代码。
测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查终端系统平台是否可以被更新，如果支持，是否提供说明更新机制的指导文档。
• 检查终端所采用的更新机制是否确保安全。
通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 终端系统平台如可以被更新，应提供说明更新机制的指导文档。
• 设备所采用的更新机制应确保安全，包括但不限于以下要求：
——通过使用适当、已声明的安全协议来确保保密性、完整性、服务真实性和保护防止重放；
——如设备可进行更新，设备必须通过加密机制验证更新内容的完整性和真实性；
——如未确认更新内容的完整性和真实性，则设备应拒绝进行更新，并删除更新的内容。

9 账户数据保护

9.1 账户数据处理

9.1.1 账户数据处理的安全要求

检测目的：所有的账户相关数据均应在输入时立即加密或者明文输入到设备安全模块中处理。

设备对账户数据的安全要求包括但不限于：

——应保护所有账户数据(包括磁条卡和IC卡)，在未破解安全检测电路情况下，没有其它方式可以获取明文账户数据，破解安全检测电路需攻击总分至少16点，同时攻击阶段分值至少8点；

——磁条卡数据安全保护及读卡器要求应与3.9节一致；

——IC卡数据安全保护及读卡器要求应与6.1一致。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查所有的账户相关数据是否均在输入时立即加密或者明文输入到设备安全模块中处理。
- 根据厂商提供资料，设计攻击场景获取明文账户数据，计算攻击分值。
- 检查终端磁条卡数据安全保护及读卡器要求是否与3.9节一致。
- 检查终端IC卡数据安全保护及读卡器要求是否与6.1一致。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备所有的账户相关数据均应在输入时立即加密或者明文输入到设备安全模块中处理。
- 设备满足保护所有账户数据(包括磁条卡和IC卡)，在未破解安全检测电路情况下，没有其它方式可以获取明文账户数据，破解安全检测电路需攻击总分至少16点，同时攻击阶段分值至少8点。
- 磁条卡数据安全保护及读卡器要求应与3.9节一致。
- IC卡数据安全保护及读卡器要求应与6.1一致。

9.1.2 独立安全机制

检测目的：单一的安全机制失效不会对设备的安全性造成损害，保护机制至少应具有2个独立安全机制。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备保护机制是否至少具有2个独立安全机制。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 单一的安全机制失效不会对设备的安全性造成损害，保护机制至少应具有2个独立安全机制。

9.2 集成条件下的账户数据保护

检测目的：通过物理或逻辑方式将经过安全认证的读卡器集成到PIN输入设备中，不会对账户数据带来新的安全漏洞或攻击路径。账户数据从输入组件到安全模块都要受到保护。

安全保护机制应符合3.2节要求。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。

- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查经过安全认证的读卡器集成到PIN输入设备时，是否会对账户数据带来新的安全漏洞或攻击路径。账户数据从输入组件到安全模块是否受到保护。
- 安全保护机制是否符合3.2节要求。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 经过安全认证的读卡器集成到PIN输入设备中，不会对账户数据带来新的安全漏洞或攻击路径。账户数据从输入组件到安全模块都要受到保护。
- 安全保护机制应符合3.2节要求。

9.3 密钥保护

检测目的：通过对设备进行渗透攻击或监控辐射（包括能量波动）的方法来识别任何用于账户数据加密的密钥，至少需要26分的识别分值和最小13分的攻击阶段分值。

公钥必须以安全方式存储或保护，防止未经授权的修改或替换。未经授权的修改或替换攻击总分至少26分，攻击阶段分值至少13分。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 根据厂商提供资料，通过对设备进行渗透攻击或监控辐射（包括能量波动）的方法设计攻击场景来识别任何用于账户数据加密的密钥，计算攻击分值。
- 根据厂商提供资料，设计攻击场景修改或替换公钥，计算攻击分值。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 通过对设备进行渗透攻击或监控辐射（包括能量波动）的方法来识别任何用于账户数据加密的密钥，至少需要26分的识别分值和最小13分的攻击阶段分值。
- 公钥必须以安全方式存储或保护，防止未经授权的修改或替换。未经授权的修改或替换攻击总分至少26分，攻击阶段分值至少13分。

9.4 加密机制

检测目的：所有账户数据加密时只能使用ANSI X9或ISO许可、符合银联Q/CUP 058规范和相关要求的加密算法和操作模式。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备所有账户数据加密时是否只使用ANSI X9或ISO许可、符合银联Q/CUP 058规范和相关要求的加密算法和操作模式。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备所有账户数据加密时是否只使用ANSI X9或ISO许可、符合银联Q/CUP 058规范和相关要求的加密算法和操作模式。

9.5 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。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备如果使用了远程密钥发布技术，是否支持发送方与接受方之间的双向认证。
- 检查设备，破坏密钥发布过程，是否导致密钥被泄露。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备如果使用远程密钥发布技术，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。

9.6 数据源认证

检测目的：设备支持对已加密信息来源的验证。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备是否支持对已加密信息来源的验证。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备支持对已加密信息来源的验证。

9.7 密钥唯一性

检测目的：设备中若保存可对交易数据进行加密的私有密钥，则须保证每台设备中私有密钥的唯一性。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 设备中若保存可对交易数据进行加密的私有密钥，检查每台设备中私有密钥是否满足唯一性。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备中若保存可对交易数据进行加密的私有密钥，则须保证每台设备中私有密钥的唯一性。

9.8 加解密数据对象控制

检测目的：不允许使用账户数据加解密密钥去对随意的数据进行加密和解密。确保账户数据密钥、密钥加密密钥和PIN加密密钥内容均不一致。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 设备是否允许使用账户数据加解密密钥去对随意的数据进行加密和解密。
- 检查设备账户数据密钥、密钥加密密钥和PIN加密密钥内容是否均不一致。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 不允许使用账户数据加解密密钥去对随意的数据进行加密和解密。
- 账户数据密钥、密钥加密密钥和PIN加密密钥内容均不一致。

9.9 远程访问

检测目的：若设备可被远程控制，则所有远程控制的操作需经验证。若无法通过验证，则拒绝远程控制。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 若设备可被远程控制，检查设备是否验证所有远程控制的操作。若无法通过验证，设备是否拒绝远程控制。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 若设备可被远程控制，则所有远程控制的操作需经验证。若无法通过验证，则拒绝远程控制。

9.10 固件审查

检测目的：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和非法的功能。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备固件及对固件的任何改动是否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。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 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。

9.11 应用真实性

检测目的：固件必须验证下载到设备中所有应用软件的合法性。如果设备允许更新应用软件或配置，则需要通过加密机制来验证应用软件的合法性和完整性。如果未确认其完整性和真实性，那么设备应拒绝进行软件更新并删除验证失败的软件。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备固件是否验证下载到设备中所有应用软件的合法性。
- 如果设备允许更新应用软件或配置，检查其是否通过加密机制来验证应用软件的合法性和完整性。如果未确认其完整性和真实性，检查设备是否拒绝进行软件更新并删除验证失败的软件。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 固件必须验证下载到设备中所有应用软件的合法性。
- 如果设备允许更新应用软件或配置，则需要通过加密机制来验证应用软件的合法性和完整性。如果未确认其完整性和真实性，那么设备应拒绝进行软件更新并删除验证失败的软件。

9.12 应用指引

检测目的：设备生产厂商应向应用程序开发人员提供明确的安全指引，实现以下安全要求：

——当终端处于加密模式时，应用程序不会被逻辑异常影响而导致明文数据的输出；
——如非绝对必要，账户数据不应被保留或者经常使用。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备生产厂商是否向应用程序开发人员提供明确的安全指引。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备生产厂商应向应用程序开发人员提供明确的安全指引，实现以下安全要求：

——当终端处于加密模式时，应用程序不会被逻辑异常影响而导致明文数据的输出；
——如非绝对必要，账户数据不应被保留或者经常使用。

9.13 固件更新

检测目的：如设备固件能够进行更新，则设备应通过加密机制验证更新固件的完整性和真实性。如未确认其完整性和真实性，则设备应拒绝进行固件更新并删除验证失败的固件。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 如设备固件能够进行更新，检查设备是否通过加密机制验证更新固件的完整性和真实性。如未确认其完整性和真实性，设备是否拒绝进行固件更新并删除验证失败的固件。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 如设备固件能够进行更新，则设备应通过加密机制验证更新固件的完整性和真实性。如未确认其完整性和真实性，则设备应拒绝进行固件更新并删除验证失败的固件。

9.14 逻辑异常

检测目的：设备不应在受异常数据的影响而泄露PIN明文、密钥明文、持卡人账户数据等敏感信息，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；
——错误的参数。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备是否受异常数据的影响而泄露PIN明文、密钥明文、持卡人账户数据等敏感信息。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备不应受异常数据的影响而泄露PIN明文、密钥明文、持卡人账户数据等敏感信息，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；

——错误的参数。

9.15 开放协议和服务

检测目的：若设备允许通过IP或公共协议（包括但不限于Wi-Fi、蓝牙等）进行通信，则需要满足第8章开放协议的相关要求。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 若设备允许通过IP或公共协议（包括但不限于Wi-Fi、蓝牙等）进行通信，检查其是否满足第8章开放协议的相关要求。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 若设备允许通过IP或公共协议（包括但不限于Wi-Fi、蓝牙等）进行通信，则需要满足第8章开放协议的相关要求。

9.16 明文数据保护

检测目的：在加密模式下，不应有允许明文数据输出的机制。加密模式与非加密模式之间的切换需要明确的认证。

在加密模式下操作时，安全模块只能将明文账户数据发送到设备中正在运行的、已经过认证的应用程序。

如非绝对必要，账户数据（不论明文或密文）不应被保留或者过频繁使用。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 在加密模式下，检查设备是否有允许明文数据输出的机制。加密模式与非加密模式之间的切换是否需要明确的认证。
- 在加密模式下操作时，检查安全模块是否只能将明文账户数据发送到设备中正在运行的、已经过认证的应用程序。
- 检查非必要情况下，账户数据（不论明文或密文）是否被保留或者过频繁使用。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 在加密模式下，不应有允许明文数据输出的机制。加密模式与非加密模式之间的切换需要明确的认证。
- 在加密模式下操作时，安全模块只能将明文账户数据发送到设备中正在运行的、已经过认证的应用程序。
- 如非绝对必要，账户数据（不论明文或密文）不应被保留或者过频繁使用。

9.17 主账号值替代

检测目的：若设备可生成PAN的替代值并输出到设备外，须保证无法从该输出结果推导出原始PAN，同时满足以下要求：

——若使用哈希算法生成PAN替代值，则需对输入数据进行“加盐”（salt）处理，“salt”应至少64位长；

——若使用哈希算法生成PAN替代值，则“salt”应当保密并被合理保护，对“salt”的攻击总分至少16点，同时攻击阶段分值至少8点。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 若设备可生成PAN的替代值并输出到设备外，检查其是否无法从该输出结果推导出原始PAN。
- 若使用哈希算法生成PAN替代值，检查设备是否对输入数据进行“加盐”（salt）处理，“salt”是否满足至少64位长。
- 若使用哈希算法生成PAN替代值，设计攻击场景获取salt。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 若设备可生成PAN的替代值并输出到设备外，须保证无法从该输出结果推导出原始PAN。
- 若使用哈希算法生成PAN替代值，则需对输入数据进行“加盐”（salt）处理，“salt”应至少64位长。
- 若使用哈希算法生成PAN替代值，则“salt”应当保密并被合理保护，对“salt”的攻击总分至少16分，同时攻击阶段分值至少8分。

9.18 密钥管理

检测目的：设备中密钥管理技术应符合5.9节要求。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备中密钥管理技术是否符合5.9节要求。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备中密钥管理技术应符合5.9节要求。

9.19 主账号防穷举

检测目的：设备应具备主账号（PAN）防穷举机制。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查设备是否具备主账号（PAN）防穷举机制。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备应具备主账号（PAN）防穷举机制。

9.20 环境和操作条件改变适应性

检测目的：环境条件或操作条件发生变化时（包括但不限于：操作电压或环境温度超出规定的范围），设备的安全性不能因此降低，不能导致设备输出明文账户数据。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 环境条件或操作条件发生变化时（包括但不限于：操作电压或环境温度超出规定的范围），检查设备的安全性是否因此降低，导致设备输出明文账户数据。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 环境条件或操作条件发生变化时（包括但不限于：操作电压或环境温度超出规定的范围），设备的安全性不能因此降低，不能导致设备输出明文账户数据。

9.21 应用隔离

检测目的：如果设备支持多应用，应用间必须强制隔离。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。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 如果设备支持多应用，检查应用间是否满足强制隔离。检查一个应用是否能够干扰或损害另一个应用或者操作系统。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 如果设备支持多应用，应用间必须强制隔离。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。

9.22 操作系统安全配置

检测目的：操作系统配置应遵循以下安全原则：
——操作系统应只包含预定操作所必需的软件（组件和服务）；
——应安全地配置操作系统，并遵循最小特权运行原则；
——设备的安全策略不允许未经授权的或不必要的功能；
——未被要求支持特定功能的API功能和指令必须禁用（在可能的情况下应删除）。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

测试过程：• 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
• 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
• 检查设备操作系统是否只包含预定操作所必需的软件（组件和服务）。
• 检查设备是否安全地配置操作系统，并遵循最小特权运行原则。
• 检查设备的安全策略是否允许未经授权的或不必要的功能。
• 检查未被要求支持特定功能的API功能和指令是否被禁用（在可能的情况下应删除）。

通过标准：• 《厂商评估调查问卷》中的回答与安全要求一致。
• 厂商提供的资料支持《厂商评估调查问卷》中的回答。
• 操作系统配置应遵循以下安全原则：
——操作系统应只包含预定操作所必需的软件（组件和服务）；
——应安全地配置操作系统，并遵循最小特权运行原则；
——设备的安全策略不允许未经授权的或不必要的功能；
——未被要求支持特定功能的API功能和指令必须禁用（在可能的情况下应删除）。

9.23 敏感服务保护

检测目的：设备敏感服务用于访问敏感功能，敏感功能涉及设备中密钥、PIN 和口令等敏感数据的处理。应对敏感服务进行有效保护并进行使用限制：
——设备的敏感服务应充分保护，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。

——必须对设备敏感服务的范围和使用时间进行限制，保证设备敏感服务不被非法使用，若超出服务范围和使用时间则设备应退出敏感服务并返回到正常模式。

检测范围：读卡器组件。

测试条件：厂商提供设计文档、源代码。

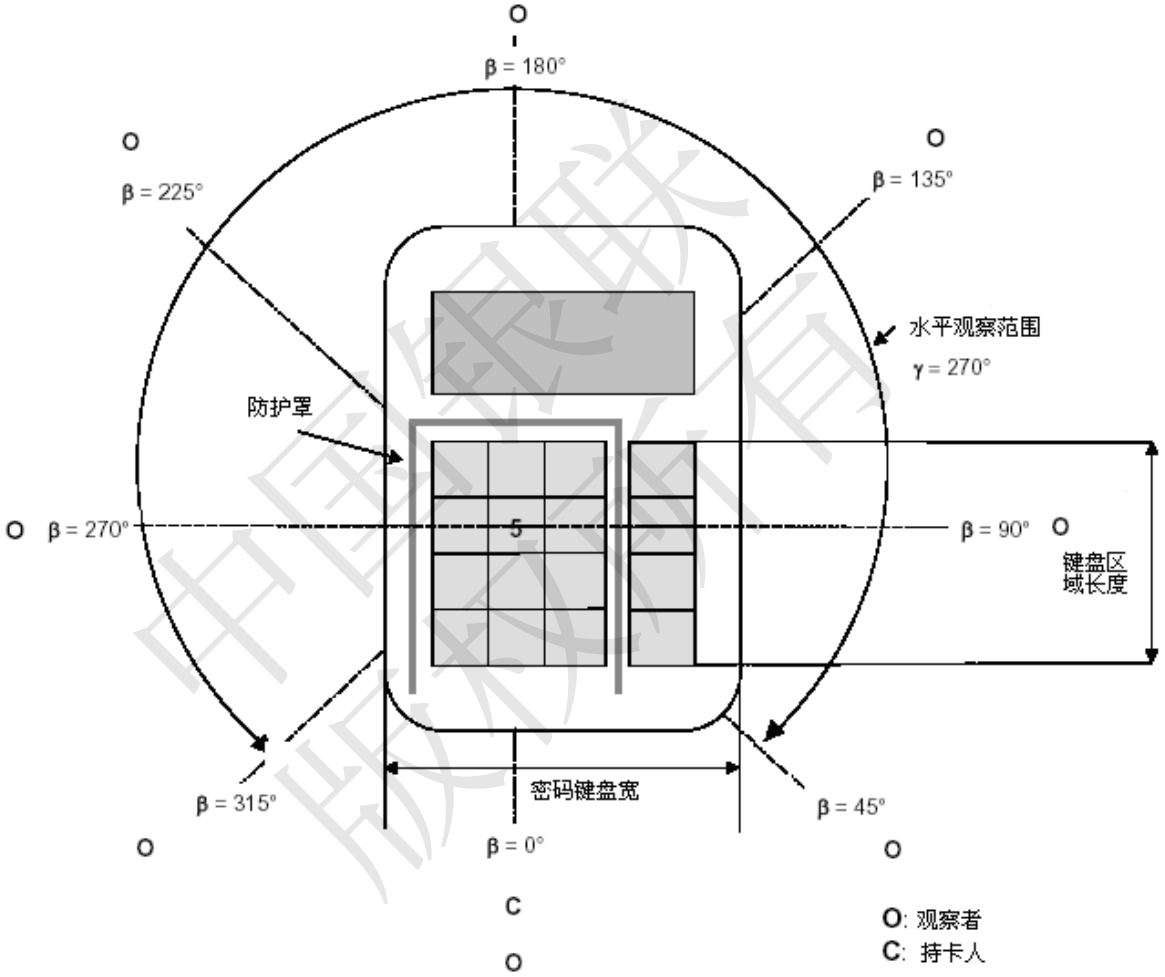
测试过程：
- 检查《厂商评估调查问卷》中的回答是否与安全要求一致。
- 检查厂商提供的资料与《厂商评估调查问卷》中的回答是否一致。
- 检查使用设备的敏感服务是否必须通过身份验证，进入或退出敏感服务是否能够泄露或改变设备中的敏感信息。
- 检查设备敏感服务的范围和使用时间是否进行限制。若超出服务范围和使用时间，设备是否退出敏感服务并返回到正常模式。

通过标准：
- 《厂商评估调查问卷》中的回答与安全要求一致。
- 厂商提供的资料支持《厂商评估调查问卷》中的回答。
- 设备的敏感服务应充分保护，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。
- 必须对设备敏感服务的范围和使用时间进行限制，保证设备敏感服务不被非法使用，若超出服务范围和使用时间则设备应退出敏感服务并返回到正常模式。

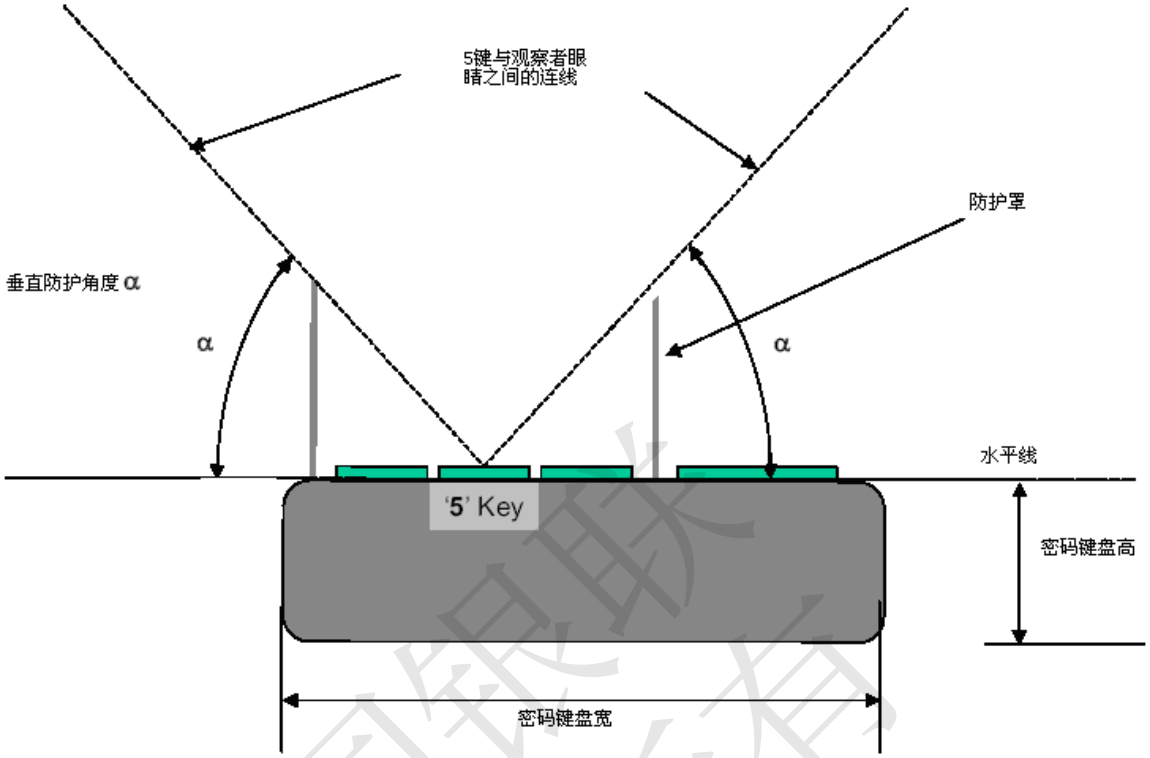
附 录 A
（规范性附录）挡板设计标准

A.1 满足PIN输入设备设计的挡板设计标准

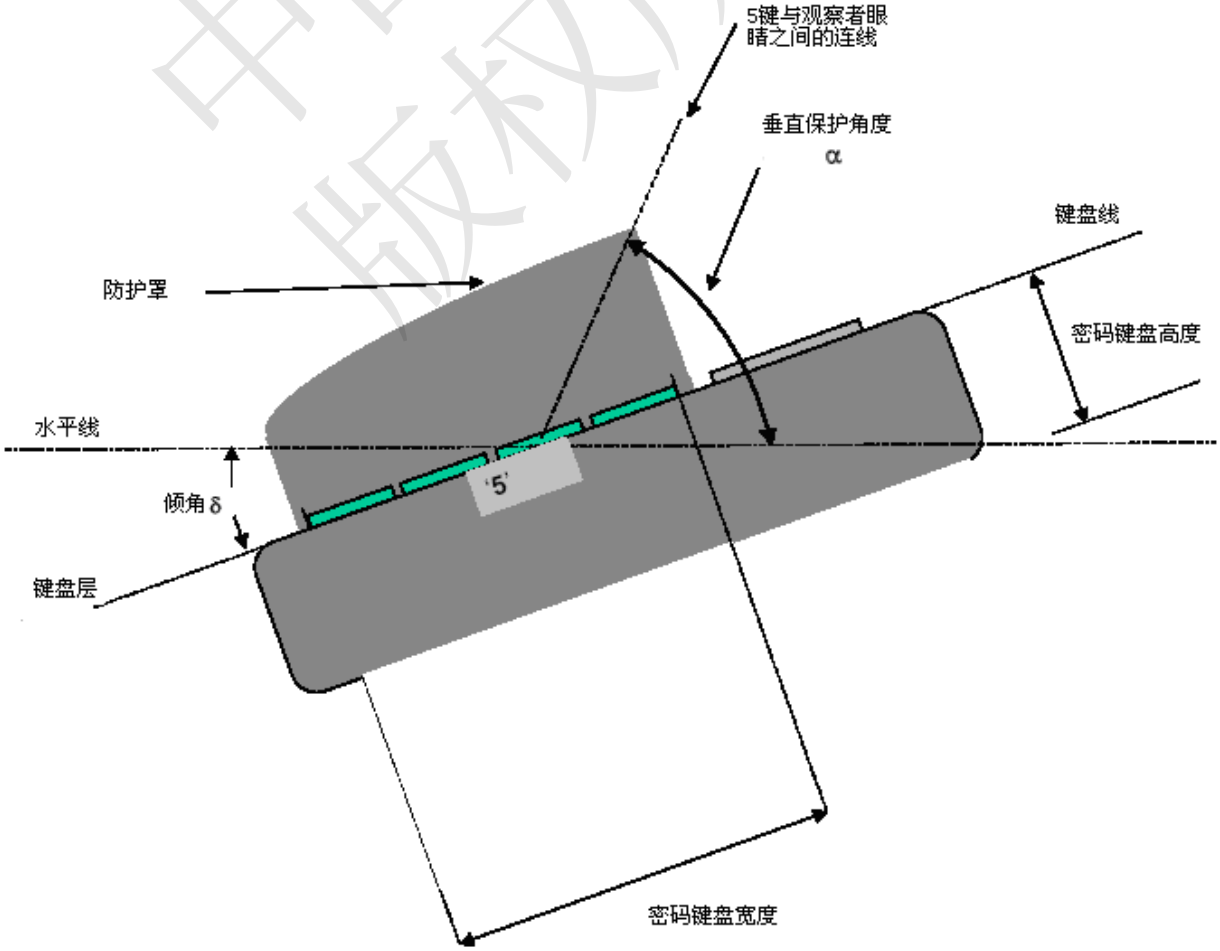
下面的例子，是一个符合安全要求的 PIN 输入设备设计的主体部分，其中就包含挡板的设计。其他设计也可以达到要求。



图A.1 含有挡板设计的 PIN 输入设备样品，俯视图



图A.2 PIN输入设备样品，正视图



图A.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：

a） 重量应不超过500g；

b） 5键处的宽度不得超过3inches或者7.62cm；

c） 5键处宽度与高度的总和应不得超过4inches或者10.16cm；

d） 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≤δ≤45°），并且要求提供以下的保护角度：

注 水平角度β	注 注释	注 垂直角度α
注 315°≤β≤45°	注 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。	注 NA
注 45°≤β≤90° 注 270°≤β≤315°	注 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°。注意：如果PIN输入设备倾斜放置，前面的挡板应该更高。	注 α≥35°
注 90°≤β≤270°	注 保护角度α至少为40°。如果键盘平面向下倾斜，则前挡板则可以适当的降低。	注 α≥40°

表A.1 测试角度要求

表A.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A.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°，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。

A.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

$\alpha \geqslant 20^{o}$。

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：

- 在 PIN 输入设备上标注
- 在显示时进行提示，尽可能使用一个“单击确认”画面
- 印在 POS 上
- 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。下面是一个矩阵的例子：

	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*

表A.2　观察区域以及 PIN 保护方法的矩阵样本

*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。

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 B
（规范性附录）攻击分值计算公式

B.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。除非评估人员认为这种方式并不适用于实际情况，否则这种方法应该被采纳。这样的话，就需要依据某个规则来认定这种方法是否适合于实际情况。

B.2 识别和攻击

攻击者在准备攻击已存在的漏洞时必须首先识别出漏洞。虽然将其分为两个步骤看起来似乎有些不必要，但这实际上是非常重要的一个步骤。为了更好地说明问题，首先考虑一个漏洞，这个漏洞在经过专家的长时间的分析后被公布出来，网络上也发布了相应的简单攻击手段。把这个和另外一个共知的但需要大量时间和资源才能攻破的但广为人知漏洞相比较。在这些案例中需要分别考虑不同的因素(例如:时间)。

B.3 需要考虑的因素

在分析漏洞攻击分值时，应当考虑下列因素：

B.3.1 识别

——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。

B.3.2 （初始）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。

往往，这些因素并不互相依赖，但是在某种程度上却是可以互相替代的。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。下面将就这些因素进行讨论。

B.3.3 攻击时间

攻击时间：指攻击者分析或者攻击所需的时间（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。

B.3.4 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的规则和理念非常熟悉，并且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。就攻击目的而言，精通人员具备顺利完成攻击的技能。

——外行：和专家和精通的人相比是外行，没有专门技术。就攻击目的而言，外行可以按照程序或手册执行基本的攻击操作，无需特别的技能。

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

B.3.5 PIN输入设备相关知识

PIN 输入设备相关的知识指获取特定的和 PIN 输入设备相关的专门技术。这点和通用的技术不同，但是也不是没有关系。可分为以下等级：

——公开的和 PIN 输入设备有关的信息（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。

——受限制的和 PIN 输入设备有关的信息（例如，从厂商技术规格说明书中获取的信息）；如果它是先申请后发放，并且发放需要注册，则此类信息也被认为是受限制的信息（如 PCI PTS POI DTRs）。

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

这里必须仔细区分用来分析漏洞和用来攻击的信息，尤其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。虽然这是潜在的，但技术水平和设备的使用之间的关系并不总是成立的，例如，当环境因素限制专家级的攻击者使用设备，或者使用那些别人已经开发出来并免费发布（例如，通过互联网）的“傻瓜式”攻击工具。

访问 PIN 输入设备也是非常重要的一个方面。假定 PIN 输入设备可以购买到，或者攻击者可以获取到，并且与其他因素一样，分析和修改 PIN 输入设备没有任何时间限制。区别在于被分析/测试设备的状态和功能。

——机械样本是非功能性的且仅仅被用来学习机械设计或者提供备份部件。

——没有工作密钥的功能性样本可以被用来测试设备的逻辑或者电气特性，但是由于其没有使用工作密钥，因此就不能用于网络支付或者由真正的支付卡进行支付。这种设备是可以买到的。

——带有工作密钥的功能性样本是全功能的设备，可以被用来验证一种攻击手段或者执行攻击。

如果在某个类别中需要超过 1 个样本，不能用样本的数量乘上分数，而应当使用下面的因子：

表 B.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

设备指那些需要用来分析或攻击漏洞的设备。

——标准设备，指用于分析漏洞或者进行攻击的，对攻击者来说可以快速使用设备。这类设备很容

易获取，例如，已经在附近的仓库中或者从互联网下载下来的。这类设备可能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。

——专业设备，攻击者不能马上获取，但是可以经过正当途径获得的设备。这包括购买中等数量的设备，（例如，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，指对公众来说还没有的设备，可能需要专门的定制，（例如，非常专业的软件）或者因为设备太专业，控制发放，甚至是严格限制。也有可能是这个设备非常昂贵（例如：离子聚焦光束，扫描式电子显微镜,以及激光打磨器）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。

——芯片级攻击设备，执行必要的芯片级攻击通常不在市场上广泛适用，而且不被允许。它非常贵，因此它自己被认为是个范畴。仅有一下几种设备属于这个范畴：

- 聚焦离子束（Focused Ion Beam）
- 扫描电子显微镜（Scanning Electron Microscope）
- 激光切割设备（Abrasive Laser Equipment）

在一个时期（识别或攻击），如果不同级别的设备都被用到，只保留最高级的设备。

如果同一个设备同时用在不同时期，不能认为设备使用两次。举个例子，设备的花费可以平分在识别阶段和攻击阶段。

部件(Parts) 指隐藏攻击痕迹必需的组件,或者替换在做数据监控或者安装通讯 bug 的攻击中损坏的组件, 例如容器部件,一个显示器或者打印机，建立数据监控或通讯 bug，或者执行攻击必须的组件。

——标准部件是攻击者非常容易得到的部件,或者是通过市场购买的或者从同类型设备样本中拆来的部件。

——专用部件(Specialized parts) 目前不是攻击者已有的，但是可以经过正当途径获得的。可能是可以从市场订购的，但需要很长的运送时间，或者说需要按批购买的组件。

——定制部件（Bespoke parts），目前还无可用的，需要专门制造。如果攻击需要专门定制部件，则这种攻击方式不大可行。

识别阶段使用的部件可以在攻击阶段使用，必须在两个阶段使用同样的分值作计算。如果部件不能容易地被复用（部件一旦被安装便不能继续使用，如与环氧树脂粘合很难分开）则部件被当做使用两次：识别阶段用一次，攻击阶段再用一次。

B.3.6 攻击阶段的评定

应注意，只有初始的攻击阶段需要被考虑，因为深入的攻击阶段可以复用设备和知识，达到最优化，在实验室的评估过程中，通常很难评估深入的攻击阶段。

在深入的攻击阶段，下列因素在计算分值中通常加以复用：

——设备

——知识

如果多个攻击场景具有相同的总分值和攻击阶段分值，那么应考虑在攻击阶段具有最少成本的攻击场景。

B.3.7 攻击成功率的评定

如果实施攻击的难度非常高，导致攻击很可能只在有限数量的目标上才能成功，则需要在下列限定条件下，考虑使用多个设备。

为了体现这一情况，目标设备的数量（例如，攻击阶段中带有工作密钥的功能样本）可以被乘以下表中的因子。

表 B.2 多个样本因子

成功概率	因子
P >= 0.5	1
0.5 > P >= 0.25	1.5
P < 0.25	2

在确定概率时，攻击的每一步都要分解为具有特征概率的独立阶段。总概率为所有因子的乘积。

如果总概率低于 0.5 时，需要合理的文档解释。确定概率的方法通常基于对设备的测试，也可能包括合理的采样以获取有意义的统计数据。

B.4 攻击分值计算方法

上一节分析了决定攻击分值的因素。下表给出了各个因素的计算规则。当某个因素接近一个边界时，评估员应当考虑表格中相关两个个数值的中间值。

针对一个既定的攻击，提出多种攻击场景的分值计算是必要的。（例如：替换专业人员的攻击时间和设备）。保留这些方案的最低分值。当分析出一个漏洞，并且这个是在公用域中，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，而不是最初来识别它的分值。

表 B.3 多个样本因子

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
	<= 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	机械样本	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
	芯片级别的攻击	7	7
特殊部件需求	无	0	0

	标准的	1	1
	专用的	3	3
	定做的	5	5

B.5 第一个攻击实例

本攻击的目标是向 PIN 输入设备中插入一个 PIN 探测 bug。这个 bug 被放入设备的键盘接口附近，位于外壳的下面，用于监控键盘信号和记录输入的 PIN 值。

B.5.1 识别阶段

对设备进行逆向工程以理解其设计原理，包括入侵检测传感器和键盘信号。这个步骤需要电子工程的专业知识，用于理解安全信号的走线和键盘扫描方法。确定入侵机制的位置，设计方法使这些机制被绕过或无效。因此本步骤需要 60 小时的时间，专家技术水平，标准设备和一个机械样本。

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

定制 bug，用于监控键盘信号和记录输入的 PIN 值。在本例中键盘扫描技术比较简单，因此可应用如下级别的因素：专家，30 小时的时间，标准部件，标准设备，复用相同的机械样本。

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

攻击者使用带有测试密钥的功能样本练习。注入测试密钥和复位入侵状态需要访问密钥装载软件或规范——需要限制级别的知识。

技术水平	设备	知识	部件	样本	时间
专家	标准	限制	标准	一个带有测试密钥的功能样本	40 小时

总结识别阶段，采用的攻击因素如下所示。

技术水平	设备	知识	部件	样本	时间
专家	标准	限制	标准	一个机械样本和一个带有测试密钥的功能样本	130 小时

B.5.2 攻击阶段

攻击者使用带有密钥的功能样本进行攻击。实施攻击的几个必须步骤如下所示。

攻击入侵检测机制以侵入设备内部。假设外壳可以使用备用的部件替换，每一路检测机制的攻击成功率为 0.9，每路机制需要一小时的时间。在本例中，一共存在 8 路入侵检测机制，但是只有 4 个需要攻击。额外需要一小时的时间用于提供攻击稳定性。

尽管攻击是脚本化的，但是仍然需要良好的机械技能和成功实施的练习。因此，技术水平可以采用精通级别。

技术水平	设备	知识	部件	样本	时间
精通	标准（复用）	公开	无	1 个带有密钥的功能样本 成功概率 $P=0.9^4\approx0.66$	5 小时

一旦侵入到设备内部，攻击者需要访问位于终端内部深层的敏感信号（例如，键盘扫描信号），这些信号由其他较难攻击的入侵检测机制保护。

技术水平	设备	知识	部件	样本	时间
专家	标准（复用）	公开	无	1 个带有密钥的功能样本 成功概率 P=0.8	12 小时

一旦上述步骤成功实施，攻击者就可以将 PIN 探测 bug 安装于键盘线上，替换外壳，测试设备。此后，设备可被放回到目标商户或商城。由于从上述步骤只能获取有限的访问空间，安装 bug 时需要专业设备。

技术水平	设备	知识	部件	样本	时间
精通	专业	公开	标准	一个带有密钥的功能样本 成功概率 P=1	6 小时

总结攻击阶段，采用的攻击因素如下所示。

技术水平	设备	知识	部件	样本	时间
专家	专业	公开	标准	一个带有密钥的功能样本 成功概率 P≈0.52	23 小时

表 B.4 插入一个 PIN 探测 bug 的攻击分值

相关方面	识别值		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，一个不带有工作密钥的功能样本	3	带有工作密钥的功能样本 成功概率 P≈0.52	4
设备	标准	1	专业	3
专用部件	标准	1	标准	1
每个阶段攻击分值		16		15
总共攻击分值		31		

B.6 第二个攻击实例

这个攻击的目标在于使用侧信道分析例如 DPA 确定 DES 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。

——PIN 输入设备没有有效的防 DPA 的功能。

攻击包含以下步骤：

——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。

——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。因为需要大量的 PIN 输入，而这些输入很难手动进行，因此会采用一种专门的机制来进行 PIN 的输入。这是定制设备，专门为这个攻击定做的，在分析阶段也会用到。

——得到一个 PIN 输入设备，并测试。我们希望观察至少几千次 PIN 输入以及随后的加密过程。在识别阶段可能会重复多次收集过程才能存储足够的数据。大约需要一周时间完成收集。由于数据捕获的时间很可能超过一周的时间，这项工作极有可能和一个模拟主机运行离线的 PIN 输入过程。

——分析采样数据，得到 PIN 加密密钥，这个过程中使用侧信道技术获取密钥。

使用和第一个例子相同的手段，估计攻击分值，如下表所示：

表 B.5 DPA 分析攻击分值例子

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	带有测试密钥的功能样本	2	带有工作密钥的功能性样本	4
设备	定制	5	专业	3
专用部件	标准	1	不需要其他的部件	0
每个阶段攻击分值		19.5		15
总共攻击分值		34.5		

附 录 C
（资料性附录）厂商评估调查问卷（范例）

C.1 物理安全

C.1.1入侵检测机制	
如终端符合此项，请描述：	
1.	防篡改机制。
2.	触发机制后的入侵响应。
3.	设备检测到的入侵行为后如何反应。(回答应包括关于入侵检测机制如何工作以及如何擦除秘密信息或（和）不可用的书面描述)。
4.	除入侵检测外，请描述防止访问敏感信息或者防止置入窃取装置的保护措施。
5.	防止设备被物理渗透攻击的机制。
6.	请合理解释,说明为什么设备的实现能够使必须有至少花费 26 分的潜在攻击才能侵入和修改设备从而泄露敏感信息或置入 PIN 窃取装置，攻击阶段分值至少 13 点，攻击时间至少 10 个小时。
7.	擦除了什么敏感信息，以及使用了什么机制进行擦除的。
8.	未被擦除的敏感信息是如何被保护的。
	备注：

C.1.2 独立安全机制	
如终端符合此项，请描述：	
1.	入侵检测和入侵证据的结合。
2.	安全机制如何工作。
3.	安全机制如何相互独立。
4.	为什么安全机制未依赖于不安全的符合和特性。
	备注：

C.1.3 环境和操作条件改变的适应性	
如终端符合此项，请描述：	
1.	设备的操作条件和环境条件。
2.	为何设备的操作条件和环境条件不会危及到设备的安全性。
3.	为确保在操作条件和环境条件改变的情况下设备的安全性所做的测试（请提供测试报告）。
4.	为何这些措施足够且有效。
	备注：

C.1.4敏感功能或信息保护	
如终端符合此项，请描述：	
1.	存在哪些敏感信息和功能。
2.	敏感功能在哪里执行，敏感信息在哪里使用。
3.	敏感信息以及处理敏感信息的功能如何被保护不受改动。
4.	请合理解释为何这些措施有效且足够，并说明为何这些措施使得对于每台设备的攻击至少花费 26 分，其中攻击阶段至少 13 分。
5.	描述用于影响安全相关功能的公钥如何被保护不会受修改或替换。
6.	请描述用于影响安全相关功能的私钥如何被保护不受改动、替换和泄露。
	备注：

C.1.5PIN输入过程监控	
如终端符合此项，请描述：	
1.	设备防止通过监听声音泄露密码的保护措施。(此处声音并非指前文所提的音调，而是指敲击键盘发出的其他声音)。
2.	设备防止监测电磁辐射的保护措施。
3.	做过的电磁辐射相关测试，并请提供测试数据。

4.	设备防止监测能量消耗的保护措施，并请提供测试数据。
5.	列入考虑的其他任何外部特征，如果可行，请提供测试数据。
6.	请合理解释为什么至少要花费 26 分（攻击阶段 13 分）才能通过监听声音、监测电磁辐射或能量消耗以窃取 PIN。
	备注：

C.1.6密钥识别分析	
如终端符合此项，请描述：	
1.	在设备设计上所考虑的入侵留痕特性，如特殊的外壳、防伪标记、染色机制等。
2.	设备或 IC 卡读卡器是否包括入侵检测机制？
3.	敏感部分是否用环氧树脂保护？如果是，请描述其类型及厚度。
4.	请合理解释为何设备或 IC 卡读卡器实现了防止设备或者 IC 卡读卡器内的任何 PIN 安全相关的密钥行为，无论是通过侵入设备或读卡器还是通过监测设备或 IC 卡读卡器的辐射波（包括能量波动），都至少要花费 35 分（攻击阶段至少 15 分）。
	备注：

C.1.7 设备显示的物理安全	
如终端符合此项，请描述：	
1.	防止更改非 PIN 数据的提示信息的防护措施。
2.	设备对于更改非 PIN 数据的提示信息的行为如何反应。
3.	合理解释为何攻击至少要花费 18 分（攻击阶段至少 9 分），才会通过更改提示信息的方式获得 PIN。
	备注：

C.1.8 防偷窥保护	
如终端符合此项，请描述：	
1.	设备提供的阻止 PIN 在持卡人输入时被监视的方法。
	备注：

C.1.9 磁条读卡器保护	
如终端符合此项，请描述：	
1.	请描述用于保护磁条阅读器磁头的技术，以及相关的硬件和软件。
2.	合理解释为何篡改或渗透设备，以对磁条于阅读器进行任何附加、替换或篡改操作以达到获得或篡改磁条磁道数据的目的，必须至少花费 16 分（攻击阶段至少 8 分）。
	备注：

C.1.10 无人值守设备防移除	
如终端符合此项，请描述：	
1.	设备实现的用来防止未经许可的移除操作的机制。
2.	防移除机制的设计，防移除机制是主动还是被动。
3.	当一个防移除机制被触发后，设备有何行为。
4.	合理解释为何对每台设备的攻击分数必须至少花费 18 分，（攻击阶段 9 分），否则无法使得防移除检测机制失效。
	备注：

C.1.11 PIN输入音调	
如终端符合此项，请描述：	
1.	每个数字键的音调。
2.	发音装置。
3.	发音装置的能量信号。
	备注：

C.2 逻辑安全

C.2.1 自检测试	
如终端符合此项，请描述：	
1.	设备或 IC 卡读卡器进行的所有自检。

2.	各种自检失败时设备或 IC 卡读卡器的反应。
3.	各种测试中触发自检的事件类型。
4.	表明自检已经执行的可见提示或数据反应。
	备注：

C.2.2 逻辑异常

如终端符合此项，请描述：	
1.	设备接受哪些命令。
2.	命令与设备模式的关系。
3.	都执行何种类型的参数和数据检查。
4.	其功能为何不会受逻辑异常的影响。
5.	为确保功能不受逻辑异常影响所做的任何测试。请提供合理解释说明为何这些实验的充分性。
6.	敏感信息或个人密码如何受到保护而不会被泄露明文。
	备注：

C.2.3 固件和应用软件的认证及更新

如终端符合此项，请描述：	
1.	归档的固件评审过程和频度。
2.	能够证明固件无隐藏、未授权或未公开的功能的评估细节。
3.	用于固件认证的密码算法和密钥长度。
4.	若升级固件时认证失败，则设备如何反应。
5.	若被拒绝，固件时如何被删除的。
	备注：

C.2.4 PIN输入区别

如终端符合此项，请描述：	
1.	持卡人输入密码数字时屏幕如何显示。
2.	输入密码时，终端操作者和/或收银台的屏幕如何显示。
	备注：

C.2.5 内存清除

如终端符合此项，请描述：	
1.	如何确保持卡人确认完整输入 PIN 后，PIN 在设备内会立刻被加密。
2.	如何确保 PIN 在加密后，在任何位置都不会有 PIN 的明文。
3.	持卡人完成输入后，PIN 以明文形式存在的最长时间。
4.	交易完成后，设备缓冲区自动清除的数据。
5.	所有进行清空的缓冲区的位置。
6.	清空缓冲区的过程。
7.	设备等待持卡人或商户响应的超时时间。
8.	设备等待超时后的行为。
	备注：

C.2.6 敏感服务

如终端符合此项，请描述：	
1.	设备或 IC 卡读卡器具有的敏感功能(敏感功能指并非终端用户可以访问的却能够影响设备安全的功能，如密钥加载)。
2.	设备或 IC 卡读卡器如何控制敏感功能的访问和使用。
3.	用于访问敏感服务的认证方法。
4.	确保进入或退出敏感服务不会泄密或影响敏感信息的措施。
5.	用来认证访问敏感服务的接口。

6.	是否有外部设备用于认证设备访问敏感服务，若有，其保护措施是什么。
7.	用于访问设备和 IC 卡读卡器内敏感服务的认证信息，当其在接口处输入/输出时是如何保护的。
8.	下列关于问题 7 中涉及的数据，哪些为真。 ☐ 输入数据时，屏幕上显示无法识别的字符。 ☐ 无法通过监听声音或电磁辐射识别输入的数据。 ☐ 退出安全模式时，内部缓冲区自动清除敏感信息。
9.	任何认证数据的管理，认证数据包括口令、密钥和硬件令牌等。 共享相同口令和密钥的设备数目： 用于认证的可用密码算法： 数据长度（密钥或口令的长度）： 认证数据如何发送至合法用户： 认证数据如何升级：
10.	设备或 IC 卡读卡器对错误认证数据的反应。
11.	使用敏感功能时，操作次数限制是多少。
12.	合理解释为何选择此数目作为限制条件。
13.	使用的操作次数限制如何将未授权用户使用敏感服务的风险最小化。
14.	若操作次数达到限制，PIN 输入设备如何反应。
15.	一旦访问敏感功能，PIN 输入设备保持非活动状态的最长时间。
16.	若非活动状态超时后，PIN 输入设备如何反应。
17.	从 PIN 输入设备开始访问敏感功能到其恢复正常模式之前的最长时间。
18.	若达到最长间隔时间，PIN 输入设备如何反应。
	备注：

C.2.7 随机数	
如终端符合此项，请描述：	
1.	随机数生成器的实现。
2.	能够证明所生成的随机数的随机性的测试。

3.	请描述随机数生成器如何保护敏感数据。
	备注：

C.2.8 PIN防穷举

如终端符合此项，请描述：

1.	哪些特性能够防止或大多数情况下杜绝窃取设备的使用以保护 PIN 不被穷举。
2.	PIN 的输入如何被限制在平均 30 秒一次。
	备注：

C.2.9 密钥管理技术

如终端符合此项，请描述：

1.	关于固定密钥、主密钥或一次一密的 PIN 保护技术。
2.	各密钥是否用于一个加解密用途？如何确保？
3.	保护密钥时，如何保护其不受非授权的更改和替换？
4.	密钥存储时，如何保证密钥分散管理？
5.	设备实现所有的加密算法。
6.	设备内的所有密钥都应该说明以下信息： 密钥命名： 密钥长度： 相关加密算法： 可能用此密钥加密的数据： 此种密钥的实例和注册数量： 设备如何确保该密钥以使其只用于既定目标：
7.	设备是否有擦除密钥的功能。 是 □　　否 □
8.	哪些密钥可能被擦除。
9.	擦除具体过程。
10.	何种情况下擦除密钥？针对所有设备状态（上电、下电、休眠）进行描述。
11.	其他可能被擦除的数据有哪些？在何种情况下？

12.	哪些密钥不会被擦除。
13.	所有设备中出现的或者使用的密钥如何加载？包括由谁生成以及密钥加载是否以加密形式、或者明文形式、还是以部分明文部分加密的形式。、
14.	是否有使用带有公钥的不对称算法替换对称密钥的密钥分配技术，请对以下几点进行描述： 利用随机数/伪随机密钥生成过程从而使生成的密钥不可预测或确定其可能密钥空间？随机数的源是否在密钥生成之前就已经做过恰当的测试？ 如何做到对公钥的认证？是否有签名分级制度？这些签名如何生成，例如，由谁签名。 是否有设备双向认证？如何使用签名，那么对签名是如何测试、接受或拒绝的？ 使用的包含对称密钥的信息是否有安全格式和安全防护？接受者是否对信息结构的正确性进行测试？如何保证对原始信息的认证，比如交换信息的签名是否经过测试。 若认证测试失败，设备如何反应。 有问题的加密算法使用哪种（些）有效的密钥长度？选定的密钥长度是否适合该算法及其安全要求？假设使用 RSA，密钥长度是否至少 1024 位。 密码成分能否被载入？输入密钥时用于加密的算法是什么？ 请描述设备中显示或使用的各密钥存储和应用的区域。 请描述设备所支持的密钥转换技术和存储机制的混合使用。（如 ANSI TR-31）。 是否设备使用了密钥推算的方法？如果使用了，请进行描述。
	备注：

C.2.10 PIN加密算法

如终端符合此项，请描述：

1.	3DES 实现是否符合 ANSI X9.52 和 ISO9564 标准？如何符合。
2.	设备是否支持 PIN Block 格式。
	备注：

C.2.11 数据加解密

如终端符合此项，请描述：	
1.	关于各个用于加密 PIN 的密钥，请简要说明哪种数据可以被加密或解密。
2.	如何把明文 PIN 数据同其他可能输入设备的数据区分开来？
3.	被加密的 PIN 数据如何区别于其他的被加密或明文数据。
4.	所有用于加密密钥的密钥。
5.	用密钥加密密钥可以加密哪些数据。
6.	这些数据如何与其他数据区别开来。
7.	加密密钥如何区别于其他数据。
8.	设备如何使得数据加密密钥、密钥加密密钥和 PIN 加密密钥对应不同的值。
	备注：
C.2.12 明文密钥安全	
如终端符合此项，请描述：	
1.	是否允许输出明文密钥或明文 PIN 的机制？若有，请描述该机制（包括如何加密密钥）。
2.	如何防止明文密钥和明文 PIN 的输出？
3.	加密密钥的明文可以存在于设备的哪个部分？
4.	在何种情况下一个密钥明文可能从上述区域转移到设备的其他区域。
	备注：
C.2.13 交易控制	
如终端符合此项，请描述：	
1.	交易是否只在持卡人的意愿下执行（无商户的帮助）？
2.	交易额是持卡人还是商户输入？
3.	如何实现输入交易额和输入 PIN 是两个不同的操作？
	备注：

C.2.14 设备显示的逻辑安全	
如终端符合此项，请描述：	
1.	防止更改非 PIN 数据的提示信息的防护措施。
2.	设备对于更改非 PIN 数据的提示信息的行为如何反应。
3.	合理解释为何攻击至少要花费 18 分（攻击阶段至少 9 分），才会通过更改提示信息的方式获得 PIN。
	备注：
C.2.15 应用隔离	
如终端符合此项，请描述：	
1.	设备是否支持多应用。
2.	如果设备支持多应用，如何确保各个应用之间相互隔离，保证一个应用的数据不可被其他应用访问。
	备注：
C.2.16 操作系统最小配置	
如终端符合此项，请描述：	
1.	设备使用的操作系统是什么。
2.	设备操作系统如何进行配置，采取什么原则。
3.	设备开启了哪些服务，对于不需要的服务如何处理。
	备注：
C.2.17 组件集成文档	
如终端符合此项，请描述：	
1.	是否有安全集成文档指令其他安全组件安全集成到设备中。
2.	提供相关集成文档。
	备注：

C.2.18 安全策略	
如终端符合此项，请描述：	
1.	设备是否有提供给用户正确使用的安全策略。
2.	安全策略主要对哪些方面进行了说明。
3.	提供相关文档
	备注：

C.3 联机PIN安全

C.3.1 密钥替换	
如终端符合此项，请描述：	
1.	使持卡人或商户可以确认命令选择键的可行方法（如按下后可以在各账户之间进行选择的键）。
2.	设备如何禁止非授权的密钥更换和滥用？
3.	如果设备支持多重密钥等级，那么设备如何识别密钥选择命令？
	备注：

C.4 脱机PIN安全

C.4.1 防渗透保护	
如终端符合此项，请描述：	
1.	用于防止侵入设备以获取或修改敏感数据的保护措施。
2.	侵入设备以获取或修改敏感数据所必须的专业技术和设备。
3.	为何必须有花费 20 分（其中攻击阶段至少 10 点，攻击时间至少 10 个小时）的攻击才可能侵入设备或 IC 卡读卡器以修改设备或 IC 卡读卡器的硬件或软件从而获取或修改敏感信息。
	备注：

C.4.2 IC卡读写器结构
如终端符合此项，请描述：

1.	合理解释为何插卡口没有足够空间放置 PIN 窃取装置。
2.	可以隐藏在 IC 卡读卡器插卡口最大物体的尺寸。
3.	IC 卡读卡器内部空间尺寸。
4.	为了评估方便，请提交关于 IC 卡读卡器的结构和尺寸信息的所有设计相关文档，装配图等。
5.	合理解释为何 IC 卡读卡器的插口无法扩大到足够置入 PIN 窃取器。
6.	所有用来防止 IC 卡读卡器插口扩大的材料或保护措施。
7.	是否有足够的空间可以同时插入两张 IC 卡而不影响正常卡片的使用。
8.	IC 卡读卡器的插口以及其如何设计以保证阻塞物或其他可疑物体能够被持卡人发现。
9.	IC 卡插入过程，包括任何插口盖的作用和功能。
10.	合理解释 IC 卡读卡器的构造如何设计从而使持卡人可以看到从插卡口处连接到外部窃取装置的电线。
11.	设备的 IC 卡插口附近是否有焊接口或插槽？如有，请合理解释为何这些不会被用于连接外部窃取器。
	备注：

C.4.3 PIN传输保护	
如终端符合此项，请描述：	
1.	设备是否同时支持密文和明文方式的 IC 卡用户认证。
2.	如果 IC 卡读卡器和设备分离，设备之间的 PIN 如何加密，请详细说明使用的算法和密钥。
3.	如果 IC 卡读卡器和设备一体，PIN 提交给 IC 卡读卡器时，用于加密的密钥和算法。
4.	什么条件下明文 PIN（或 PIN Block）可能输出到设备或 IC 卡读卡器外。
	备注：

C.5 集成安全

C.5.1 配置管理	
如终端符合此项，请描述：	
1.	所有设计参考文档，能够提供物理和逻辑安全信息（与 PIN 输入和读卡功能相关的）的装配图、原理图和数据手册。
	备注：

C.5.2 PIN输入功能集成	
如终端符合此项，请描述：	
1.	所有设计参考文档，能够提供信息表明一个通过认证的安全组件集成到终端不会影响整个设备保护级别，包括装配图、原理图和数据手册。
2.	如何保证每个已通过认证的安全组件的集成方式严格按照组件生产商的推荐执行。
3.	为什么一个已通过认证的安全组件失效、移除和缺失时不会导致另一个已通过认证的安全组件泄露任何与 PIN 相关的敏感信息。
4.	当已通过认证的安全组件失效、移除和缺失时，防止 PIN 输入设备回退到不安全模式的机制。
5.	用于验证上述措施有效性的测试。
	备注：

C5.3.1 安全等级保持	
如终端符合此项，请描述：	
1.	所有设计参考文档，能够提供信息表明一个通过认证的安全组件集成到终端不会引入新的攻击 PIN 的方式，包括装配图、原理图和数据手册。
2.	如何保证每个已通过认证的安全组件的集成方式严格按照组件生产商的推荐执行。
3.	为什么安全组件的失效不会引入新的攻击 PIN 的方式，例如 PIN 输入设备不会回退到不安全模式。
	备注：

C5.3.2 防卡片盗取
如终端符合此项，请描述：

1.	设备防止银行卡被保存或盗取的保护措施。
2.	是否使用了主动或被动机制。
3.	如果上述机制导致设备被锁定，描述如何进行解锁。
4.	请合理解释为何设备的实现能够有效防止黎巴嫩环的攻击。
5.	用于验证上述措施有效性的测试。
	备注：

C5.3.3 组件隔离

如终端符合此项，请描述：

1.	所有设计参考文档，能够定义安全和非安全组件之间的逻辑和物理隔离，包括用户指南、设备的逻辑结构规范、设备的接口规范或软件实现。
	备注：

C5.3.4 设备显示安全

如终端符合此项，请描述：

1.	描述交易流程中硬件和软件组件如何控制显示和设备。
2.	如何强制保证显示给持卡人的信息与运行状态（例如，安全和非安全模式）是对应的。
3.	如果使用加密方式，描述使用的技术，涉及的组件和密钥管理。
4.	接收的外部设备的命令是否会影响显示信息与设备运行状态的对应性。 是 □ 否 □ 如果是，使用了何种认证方式。描述其中的算法，密钥和密钥管理。
5.	请合理解释，说明为什么必须有至少花费 18 分的潜在攻击（其中实施阶段至少 9 分）才能修改显示信息和运行状态的对应性。
	备注：

C5.3.5 密码输入接口控制

如终端符合此项，请描述：

1.	设备的哪些接口可以接受数字输入。

2.	设备的哪些接口用于输入银行卡密码。
3.	如果有其他可用于输入数字的接口，什么机制保证该接口不会被非法用于输入 PIN。
	备注：

C5.3.6 设备移除要求

如终端符合此项，请描述：

1.	设备是否包含在 C1.9 评估下的安全组件。
2.	保护组件不被未授权移除的机制。
3.	该机制的设计情况。
4.	该机制是主动的还是被动的。
5.	当机制被触发时会发生什么情况。
6.	安装，激活，暂时禁用和重新激活的方法。
7.	如果有密码或其他秘密数据用于该机制，描述初始化过程和使用方式。
8.	请合理解释，说明为什么必须有至少花费 18 分的潜在攻击（其中实施阶段至少 9 分）才能禁止触发机制来未授权移除组件。
9.	所有设计参考文档，提供关于保护系统，防止未授权移除的信息，包括装配图，原理图和数据手册。
10.	集成文档的审阅流程和更新的发布周期，以及发布周期和设计/生产周期的关系。
11.	集成文档的分发流程。
12	所有设计参考文档，提供关于嵌入式设备的保护系统，防止未授权移除的信息，包括装配图，原理图和数据手册。
	备注：

C.6 开放协议

C.6.1 协议和接口声明和定义

如终端符合此项，请描述：	
1.	使用开放协议的所有物理和逻辑接口。分别描述接口名称和相应的参考文档。
2.	可用于上述接口的所有协议和服务。分别描述协议和服务名称以及相应的参考文档。
3.	上述接口是如何配置以接收命令的。
4.	针对每个接口，由哪个组件实现协议？如果是安全协议，描述相应的软件实现。
	备注：
C.6.2 漏洞评估	
如终端符合此项，请描述：	
1.	为厂商提供的漏洞评估过程与文档。
2.	厂商用于检测所有接口漏洞的过程。
3.	厂商漏洞评估过程如何描述漏洞的分类与识别流程，包括正确的描述，关键程度和解决措施。
4.	厂商关于新漏洞的及时检测的过程，确认过程中存在审计记录。
5.	平台上所有可用的协议和服务的参考文档。
6.	上述协议和服务的漏洞评估如何执行，为什么所做评估能保证不含可被利用的漏洞。
7.	漏洞评估文档，漏洞调查证据和测试证据。
8.	漏洞发布措施的参考文档。
9.	厂商对于新发现的漏洞的及时解决措施，以及持续更新和记录所有漏洞的流程。
	备注：
C.6.3 厂商指南	
如终端符合此项，请描述：	
1.	安全使用所有逻辑和物理接口的厂商安全指南。
2.	安全使用所有协议和服务的厂商安全指南。

3.	所有逻辑和物理接口的默认配置的厂商安全指南。
4.	密钥和证书使用的厂商安全指南。
	备注：

C.6.4 运行测试

如终端符合此项，请描述：

1.	描述所有使用的开放安全协议。
2.	用于提供数据机密性的安全协议的加密机制。
3.	用于提供数据完整性的安全协议的机制。
4.	用于提供服务器认证的安全协议的机制。
5.	提供异常处理和重放检测的安全协议的机制的相关文档。
6.	用于提供会话管理的安全协议的加密机制。描述协议名称和参考文档。
7.	设备会话管理的特性，确保连接只在必要时开启。
8.	设备会话管理的特性，确保设备限制设备所维持的并发连接的数量。
	备注：

C.6.5 管理和维护

如终端符合此项，请描述：

1.	厂商配置管理的流程。
2.	厂商维护的流程。
3.	厂商更新的流程，包括软件和固件更新。
4.	厂商用于升级配置的软件的认证和安全流程。描述机密性，完整性，服务器认证和防止重放的机制。
5.	如果真实性未得到确认的流程。
	备注：

C.7 账户数据保护

C.7.1 账户数据处理	
如终端符合此项，请描述：	
1.	实现账户数据保护功能的组件。
2.	对于每一已识别的组件，账户信息何时何种方式被加密。
3.	除了加密，安全控制器可以执行的其他操作。
4.	对于每一已识别的操作，为什么这些操作不会影响加密功能的安全性。
5.	请回答 D4.1 节防渗透保护部分的问题。
6.	请回答 C1.9 节磁条读卡器保护部分的问题。
	如果主账号密钥为手动输入，请回答 7-9 三个问题。
7.	防止设备被渗透攻击获取或修改账户数据的保护措施。
8.	为获取或修改账户数据对设备而进行渗透攻击所必须的专业技能和设备。
9.	请合理解释，说明为什么必须有至少花费 16 分的潜在攻击（其中实施阶段至少 8 分）才能对设备进行渗透攻击以获取或修改账户信息。
	如果设备支持非接模式，请回答 10-12 三个问题。
10.	保护非接数据传输的机制。
11.	为获取或修改账户数据对设备而进行渗透攻击所必须的专业技能和设备。
12.	请合理解释，说明为什么必须有至少花费 16 分的潜在攻击（其中实施阶段至少 8 分）才能对设备的硬件或软件进行渗透攻击以获取或修改账户信息。
13.	防篡改机制。
14.	触发机制后的入侵响应。
15.	设备检测到的入侵行为后如何反应。(回答应包括关于入侵检测机制如何工作以及如何擦除秘密信息或（和）不可用的书面描述)。
16.	除入侵检测外，请描述防止访问账户信息或者防止置入窃取装置的保护措施。

17.	防止设备被物理渗透攻击的机制。
18.	请合理解释，说明为什么 PIN 输入设备的实现能够使必须有至少花费 16 分的潜在攻击（实施阶段至少 8 分）才能侵入和修改设备从而泄漏敏感信息或植入账户信息窃取装置。
19.	擦除了什么敏感信息，以及使用了什么机制进行擦除的。
20.	未被擦除的敏感信息是如何被保护的。
	备注：

C.7.2 集成条件下的账户数据保护

如终端符合此项，请描述：

1.	所有设计参考文档，能够提供信息关于已通过认证的组件集成到 PIN 输入设备中不会对账户数据引入新的攻击路径，包括装配图、 原理图和数据手册。
2.	如何根据组件生产商的推荐保证已通过认证的组件的集成被严格执行。
3.	为什么组件的失效不会对账户数据带来新的攻击路径。
4.	设备组件是否允许访问其内部存储或服务区域。 是 □ 否 □
5.	如果上述回答是，内部区域的设计如何阻止被账户数据的访问。
6.	如果上述回答是，导致账户数据被立即清除的机制。
7.	机制是如何触发的。
8.	账户数据擦除方法。
	备注：

C.7.3 密钥保护

如终端符合此项，请描述：

1.	在设备需求范围内，设备存储和使用密钥的设备组件。
2.	设备实现的不同的加密操作，操作是由软件还是硬件实现的，操作是如何防止旁路攻击的。

3.	由加密处理组件实现，用于防止针对加密注入错误的毛刺攻击和获取密钥的芯片级攻击的保护措施。
4.	设备组件设计上所考虑的入侵留痕特性，如特殊的外壳、防伪标记、染色机制等。
5.	在这些组件中设备是否包含入侵检测和响应机制。 是 □　　否 □ 如果回答是，回答 C7.1 的问题。
6.	在这些组件中设备是否包含反入侵机制。 是 □　　否 □ 如果回答是，回答 C7.1 的问题。
7.	请合理解释为何设备实现了防止获取设备内的任何账户数据加密的相关的密钥的行为，无论是通过侵入设备还是通过监测设备的辐射波（包括能量波动），都至少要花费 26 分（实施阶段至少 13 分）。
8.	公钥的完整性如何保证。
9.	公钥的真实性如何保证。
10.	请合理解释为何设备实现了防止修改设备内的任何公钥的行为，无论是通过侵入设备还是通过监测设备的辐射波（包括能量波动），都至少要花费 26 分（实施阶段至少 13 分）。
	备注：

C.7.4 加密机制

如终端符合此项，请描述：	
1.	使用的加密算法。
2.	使用的填充机制。
3.	使用的运算模式。
4.	使用的密钥长度。
5.	所有设计参考文档，能够提供信息关于使用的加密算法，填充机制和运算模式，包括安全评估报告，原理图，数据手册，厂商测试流程和测试报告。
6.	如果使用了非标准的运算模式，提供专家审阅的凭据，以证明加密算法使用的运算模式的安全性已得到评估。

7.	审阅的专家与厂商的独立性如何保证。
	备注：

C.7.5 远程密钥发布

如终端符合此项，请描述：	
1.	设备如何支持双向认证。
2.	提供双向认证的机制。
3.	双向认证过程中传输的信息如何保证时效性和生存周期。
	备注：

C.7.6 数据源认证

如终端符合此项，请描述：	
1.	提供数据源认证的机制。
	备注：

C.7.7 密钥唯一性

如终端符合此项，请描述：	
1.	保证设备使用的密钥唯一性的过程。
	备注：

C.7.8 加解密数据对象控制

如终端符合此项，请描述：	
1.	对于设备中存储的用于加密账户数据的密钥，描述何种类型的数据可以被加密，解密，签名和验签。
2.	明文账户信息与向设备输入的其他信息是如何区分的。
3.	密文账户信息与其他密文或明文信息是如何区分的。
4.	所有的账户信息密钥加密密钥。

5.	可以使用密钥加密密钥加密的账户信息。
6.	上述账户信息如何与其他信息相区分。
7.	账户信息加密密钥如何与其他信息相区分。
8.	设备如何保证账户信息加密密钥，密钥加密密钥和 PIN 加密密钥具有不同的值，特别地，设备中的任何一个密钥都不能与其他密钥的值相同。
	备注：

C.7.9 远程访问

如终端符合此项，请描述：

1.	设备中什么组件可以远程连接。
2.	远程连接使用的机制和受到影响的设备组件。
3.	对于尝试初始化访问的实体，如何保证它的责任。
4.	访问尝试的时效性和生存期如何保证。
5.	远程连接使用了什么加密算法（包括填充机制和运算模式），协议，密钥长度。
6.	如果访问请求不能得到认证，设备有何响应。
7.	如果连接被拒绝，如何放弃连接。
	备注：

C.7.10 固件审查

如终端符合此项，请描述：

1.	归档的软件开发流程，应详细描述如何进行固件审查和测试，以保证不受到安全漏洞影响。
2.	能够证明固件无隐藏、未授权或未公开的功能的评估细节。
3.	使用的编译器设备，以最大程度地解决已知的漏洞。
4.	所有的解决技术，比如地址空间随机化布局（ASLR），数据执行阻止（DEP），哈佛结构和栈检测，帮忙阻止常见的攻击，包括在 B2 和其他相关要求下，测试实验室如何认可这些技术。

	备注：

C.7.11 应用真实性

如终端符合此项，请描述：

1.	设备的哪些组件支持装载应用。
2.	应用真实性校验使用什么算法以及密钥长度。
3.	如果应用真实性校验失败，设备有何反应。
4.	如果应用被拒绝装载，应用如何被删除。
5.	设备的哪些组件支持软件应用/配置的更新。
6.	更新所用机制以及受到影响的设备组件。
7.	软件应用/配置真实性检验使用算法和密钥长度。
8.	软件应用/配置更新的真实性检验失败时，设备有何反应。
9.	如果软件应用/配置更新被拒绝，其如何被删除。
	备注：

C.7.12 应用指引

如终端符合此项，请描述：

1.	提供给软件开发者的指南文档。
	备注：

C.7.13 固件更新

如终端符合此项，请描述：

1.	支持固件或软件更新的设备组件。
2.	初始装载固件所用方法，以及固件更新所用方法。
3.	固件/软件更新时使用的机制，以及受影响的设备组件。

4.	固件/软件真实性校验使用的算法和密钥长度。
5.	生产阶段设备装载的所有公私钥和密钥。
6.	如果固件/软件更新时真实性校验失败，设备有何反应。
7.	如果固件/软件更新时被拒绝，其如何被删除。
	备注：

C.7.14 逻辑异常

如终端符合此项，请描述：

1.	终端提供的所有逻辑和物理接口，以及这些接口是如何被配置以及接受命令的。
2.	设备的源代码所用语言，每个安全处理元件所用操作系统的类型和配置。
3.	所有由软件处理的命令，包括但不限于 SQL 命令和操作系统命令。
4.	哪些命令由受影响的设备组件接受。
5.	这些命令和设备模式是如何对应的。
6.	执行何种类型的参数和数据检查。
7.	为什么功能不会受到逻辑异常的影响。
8.	为确保功能不受逻辑异常影响所做的任何测试。请提供合理解释说明为何这些实验的充分性。
9.	如何阻止账户信息被明文输出。
10.	终端的设计是否允许非固件应用执行。 是 □ 否 □ 由处理器提供给非固件应用执行时所有的固件功能（例如，PIN 输入，密码运算操作和提示控制等等）。
	备注：

C.7.15 开放协议和服务

如终端符合此项，请描述：

1.	C6 部分开放协议特性部分的安全要求是如何满足的。
	备注：

C.7.16 明文数据保护

如终端符合此项，请描述：	
1.	是否存在允许账户信息明文输出的机制。 是 □ 否 □ 如果回答是，请描述这些机制。
2.	允许设备在加密和非加密模式切换的机制。
3.	如何阻止账户信息被明文输出。
4.	设备的哪些组件允许使能和禁用加密功能。
5.	如何保证对尝试初始使能或禁用的实体进行审计。
6.	如何保证使能或禁用尝试的新鲜性和生存期。
7.	远程使能或禁用所使用的加密算法（包括填充机制和运算模式），协议和密钥长度。
8.	对于通过已截短的账号输出信息获取完整的主账号的攻击，设备采用的保护机制（机制提供的保护程度应等价于，仅知道前 6 位和后 4 位数字推断出 16 位的主账号）。
9.	设备装载应用的流程。
10.	如何阻止其他应用访问设备中残留的账户信息。
11.	如何保证加密后账户信息不会以明文方式保存在任何地方。
12.	交易完成后账户明文信息可以存在的最长时间。
13.	在交易中，设备的哪些组件使用了哪些敏感信息（账户信息、密钥）。
14.	交易的结束是如何定义的。
15.	交易完成时设备内部缓存中自动清除的数据。
16.	所有被清除的缓存的位置。

17.	清除缓存的过程。
18.	设备等待持卡人或后台系统的超时时间。
19.	设备超时后的行为。
	备注：

C.7.17 主账号值替代

如终端符合此项，请描述：

1.	主账号替代值如何生成。
2.	证明仅从替代值推断原始主账号不必随机猜测的概率高的测试。
3.	加盐处理时使用的盐值长度。
4.	产生盐值的方法，包括随机数生成方式。
5.	请合理解释，说明为什么必须有至少花费 16 分的潜在攻击（实施阶段至少 8 分）才能侵入设备的硬件或软件从而获取或修改盐值。
	备注：

C.7.18 密钥管理

如终端符合此项，请描述：

1.	关于固定密钥、主密钥或一次一密的 PIN 保护技术。
2.	各密钥是否只用于一个加解密用途？如何确保？
3.	保存密钥时，如何保护其不受非授权的更改和替换？
4.	密钥存储时，如何保证密钥分散管理？
5.	设备实现所有的加密算法。
6.	设备内的所有密钥都应该说明以下信息： •密钥命名： •密钥长度： •相关加密算法： •可能用此密钥加密的数据： •此种密钥的实例和注册数量：

	• PIN 输入设备如何确保该密钥以使其只用于既定目的：
7.	设备是否有擦除密钥的功能？ 是 □ 否 □
8.	哪些密钥可能被擦除？
9.	擦除具体过程。
10.	何种情况下擦除密钥？针对所有设备状态（上电、下电、休眠）进行描述。
11.	其他可能被擦除的数据有哪些？在何种情况下？
12.	哪些密钥不会被擦除？
13.	所有设备中出现的或者使用的密钥如何加载？包括由谁生成以及密钥加载是否以加密形式、或者明文形式、还是以部分加密部分明文的形式。
14.	是否有使用带有公钥的不对称算法替换对称密钥的密钥分配技术，请对以下几点进行描述： •利用随机/伪随机密钥生成过程从而使生成的密钥不可预测或确定其可能密钥空间？随机数的源是否在密钥生成之前就已经过恰当的测试？ •如何做到对公钥的认证？是否有签名分级制度？这些签名（密钥交换签名公钥）如何生成，例如：由谁签名。 •是否有设备双向认证？如果使用签名，那么对签名是如何测试、接受或拒绝的？ •使用的包含对称密钥的信息是否有安全格式和安全防护？接收者是否对信息结构的正确性进行测试？如何保证对原始信息的认证，比如交换信息的签名是否经过测试？
15.	如何保证来源的真实性，例如交换信息的签名是否被校验。 •如果真实性校验失败设备的反应。 •其中使用的加密算法使用的有效的密钥长度。 •选择的密钥长度对于算法和其保护目的是否合适。 是 □ 否 □ •如果使用了 RSA 算法，密钥长度是否至少为 2048 位。 是 □ 否 □
16.	使用的哈希算法和其用途。

17.	密码成分能否被载入？输入密钥时用于加密的算法是什么？
18.	请描述设备中显示或使用的各密钥存储和应用的区域。
19.	请描述 PIN 输入设备所支持的密钥交换技术和存储机制的混合使用。（如 ANSI TR-31）。
20.	设备生成的密钥如何被存储和使用。
21.	设备是否使用了密钥推算的方法？如果使用了，请对方法进行描述。
22.	是否存在密钥为其他密钥的变种。如果是，描述为何变种密钥的保护强度等同或高于原始密钥的保护强度。
	备注：

C.7.19 主账号防穷举

如终端符合此项，请描述：	
1.	设备哪些特性能够防止或有效杜绝窃取设备的使用以保护主账号不被穷举。
	备注：

C.7.20 环境和操作条件改变适应性

如终端符合此项，请描述：	
1.	设备的操作条件和环境条件。
2.	入侵检测单元中包含的所有组件的温度范围。
3.	使用的任何毛刺检测和预防措施。
4.	为何设备的操作条件和环境条件不会危及到设备的安全性。
5.	为确保在操作条件和环境条件改变的情况下设备的安全性所做的测试（请提供测试报告）。
6.	为何这些措施足够且有效。
	备注：

C.7.21 应用隔离

如终端符合此项，请描述：	
1.	设备是否支持多应用。如果支持，请提供支持的应用列表，并标出哪些有安全影响。描述那些有安全影响的应用如何与其他应用隔离。
2.	对于每个安全相关的应用，分类列出数据对象和它们的位置。
3.	设备允许执行非存储于 ROM 中的配置和程序数据（例如处理器，微控制器和 FPGA 等等）的机制。
4.	设备是否依赖于使用不同的处理器提供固件和其他应用的隔离。如果是，描述这些处理器通信的方法，包括所有的物理接口和 API 等。
5.	哪些机制保证了不同应用/固件的代码和数据对象是隔离的。
6.	提供阻止用于存储数据对象的存储器执行的机制。
	备注：

C.7.22 操作系统安全配置

如终端符合此项，请描述：	
1.	设备是否实现了商业操作系统，定制的操作系统或其他机制。如果设备使用了商业操作系统，说明系统的名称和版本。
2.	保证操作系统仅包含制定操作必要的组件和服务的方法。
3.	操作系统维护和更新的流程。
4.	请合理解释为何用于执行最小特权的方法是有效的。
5.	请合理解释为何配置列表中列出的所有组件和服务是必要的。
6.	描述设备强制执行的安全策略，不允许未授权和不必要的功能。
7.	请合理解释为何移除那些未被要求支持特定功能的 API 功能和命令的行为是不可行的。
	备注：

C.7.23 敏感服务保护

如终端符合此项，请描述：

1.	设备具有的敏感功能（敏感功能指并非终端用户可以访问的却能够影响设备安全的功能，如密钥加载，用户角色的定义和维护）。
2.	设备如何控制敏感功能的访问和使用。
3.	用于访问敏感服务的认证方法。
4.	确保进入或退出敏感服务不会泄密或影响敏感信息的措施。
5.	用来认证访问敏感服务的接口。
6.	是否有外部设备用于认证访问敏感服务。
7.	用于访问敏感服务的认证信息，当其在接口处输入/输出时是如何保护的。
8.	下列关于问题 7 中涉及的数据，哪些为真： ☐ 输入数据时，屏幕上显示无法识别的字符 ☐ 无法通过监听声音或电磁辐射识别输入的数据 ☐ 退出安全模式时，内部缓冲区自动清除敏感信息
9.	任何认证数据的管理，认证数据包括口令、密钥和硬件令牌等 ● 共享相同口令和密钥的设备数目： ● 用于认证的可用密码算法： ● 数据长度（密钥或口令的长度）： ● 认证数据如何发送至合法用户： ● 认证数据如何升级：
10.	设备对错误认证数据的反应。
11.	所有用于向设备装载密钥的方法。
12.	使用敏感功能时，操作次数限制是多少。
13.	合理解释为何选择此数目作为限制条件。
14.	使用的操作次数限制如何将未授权用户使用敏感服务的风险最小化。
15.	若操作次数达到限制，设备如何反应。
16.	一旦访问敏感功能，设备保持非活动状态的最长时间。

17.	若非活动状态超时后，设备如何反应。
18.	从设备开始访问敏感功能到其恢复正常模式之前的最长时间。
19.	若到达最长间隔时间，设备如何反应。
	备注：

附 录 D
（规范性附录）被认可算法的最小密钥或等效密钥长度

下面所提到算法的最小密钥长度和运算参数，要求用于密钥的传输，替换或者建立和相关的安全数据保护。其他密钥长度和算法可能支持非支付交易。

算法	DES	RSA	Elliptic Curve	DSA	AES
最小密钥长度 bits	112	2048	224	2048/224	128

密钥加密密钥的安全等级要等于或高于其他密钥强度，以便保护其他密钥。该密钥用于存储、加载和传输其他密钥。以下每一行内的算法和密钥长度被认为是等效的。

算法	DES	RSA	Elliptic Curve	DSA/D-H	AES
最小密钥长度 bits	112	1024	160	1024/160	-
最小密钥长度 bits	168	2048	224	2048/224	-
最小密钥长度 bits	-	3072	256	3072/256	128
最小密钥长度 bits	-	7680	384	7680/384	192
最小密钥长度 bits	-	15360	512	15360/512	256

DES 是指 TDES 密钥没有偶校验位。RSA 密钥的长度指的是模大小。椭圆曲线密钥强度指的是椭圆曲线基点在椭圆曲线阶的最小值，这个阶比域的规模稍小。DSA 密钥大小指的是模大小和一个大子群的最小值。

对于的 Diffie-Hellman 的实现：

实体必须安全地生成和分发规定范围内的参数：发生器 G，素数 P 和参数 Q，大素数因子（P-1），素数 P 必须至少为 2048 位长，参数 Q 必须至少为 224 位长。每个实体都将产生一个私钥 x 和公钥 y 和参数（p,g,q）。每一个私钥都是唯一，不可预知的，需要有文档描述密钥生成过程使用的真随机数发生器。

实体必须验证 Diffie-Hellman 的公钥用作 DSA，证书或者基于对称密码算法计算 MAC(基于 TDES 参照文档 ISO 16609 – Banking –Requirements for message authentication using symmetric techniques; Method 3 should be used)。

终端在支持上述国际通用商用密码基础上，可按国家商用密码管理办公室要求，根据金融密钥体系实际要求，支持 SM2、SM4、SM3 算法，用于数据加密和摘要计算。