Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.3.2—2014

银联卡受理终端安全规范
第 3 卷：检测卷
第 2 部分：产品分类安全检测要求

Security Specifications for Terminal Accepting UnionPay Card
Volume 3: Testing Requirements
Part 2: Testing Requirements for Product 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2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 2 部分：产品分类安全检测要求

1 范围

本部分对受理终端各类产品的安全检测进行说明，与《受理终端安全规范-第2卷：产品卷》（007.2-2014）各部分的安全要求相对应。

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
Q/CUP 007.2 银联卡受理终端安全规范-第2卷：产品卷
Q/CUP 007.4 银联卡受理终端安全规范-第4卷：辅助卷
Q/CUP 056 银联卡支付应用软件安全规范
ANSI X9.19 Financial Institution Retail Message Authentication 金融机构零售业务信息认证
ANSI X9.8 Personal Identification Number (PIN) Management and Security 个人识别码管理和安全
银联风管委【2013】9号 银联卡收单机构账户信息安全管理标准
银联风管委【2006】6号 银联卡账户信息与交易数据安全管理规则
第三方机构接入银联的技术安全要求

3 销售点（POS）终端安全检测

3.1 基础安全要求

检测目的：POS终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求。

对于分体式终端（终端主机与独立密码键盘配合使用），终端主机也应满足第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求。

POS终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第3部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

检测范围：销售点终端。

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。

- 按照《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》第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的检测案例进行测试。
- 按照《银联卡受理终端安全规范-第1卷：基础卷-第3部分：管理安全》的要求设计检测案例进行测试。

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。
- POS终端满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求。
- POS终端满足《银联卡受理终端安全规范-第1卷：基础卷-第3部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

3.2 传输安全要求

检测目的：若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。

检测范围：销售点终端。

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。
- 按照《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》中第8章模块六开放协议的检测案例进行测试。

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。
- 若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。

3.3 账户数据保护要求

检测目的：在设备中传输账户数据（主要指完整磁道信息）时，应满足以下安全要求：——应保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改。攻击总分至少16分，同时攻击阶段分值至少8分。——如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。识别该加密传输涉及的密钥，或者是对所涉及的公钥进行未经授权的修改或替换，均至少需要26分的识别分值和最小13分的攻击阶段分值。

《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护为终端可选模块要求。建议终端支持。

检测范围：销售点终端。

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。
- 按照本项规范要求和《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》中第 9 章模块七账户数据保护的检测案例进行测试。

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。
- 保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改；如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。达到上述内容对应的攻击分值要求。
- 终端对账户数据（包括磁条卡和 IC 卡）的保护满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求（可选）。

3.4 终端管理和应用安全

3.4.1 操作员编号和密码

检测目的：POS 的每个操作员应有独立的编号和密码。操作员编号至少为 2 位数字或字母，密码至少为 4 位数字。POS 终端应具备操作员密码校验功能，校验失败时禁止交易。

检测范围：销售点终端。

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。
- 对操作员独立的编号和密码进行有效性验证。

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。
- POS 的每个操作员具有独立的编号和密码。操作员编号至少为 2 位数字或字母，密码至少为 4 位数字。POS 终端具备操作员密码校验功能，校验失败时禁止交易。

3.4.2 二级密钥体系

3.4.2.1 终端主密钥(TMK)

检测目的：用于对工作密钥(WK)进行加密保护，POS 中心为每台 POS 终端分配唯一的 TMK，TMK 应至少采用双倍长密钥。

检测范围：销售点终端。

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。
- 对终端主密钥功能进行有效性验证。

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。
- TMK 至少采用双倍长密钥。

3.4.2.2 工作密钥（WK）

检测目的：通常用于对个人标识码(PIN)加密的 PIK、进行报文鉴别(MAC)的 MAK、进行磁道加密的 TDK（磁道数据密钥）。

工作密钥（WK）由 POS 前置机的加密机产生，在 POS 终端每次签到时从 POS 中心利用 TMK 加密后下载，并由 TMK 加密存储。

POS 终端工作密钥在下载时必须以密文传送，严禁明文传送。

检测范围：销售点终端。

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。
- 对终端的工作密钥机制进行有效性验证。

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。
- 工作密钥包括对个人标识码(PIN)加密的 PIK、进行报文鉴别(MAC)的 MAK、进行磁道加密的 TDK（磁道数据密钥）。
- 工作密钥（WK）由 POS 前置机的加密机产生，在 POS 终端每次签到时从 POS 中心利用 TMK 加密后下载，并由 TMK 加密存储。
- POS 终端工作密钥在下载时必须以密文传送，严禁明文传送。

3.4.3 加密安全

检测目的：采用安全、可靠的加密算法，保证 POS 交易数据的完整性和隐私性。POS 终端 PIN 加密应至少采用双倍长密钥。

POS 终端应对上送的磁道信息进行加密，加密方式与 POS 中心约定。

检测范围：销售点终端。

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。
- 对加密算法和长度机制进行有效性验证。

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。
- POS 终端 PIN 加密至少采用双倍长密钥。
- 若 POS 终端对上送的磁道信息进行加密，加密方式与 POS 中心约定，加密功能正确实现。
- 应保证终端与后台系统间交互数据的真实性、完整性。

3.5 辅助安全要求

3.5.1 地理位置信息

检测目的：终端宜具备地理位置信息获取和上送能力。

若终端支持该项功能，应满足以下要求：

应对地理位置信息获取和上送的相关软硬件模块进行保护，防止被不正当移除、关闭或破坏；

应对地理位置信息进行有效保护，防止其被篡改。

检测范围：支持地理位置获取和上送能力的销售点终端。

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。
- 结合厂商提交的材料，对地理位置信息获取和上送的相关软硬件模块设计攻击场景。
- 结合厂商提交的材料，验证地理位置信息获取和上送的保护和防篡改机制有效性。

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。
- 对地理位置信息获取和上送的相关软硬件模块进行保护，防止被不正当移除、关闭或破坏；
- 对地理位置信息进行有效保护，防止其被篡改。

3.5.2 防切机转网

检测目的：终端可根据管理机构要求支持防切转网功能，具体参照《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）要求。

检测范围：支持防切机转网功能的销售点终端。

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。
- 对终端防切机转网机制进行有效性验证。

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。
- 终端可根据管理机构要求支持防切转网功能，满足《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）的要求。

4 无人值守（自助）终端安全检测

4.1 基础安全要求

检测目的：自助终端应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。

无人值守（自助）终端《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

检测范围：无人值守（自助）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。
- 按照《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》第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的检测案例进行测试。
- 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》的要求设计检测案例进行测试。

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。
- 自助终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。
- 自助终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

4.2 集成要求

检测目的：自助终端应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 7 章模块五集成安全的要求。

检测范围：无人值守（自助）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。
- 按照《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》中第 7 章模块五集成安全的检测案例进行测试。

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。
- 自助终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 7 章模块五集成安全的要求。

4.3 传输安全要求

检测目的：若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则应满足《银联卡受理终

端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 8 章模块六开放协议的要求。

检测范围：无人值守（自助）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。
- 按照《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》中第 8 章模块六开放协议的检测案例进行测试。

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。
- 若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 8 章模块六开放协议的要求。

4.4 账户数据保护要求

检测目的：在设备中传输账户数据（主要指完整磁道信息）时，应满足以下安全要求：——应保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改。攻击总分至少 16 分，同时攻击阶段分值至少 8 分。——如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。识别该加密传输涉及的密钥，或者是对所涉及的公钥进行未经授权的修改或替换，均至少需要 26 分的识别分值和最小 13 分的攻击阶段分值。《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）

《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护为终端可选模块要求。建议终端支持。

检测范围：无人值守（自助）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。
- 按照本项规范要求和《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》中第 9 章模块七账户数据保护的检测案例进行测试。

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。
- 保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改；如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。达到上述内容对应的攻击分值要求。
- 终端对账户数据（包括磁条卡和 IC 卡）的保护满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求（可选）。

4.5 其他要求

4.5.1 一机一钥

检测目的：无人值守（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。

检测范围：无人值守（自助）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。
- 对“一机一钥”机制进行有效性验证。

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。
- 自助终端的机柜钥匙须一机柜一钥匙，不能多机柜共用一把钥匙。

5 个人支付终端安全检测

5.1 基础安全要求

检测目的：终端应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）检测范围：个人支付终端。

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。

《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》• 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》的要求设计检测案例进行测试。

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。
- 终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）

5.2 账户数据保护

检测目的：终端对账户数据（包括磁条卡和 IC 卡）的保护应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求。

检测范围：无人值守（自助）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。
- 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》的要求设计检测案例进行测试。

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。
- 终端对账户数据（包括磁条卡和 IC 卡）的保护满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求。

5.3 其他要求

5.3.1 物理要求

检测目的：输入 PIN 的模块或 IC 卡读写器应经过合理设计，以保证无法利用在零售市场上可买到的商品组件来组装 PIN 输入设备或 IC 卡读写器。

检测范围：个人支付终端。

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。
• 对独特外观机制进行有效性验证。

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。
• 输入 PIN 的模块或 IC 卡读写器经过合理设计，以保证无法利用在零售市场上可买到的商品组件来组装 PIN 输入设备或 IC 卡读写器。

5.3.2 逻辑要求

5.3.2.1 自检测试

检测目的：终端要实现自检功能，其中包括完整性和真实性测试，包括开机以及每天检查，检测包括固件、表征篡改迹象的安全机制，以及终端是否处于被攻击状态。当自检失败时，终端及其功能可在安全的方式下失效。

检测范围：个人支付终端。

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。
• 对终端自检机制进行有效性验证。

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。
• 终端的自检功能包括完整性和真实性测试，包括开机以及每天检查，检测包括固件、表征篡改迹象的安全机制，以及终端是否处于被攻击状态。当自检失败时，终端及其功能可在安全的方式下失效。

5.3.2.2 固件更新

检测目的：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。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。

检测范围：个人支付终端。

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。
• 对终端固件更新的安全机制进行有效性验证。

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。
• 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或清除设备中所有的密钥。

5.3.2.3 内存清除

检测目的：设备在下面任一情况必须自动清空其内部保存的 PIN 信息：
交易已经从终端正确发出；
PIN 输入后等待持卡人或商户的响应超时。

检测范围：具有输入 PIN 功能的个人支付终端。

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。
• 对终端内存清除进行有效性验证。

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。
• 设备在下面任一情况必须自动清空其内部保存的 PIN 信息：
交易已经从终端正确发出；
PIN 输入后等待持卡人或商户的响应超时。

5.3.2.4 密钥存放管理

检测目的：终端内应有独立的不可读区域，存放终端私钥、终端密钥等代表终端唯一性的重要信息。不应存在机制，允许输出明文私钥、明文密钥或者明文 PIN，或者使用本身可能已经泄露的密钥来加密密钥或 PIN，或者从高安全级组件向低安全级组件传输明文密钥。

检测范围：个人支付终端。

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。
• 对终端密钥存放管理机制进行有效性验证。

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。
• 终端内应有独立的不可读区域，存放终端私钥、终端密钥等代表终端唯一性的重要信息。不应存在机制，允许输出明文私钥、明文密钥或者明文 PIN，或者使用本身可能已经泄露的密钥来加密密钥或 PIN，或者从高安全级组件向低安全级组件传输明文密钥。

5.3.2.5 密钥替换

检测目的：如果终端能够保存多个加密密钥而且能够在外部选择加密 PIN 的密钥，那么终端禁止未经授权的密钥替换和密钥滥用。

检测范围：能保存多个加密密钥而且能够在外部选择加密 PIN 密钥的个人支付终端。

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。
• 对终端密钥替换进行有效性验证。

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。
• 终端禁止未经授权的密钥替换和密钥滥用。

5.3.2.6 合法性认证

检测目的：个人支付终端首次使用时应与持卡人进行有效身份绑定，每次应用之前需与后台进行合法性认证。

检测范围：个人支付终端。

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。
• 对终端合法性认证进行有效性验证。

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。
• 首次使用时终端与持卡人进行有效身份绑定，每次应用之前与后台进行合法性认证。

5.3.2.7 PIN 加密

检测目的：在个人终端使用过程中应保证 PIN 的密文传输：
对于 PIN 的输入，如通过终端设备输入，应在终端设备加密，加密算法可采用对称加密算

法或非对称加密算法。对称加密算法应保证加密密钥一机一密，且密钥应保存在终端设备的安全芯片或处理器的安全区域中；采用非对称加密算法，应保证公钥不能被随意读取、更改、破坏，私钥应统一管理和分发，并确保私钥在服务器的安全存储。

如 PIN 通过手机、PC 机等主机设备进行输入，需采取技术措施防止密码盗取，技术手段可包括但不限于以下方式。对于反复尝试并输入错误密码超过一定次数的，进行软件登录和支付交易控制，必要时可根据业务规则予以交易阻断。

- 所有用户输入的客户端登录密码、银行卡密码等敏感信息不得在界面上显示明文；
- 密码等敏感信息采用软键盘方式输入；
- 敏感信息输入后需要立即采用健壮的算法加密。

检测范围：具有输入 PIN 功能的个人支付终端。

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。
- 对终端PIN加密进行有效性验证。

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。
- 如通过终端设备输入，PIN 的输入在终端设备加密，加密算法采用对称加密算法或非对称加密算法。对称加密算法保证加密密钥一机一密，且密钥应保存在终端设备的安全芯片或处理器的安全区域中；采用非对称加密算法，公钥不能被随意读取、更改、破坏，私钥应统一管理和分发，并确保私钥在服务器的安全存储。
- 如 PIN 通过手机、PC 机等主机设备进行输入，须采取技术措施防止密码盗取。对于反复尝试并输入错误密码超过一定次数的，进行软件登录和支付交易控制，必要时可根据业务规则予以交易阻断。

5.3.2.8 账户信息保护

检测目的：终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡数据、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。

磁道信息应由个人支付终端设备读取并在终端内完成加密，不允许以全明文形式出现在个人终端、手机、PC 内存、客户端等交易通信过程中。

对磁道进行加密的算法可采用对称加密算法和非对称加密算法。采用对称加密算法应保证加密密钥仅由本终端使用，且存储于安全芯片或处理器的安全区域中；采用非对称加密算法应保证公钥不能被随意读取、更改、破坏，私钥应统一管理和分发，并确保私钥在服务器的安全存储。

如业务涉及卡号显示，须进行屏蔽保护，卡号的前六位和后四位正常显示，其余卡号位进行‘*’屏蔽。

检测范围：个人支付终端。

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。
- 对终端账户信息保护机制进行有效性验证。

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。
- 终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡数据、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。
- 磁道信息应由个人支付终端设备读取并在终端内完成加密，不允许以全明文形式出现在个

人终端、手机、PC 内存、客户端等交易通信过程中。

- 对磁道采用对称加密算法保证加密密钥仅由本终端使用，且存储于安全芯片或处理器的安全区域中；采用非对称加密算法保证公钥不能被随意读取、更改、破坏，私钥统一管理和分发，并确保私钥在服务器的安全存储。
- 如业务涉及卡号显示，须进行屏蔽保护，卡号的前六位和后四位正常显示，其余卡号位进行‘*’屏蔽。

5.3.2.9 报文的完整性要求

检测目的：应保证交易报文在通信过程中的完整性。防止交易报文中涉及的交易金额、交易日期、订单号等重要信息在交易过程中被非法篡改。

检测范围：个人支付终端。

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。
- 对终端报文完整性保护机制进行有效性验证。

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。
- 应保证交易报文在通信过程中的完整性。防止交易报文中涉及的交易金额、交易日期、订单号等重要信息在交易过程中被非法篡改。

5.3.2.10 远程控制

检测目的：终端应具备防远程控制安全机制，防止非法利用木马等病毒远程控制设备，进行非法交易。

检测范围：个人支付终端。

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。
- 对终端远程控制机制进行有效性验证。

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。
- 终端须具备防远程控制安全机制，防止非法利用木马等病毒远程控制设备，进行非法交易。

5.4 辅助安全要求

5.4.1 对应支付应用软件要求

检测目的：装载于手机、PC 等设备，与受理终端配合使用的应用软件应满足《银联卡支付应用软件安全规范》（Q/CUP 056）要求。

检测范围：装有支付应用软件的个人支付终端。

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。
- 对终端支付应用软件进行安全有效性验证。

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。
- 装载于手机、PC 等设备，与受理终端配合使用的应用软件满足《银联卡支付应用软件安全规范》（Q/CUP 056）要求。

5.4.2 后台系统控制

检测目的：个人支付终端的使用前，应向业务后台系统提交终端信息，由业务后台系统完成对终端的认

证。持卡人在终端上录入或由终端读取银行卡信息，供后台系统对终端和卡片进行关联，并在支付过程中控制终端可使用卡片的数量，以保证个人终端设备的个人使用。

检测范围：个人支付终端。

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。
- 对终端与后台系统认证机制进行安全有效性验证。

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。
- 终端的使用前须向业务后台系统提交终端信息，由业务后台系统完成对终端的认证。持卡人在终端上录入或由终端读取银行卡信息，供后台系统对终端和卡片进行关联，并在支付过程中控制终端可使用卡片的数量，以保证个人终端设备的个人使用。

6 独立部件安全检测

6.1 密码键盘

检测目的：密码键盘应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。

密码键盘应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

检测范围：可作为独立部件装配到其他终端中的密码键盘，实现 PIN 输入安全功能的设备，包括 POS 主机等设备的外接密码键盘和无人值守（自助）终端的加密 PIN 键盘（EPP）。

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。
- 按照《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》第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的检测案例进行测试。
- 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》的要求设计检测案例进行测试。

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。
- 密码键盘满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。
- 密码键盘满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

6.2 读卡器

检测目的：读卡器应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求。

读卡器应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

检测范围：可作为独立部件装配到其他终端（例如无人值守的（自助）终端等）中，实现银行卡数据安

全读取功能的设备，包括 IC 卡读卡器和磁条卡读卡器。与移动电话、个人电脑、平板电脑等设备及其装载的应用程序相配合，实现个人支付功能的读卡终端设备，不包含在本部分范围内。

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。
- 按照《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》第 9 章模块七账户数据保护的检测案例进行测试。
- 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》的要求设计检测案例进行测试。

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。
- 读卡器满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求。
- 读卡器满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

7 电话终端安全检测

7.1 电话终端 I 型

7.1.1 密钥体系和加密模块

检测目的：签到密钥模式分为二级密钥：密钥加密密钥（KEK）和工作密钥（WK）。其中 KEK 又称终端主密钥，用于对工作密钥进行加密保护。

终端主密钥存放于 TSAM 卡中，不同 TSAM 卡应注入不同的终端主密钥，实现“一机一密”要求。电话终端 I 型由 TSAM 卡实现对磁道信息和 PIN 的加密，实现报文 MAC 计算。

检测范围：I 型电话终端。

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。
- 对终端密钥体系和加密模块机制进行有效性验证。

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。
- 签到密钥模式分为二级密钥：密钥加密密钥（KEK）和工作密钥（WK）。其中 KEK 又称终端主密钥，用于对工作密钥进行加密保护。
- 电话终端 I 型由 TSAM 卡实现对磁道信息和 PIN 的加密，实现报文 MAC 计算。
- 终端主密钥存放于 TSAM 卡中，不同 TSAM 卡应注入不同的终端主密钥，实现“一机一密”要求。

7.1.2 工作密钥生成

检测目的：工作密钥包括 PIN 加密密钥 PIK、磁道加密密钥 TDK 和 MAC 计算密钥 MAK。使用主密钥产生工作密钥的过程如下：
- TSAM 卡产生一个 4 字节的随机数；
- TSAM 卡提取随机数序号（4 字节，以 16 进制表示），该序号在 TSAM 上每操作一次后自动加 1；
- TSAM 卡将序号和随机数合并成 8 字节的计算因子（前 4 字节为序号、后 4 字节为随机数）；

- 用主密钥对计算因子做 3DES 运算获得工作密钥。

检测范围：I 型电话终端。

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。
- 对终端工作密钥生成机制进行有效性验证。

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。
- 工作密钥包括 PIN 加密密钥 PIK、磁道加密密钥 TDK 和 MAC 计算密钥 MAK。
- 使用主密钥产生工作密钥的过程如下：

  1、TSAM 卡产生一个 4 字节的随机数；

  2、TSAM 卡提取随机数序号（4 字节，以 16 进制表示），该序号在 TSAM 上每操作一次后自动加 1；

  4、TSAM 卡将序号和随机数合并成 8 字节的计算因子（前 4 字节为序号、后 4 字节为随机数）；

  5、用主密钥对计算因子做 3DES 运算获得工作密钥。

7.1.3 传输安全要求

检测目的：若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。

检测范围：I型电话终端。

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。
- 按照《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》第8章模块六开放协议的要求进行测试。

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。
- 电话终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。

7.1.4 其他要求

7.1.4.1 PIN 和磁道加密

检测目的：PIN 加密算法使用双倍长密钥算法进行加密，PIN 加密必须使用 3DES 算法。

检测范围：I 型电话终端。

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。
- 对终端PIN和磁道数据加密功能进行有效性验证。

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。
- PIN加密算法使用双倍长密钥算法进行加密，PIN加密必须使用3DES算法。

7.1.4.2 MAC 计算

检测目的：从报文类型到有效数据域之间的部分构成 MAC ELEMEMENT BLOCK（MAB），MAC 的加密算法不强制要求，建议采用 ANSI 9.19 算法，详细算法见《中国银联电话支付终端应用规范》附录 E。

检测范围：I 型电话终端。

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。
- 对终端MAC计算功能进行有效性验证。

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。
- 若计算 MAC 采用 ANSI 9.19 算法，符合《中国银联电话支付终端应用规范》附录 E。

7.1.4.3 账户信息

检测目的：电话支付终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡磁道信息、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。
电话支付终端应确保本规范所涉及键盘输入信息的安全，禁止通过重拨等功能获取相关资料。

检测范围：I 型电话终端。

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。
- 对账户信息保护功能进行有效性验证。

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。
- 电话支付终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡磁道信息、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。
- 终端确保键盘输入信息的安全，禁止通过重拨等功能获取相关资料。

7.1.4.4 终端关联

检测目的：电话支付终端建立终端序列号（也称终端编号）、安全加密模块号（I型为TSAM卡号）、电话号码（或IMSI号码）三者的关联，对于三者中关联有一个不匹配的，电话支付中心应拒绝该终端发起的所有交易请求。

检测范围：I型电话终端。

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。
- 对终端关联验证有效性。

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。
- 终端编号、TSAM卡号、IMSI号码三者的关联，对于三者中关联有一个不匹配的，电话支付中心应拒绝该终端发起的所有交易请求。

7.2 电话终端 II 型

7.2.1 基础安全要求

检测目的：电话终端II型应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求。

对于分体式终端（终端主机与独立密码键盘配合使用），在无其他功能要求和说明的情况下，终端主机亦可参照第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求以提升主机安全性。

终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第3部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

检测范围：II 型电话终端。

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。
- 按照《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》第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的检测案例进行测试。
- 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》的要求设计检测案例进行测试。

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。
- 电话终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 1 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。
- 电话终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

7.2.2 传输安全要求

检测目的：若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。

检测范围：II型电话终端。

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。
- 按照《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》第8章模块六开放协议的要求进行测试。

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。
- 电话终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。

7.2.3 账户数据保护要求

检测目的：在设备中传输账户数据（主要指完整磁道信息）时，应满足以下安全要求：——应保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改。攻击总分至少16分，同时攻击阶段分值至少8分。——如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。识别该加密传输涉及的密钥，或者是对所涉及的公钥进行未经授权的修改或替换，均至少需要26分的识别分值和最小13分的攻击阶段分值。《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）

《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中

第9章模块七账户数据保护为终端可选模块要求。建议终端支持。

检测范围： II 型电话终端。

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。
- 试用情况见检测目的。
- 按照本项规范要求和《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》中第 9 章模块七账户数据保护的要求进行测试。

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。
- 保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改；如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。达到上述内容对应的攻击分值要求。
- 电话终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第9章模块七账户数据保护的要求（可选）。

7.2.4 其他要求

7.2.4.1 密钥体系

检测目的：签到密钥模式分为二级密钥：密钥加密密钥（KEK）和工作密钥（WK）。其中KEK又称终端主密钥，用于对工作密钥进行加密保护，每台电话支付终端与电话支付中心共享唯一的主密钥。终端主密钥必须有安全保护措施，智能写入并参与运算，不能被读取。终端主密钥应具有唯一性，即不同电话支付终端应设置不同的终端主密钥，实现“一机一密”。工作密钥包括PIN加密密钥PIK、磁道加密密钥TDK和MAC计算密钥MAK。工作密钥由电话支付中心加密机产生，电话支付终端每次签到时从电话支付中心利用KEK加密后下载，并由KEK加密存储，严禁明文传送。每次签到更新不同的工作密钥对PIN、磁道信息等交易敏感信息进行加密。

检测范围：II型电话终端。

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。
- 对终端密钥体系进行有效性验证。

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。
- 签到密钥模式分为二级密钥：密钥加密密钥（KEK）和工作密钥（WK）。其中 KEK 又称终端主密钥，用于对工作密钥进行加密保护，每台电话支付终端与电话支付中心共享唯一的主密钥。终端主密钥必须有安全保护措施，智能写入并参与运算，不能被读取。
- 终端主密钥应具有唯一性，即不同电话支付终端应设置不同的终端主密钥，实现“一机一密”。工作密钥包括 PIN 加密密钥 PIK、磁道加密密钥 TDK 和 MAC 计算密钥 MAK。工作密钥由电话支付中心加密机产生，电话支付终端每次签到时从电话支付中心利用 KEK 加密后下载，并由 KEK 加密存储，严禁明文传送。每次签到更新不同的工作密钥对 PIN、磁道信息等交易敏感信息进行加密。

7.2.4.2 MAC 计算

检测目的：从报文类型到有效数据域之间的部分构成MAC ELEMEMENT BLOCK（MAB），MAC的加密算法不强制要求，建议采用ANSI 9.19算法，详细算法见《中国银联电话支付终端应用规范》附录E。

检测范围：II型电话终端。

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。
- 对终端MAC计算功能进行有效性验证。

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。
- 从报文类型到有效数据域之间的部分构成 MAC ELEMEMENT BLOCK（MAB），MAC 的加密算法不强制要求，建议采用 ANSI 9.19 算法，详细算法见《中国银联电话支付终端应用规范》附录 E。

7.2.4.3 PIN 加密

检测目的：PIN加密采用ANSI X9.8 Format（带主账号信息）算法进行格式化，再使用双倍长密钥算法进行加密。电话支付终端要支持以上两种算法。具体的方法见《中国银联电话支付终端应用规范》附录C。PIN加密必须使用3DES算法。

检测范围：II型电话终端。

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。
- 对终端PIN加密功能进行有效性验证。

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。
- PIN 加密采用 ANSI X9.8 Format（带主账号信息）算法进行格式化，再使用双倍长密钥算法进行加密。电话支付终端要支持以上两种算法。具体的方法见《中国银联电话支付终端应用规范》附录 C。PIN 加密必须使用 3DES 算法。

7.2.4.4 磁道处理

检测目的：对于磁道信息，应将二磁道信息和三磁道信息（如果存在）合并，并采用TDK进行加密，相关算法详见《中国银联电话支付终端应用规范》附录D。

检测范围：II型电话终端。

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。
- 验证磁道处理有效性。

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。
- 若处理磁道信息，符合《中国银联电话支付终端应用规范》附录D。

7.2.4.5 账户信息

检测目的：电话支付终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡磁道信息、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。

电话支付终端应确保本规范所涉及键盘输入信息的安全，禁止通过重拨等功能获取相关资料。

检测范围：II型电话终端。

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。

- 验证话支付终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡磁道信息、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。
- 验证电话支付终端，确保本规范所涉及键盘输入信息的安全，禁止通过重拨等功能获取相关资料。

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。
- 电话支付终端只能在交易存储转发及冲正处理过程中保存必需的最基本的账户信息，不得存储银行卡磁道信息、卡片验证码、个人标识代码（PIN）及卡片有效期等敏感信息。
- 电话支付终端确保本规范所涉及键盘输入信息的安全，禁止通过重拨等功能获取相关资料。

7.2.4.6 终端关联

检测目的：电话支付终端应建立终端编号、安全加密模块号（II型为密码键盘序列号）、电话号码（或IMSI号码）三者的关联，对于三者中关联有一个不匹配的，电话支付中心应拒绝该终端发起的所有交易请求。

检测范围：II型电话终端。

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。
- 对终端关联验证有效性。

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。
- 终端编号、密码键盘序列号、IMSI号码三者的关联，对于三者中关联有一个不匹配的，电话支付中心应拒绝该终端发起的所有交易请求。

7.3 辅助安全要求

7.3.1 地理位置信息

检测目的：终端宜具备地理位置信息获取和上送能力。

若终端支持该项功能，应满足以下要求：

——应对地理位置信息获取和上送的相关软硬件模块进行保护，防止被不正当移除、关闭或破坏；

——应对地理位置信息进行有效保护，防止其被篡改。

检测范围：II型电话终端。

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。
- 检测终端获取地理位置信息和上送。
- 检查硬软件对获取和上送信息的防护。

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。
- 对地理位置信息获取和上送的相关软硬件模块进行保护，防止被不正当移除、关闭或破坏。
- 对地理位置信息进行有效保护，防止其被篡改。
- 终端宜具备地理位置信息获取和上送能力。

7.3.2 防切机转网

检测目的：终端可根据管理机构要求支持防切转网功能，具体参照《银联卡受理终端安全规范-第4卷：

辅助卷-第1部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）要求。

检测范围：II型电话终端。

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。
• 验证终端可根据管理机构要求支持防切转网功能。

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。
• 应符合《银联卡受理终端安全规范-第4卷：辅助卷-第1部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）要求

8 智能终端安全检测

8.1 基础安全要求

检测目的：智能终端应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。

对于分体式终端（终端主机与独立密码键盘配合使用），在无其他功能要求和说明的情况下，终端主机亦可参照第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求以提升主机安全性

智能终端应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

检测范围：智能终端。

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。
• 按照《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》的要求设计检测案例进行测试。
• 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求设计检测案例进行测试。

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。
• 终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。
• 终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。

8.2 传输安全要求

检测目的：若智能终端利用开放安全协议和传输协议通过公共网络进行数据传输，则应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 8 章模块六开放协议的要求。

检测范围：智能终端。

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。
- 按照《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》中第 8 章模块六开放协议的检测案例进行测试。

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。
- 若终端利用开放安全协议和传输协议通过公共网络进行数据传输，则满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 8 章模块六开放协议的要求。

8.3 账户数据保护要求

检测目的：在设备中传输账户数据（主要指完整磁道信息）时，应满足以下安全要求：——应保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改。攻击总分至少 16 分，同时攻击阶段分值至少 8 分。——如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。识别该加密传输涉及的密钥，或者是对所涉及的公钥进行未经授权的修改或替换，均至少需要 26 分的识别分值和最小 13 分的攻击阶段分值。《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）

《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护为终端可选模块要求。建议终端支持。

检测范围：智能终端。

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。
- 按照本项规范要求和《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》的要求设计检测案例进行测试。

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。
- 保证账户数据在从读卡器获取到进入最终加密设备完成加密运算的整个过程中不被泄露或篡改；如果最终的账户数据加密设备和读卡器不是一体的，或两者是一体的但传输线路不在保护区域内，则数据必须通过加密传输。达到上述内容对应的攻击分值要求。
- 终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求。

8.4 其他要求

8.4.1 操作系统安全

8.4.1.1 系统内核加载安全

检测目的：终端应保证操作系统内核加载安全，以防止非法厂商在终端上运行自身定制、不符合本安全标准的操作系统，具体要求包括但不限于：

应保证操作系统内核加载过程的安全，应保证用于系统内核加载的相关模块在终端出厂后不能被篡改。

操作系统内核受管理方（银行卡组织及其授权机构，或其他智能终端系统管理运营方及其授权机构）应对操作系统内核进行签名，终端应防止未被签名的内核运行。

检测范围：智能终端。

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。
- 对系统内核加载安全进行有效性验证。

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。
- 终端应保证操作系统内核加载安全，以防止非法厂商在终端上运行自身定制、不符合本安全标准的操作系统。
- 保证操作系统内核加载过程的安全，保证用于系统内核加载的相关模块在终端出厂后不能被篡改。
- 操作系统内核受管理方（银行卡组织及其授权机构，或其他智能终端系统管理运营方及其授权机构）对操作系统内核进行签名，终端防止未被签名的内核运行。

8.4.1.2 系统更新与升级安全

检测目的：终端应防止用户非法刷机及非法升级。如果系统存在更新或升级需求，应在安全环境下由终端管理机构或其授权机构进行更新或升级。

检测范围：智能终端。

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。
- 对系统更新与升级安全进行有效性验证。

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。
- 终端应防止用户非法刷机及非法升级。如果系统存在更新或升级需求，应在安全环境下由终端管理机构或其授权机构进行更新或升级。

8.4.1.3 资源访问权限控制

检测目的：操作系统应控制应用软件对设备资源的访问权限，包括对系统自身资源的访问和对外部设备的访问。

系统自身资源的访问权限由操作系统通用配置功能完成。

应用软件对外部设备资源的访问权限控制，通过定制操作系统实现。需设置权限控制的资源包括但不限于：

——磁条卡读卡器访问权限

——接触式 IC 卡读卡器访问权限

——非接 IC 卡读卡器访问权限

——证书管理与加密运算模块（安全模块）访问权限（安全模块功能见《银联卡受理终端安全规范-第 1 卷：基础卷-第 4 部分：硬件要求-20140725》）

——打印机访问权限

——密码键盘访问权限

——如存在电子签名设备、扫描设备等外设，应设置相应访问权限

以上资源访问权限均仅授予银联卡支付应用软件及经智能终端及支付系统管理方（银行卡组织及其授权机构、或其他系统管理运营方及其授权机构）认可的特定第三方行业应用软件，且对各资源的授权互相独立，访问权限应分别管理和授予。

检测范围：智能终端。

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。
- 对资源访问权限控制进行有效性验证。

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。
• 操作系统应控制应用软件对设备资源的访问权限，包括对系统自身资源的访问和对外部设备的访问。
• 系统自身资源的访问权限由操作系统通用配置功能完成。。
• 应用软件对外部设备资源的访问权限控制，通过定制操作系统实现。
• 需设置权限控制的资源包括但不限于：
——磁条卡读卡器访问权限
——接触式 IC 卡读卡器访问权限
——非接 IC 卡读卡器访问权限
——证书管理与加密运算模块（安全模块）访问权限（安全模块功能见《银联卡受理终端安全规范-第 1 卷：基础卷-第 4 部分：硬件要求-20140725》）
——打印机访问权限
——密码键盘访问权限
——如存在电子签名设备、扫描设备等外设，应设置相应访问权限
以上资源访问权限均仅授予银联卡支付应用软件及经智能终端及支付系统管理方（银行卡组织及其授权机构、或其他系统管理运营方及其授权机构）认可的特定第三方行业应用软件，且对各资源的授权互相独立，访问权限分别管理和授予。

8.4.1.4 应用间数据交换

检测目的：运行于智能终端系统上的多个应用间可以以进程间通信的方式交换数据，如 IPC 的方式等。进程间的通信必须保证的数据的安全，防止被其它非法授权的应用窥探。若应用程序需调用其他程序或者系统中的一些敏感程序的组件，应通过设置权限的方式保证系统和应用程序的安全。

检测范围：智能终端。

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。
• 对应用间数据交换进行有效性验证。

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。
• 运行于智能终端系统上的多个应用间可以以进程间通信的方式交换数据，如 IPC 的方式等。进程间的通信必须保证的数据的安全，防止被其它非法授权的应用窥探。
• 若应用程序需调用其他程序或者系统中的一些敏感程序的组件，通过设置权限的方式保证系统和应用程序的安全。

8.4.1.5 应用软件管理

检测目的：终端应提供应用软件安全下载、安装和更新的管理能力，应用安装权限应授予专用应用管理客户端，应用软件及相关补丁应通过银行卡组织或其他智能终端系统管理运营方管理或由其授权管理的合法渠道下载。
智能终端应用管理客户端具有安装应用的唯一权限，应用的安装应通过智能终端应用管理客户端并连接应用管理后台系统进行。应通过数字签名等技术手段，使下列应用不能够在终端上安装使用：
从其他第三方行业应用下载的应用程序；
通过 Micro-SD 卡或者其他 USB 接口设备拷入的应用程序；
其他非智能终端应用管理客户端途径获得的应用。

在软件安装或更新过程中，应确保所安装或更新的应用软件版本有效，安装或更新过程应在安装包完整、安全的前提下进行。空中方式下载安装或更新客户端支付软件时需要采用安全报文，保证软件传输过程的机密性、完整性。

应用安装程序应通过智能终端应用管理后台进行签名，应用安装前，安装文件应首先通过智能终端的签名验证。

检测范围：智能终端。

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。
- 对应用软件管理进行有效性验证。

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。
- 终端应提供应用软件安全下载、安装和更新的管理能力，应用安装权限应授予专用应用管理客户端，应用软件及相关补丁应通过银行卡组织或其他智能终端系统管理运营方管理或由其授权管理的合法渠道下载。
- 智能终端应用管理客户端具有安装应用的唯一权限，应用的安装应通过智能终端应用管理客户端并连接应用管理后台系统进行。应通过数字签名等技术手段，使下列应用不能够在终端上安装使用：
- 从其他第三方行业应用下载的应用程序；
- 通过 Micro-SD 卡或者其他 USB 接口设备拷入的应用程序；
- 其他非智能终端应用管理客户端途径获得的应用。
- 在软件安装或更新过程中，应确保所安装或更新的应用软件版本有效，安装或更新过程应在：安装包完整、安全的前提下进行。空中方式下载安装或更新客户端支付软件时需要采用安全报文，保证软件传输过程的机密性、完整性：
- 应用安装程序应通过智能终端应用管理后台进行签名，应用安装前，安装文件应首先通过智能终端的签名验证。

8.4.2 证书管理与加密运算模块安全

检测目的：证书管理与加密运算模块应具备的硬件安全功能包括但不限于：

——应提供对称和非对称等通用密码算法的专用计算功能；

——应提供随机数发生功能，以产生随机数辅助证书管理与加密运算模块实现其安全应用，如产生的随机数与敏感信息有关或与智能终端后台系统安全验证有关，则该随机数生成功能

——应经过评估，以保证产生的随机数无法被预测；

——应具备硬件防攻击机制，保障证书管理与加密运算模块在受到攻击后立即出于不可操作状态，并立即擦除模块中存放的私密信息；

——应具备异常处理机制，包括但不限于：

1、应具备环境异常检测处理机制，包括但不限于温度、电压、时钟频率等检测处理机制；

2、应具备程序执行异常检测处理机制；

3、应具备逻辑模块异常检测处理机制，例如算法模块溢出、寻址空间越界等异常的检测及处理机制；

证书管理与加密运算模块应提供相应的访问控制策略，对模块的访问应遵循该机制，以防止对模块的非法越权操作；

应具备相应删除机制，保证敏感数据在使用后立即从存储区域中删除；

改变设备环境条件或操作条件不会影响证书管理与加密运算模块安全性。

检测范围：智能终端。

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。
• 对证书管理与加密运算模块安全进行有效性验证。

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。
• 证书管理与加密运算模块应具备的硬件安全功能包括但不限于：
——应提供对称和非对称等通用密码算法的专用计算功能；
——应提供随机数发生功能，以产生随机数辅助证书管理与加密运算模块实现其安全应用，如产生的随机数与敏感信息有关或与智能终端后台系统安全验证有关，则该随机数生成功能应经过评估，以保证产生的随机数无法被预测；
——应具备硬件防攻击机制，保障证书管理与加密运算模块在受到攻击后立即出于不可操作状态，并立即擦除模块中存放的私密信息；
——应具备异常处理机制，包括但不限于：
1、应具备环境异常检测处理机制，包括但不限于温度、电压、时钟频率等检测处理机制；
2、应具备程序执行异常检测处理机制；
3、应具备逻辑模块异常检测处理机制，例如算法模块溢出、寻址空间越界等异常的检测及处理机制；
——证书管理与加密运算模块应提供相应的访问控制策略，对模块的访问应遵循该机制，以防止对模块的非法越权操作；
——应具备相应删除机制，保证敏感数据在使用后立即从存储区域中删除；
——改变设备环境条件或操作条件不会影响证书管理与加密运算模块安全性。

8.5 辅助安全要求

8.5.1 地理位置信息

检测目的：终端宜具备地理位置信息获取和上送能力。
若终端支持该项功能，应满足以下要求：
——应对地理位置信息获取和上送的相关软硬件模块进行保护，防止被不正当移除、关闭或破坏；
——应对地理位置信息进行有效保护，防止其被篡改。

检测范围：智能终端。

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。
• 对地理位置信息进行有效性验证。

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。
• 若终端支持该项功能，满足以下要求：
——对地理位置信息获取和上送的相关软硬件模块进行保护，防止被不正当移除、关闭或破坏；
——对地理位置信息进行有效保护，防止其被篡改。

8.5.2 防切机转网

检测目的：终端可根据管理机构要求支持防切转网功能，具体参照《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）要求。

检测范围：智能终端。

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。
- 按照《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）要求设计检测案例进行测试。

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。
- 终端可根据管理机构要求支持防切转网功能，满足《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）的要求。

8.5.3 应用软件安全

检测目的：智能设备上安装和使用的支付应用软件应满足《银联卡支付应用软件安全规范》（Q/CUP 056），具体依据相应安全认证规则操作。

支付应用软件与后台系统间应采用双向认证保证传输线路安全，且所使用的证书和密钥应存储于证书管理与加密运算模块中。

非支付应用软件建议参照上述规范要求进行开发、维护和管理。

检测范围：智能终端。

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。
- 按照《银联卡支付应用软件安全规范》（Q/CUP 056）的要求设计检测案例进行测试。

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。
- 终端满足《银联卡支付应用软件安全规范》（Q/CUP 056）的安全要求。

9 mPOS 通用技术安全检测

9.1 安全目标

9.1.1 账户信息安全保护

检测目的：受理终端应对账户信息进行安全保护。账户信息保护要求参见《银联卡收单机构账户信息安全管理标准》（银联风管委【2013】9号）和《银联卡账户信息与交易数据安全管理规则》（银联风管委【2006】6号）。其中，完整磁道信息、PIN、卡片验证码、卡片有效期等敏感数据应被安全加密和解密，在受理终端和后台系统的硬件加密模块之外不得以明文形式出现，终端不应输出完整的主账号（卡号）信息，应保证数据在处理和传输过程中不被泄露、窃取和篡改。任何设备和系统均不得存储敏感数据（即使已经加密），账户信息只用于完成当前合法银联卡交易，不得用于任何其他用途。

检测范围：mPOS

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。
- 对账户信息保护的有效性进行验证

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。
- 账户信息保护要求必须符合《银联卡收单机构账户信息安全管理标准》（银联风管委【2013】9 号）和《银联卡账户信息与交易数据安全管理规则》（银联风管委【2006】6 号）标准的

要求。

- 其中，完整磁道信息、PIN、卡片验证码、卡片有效期等敏感数据必须被安全加密和解密，在受理终端和后台系统的硬件加密模块之外不得以明文形式出现，终端不应输出完整的主账号（卡号）信息，必须保证数据在处理和传输过程中不被泄露、窃取和篡改。
- 任何设备和系统均不得存储敏感数据（即使已经加密），账户信息只用于完成当前合法银联卡交易，不得用于任何其他用途。

9.1.2 交易信息安全保护

检测目的：除卡号、PIN、磁道信息、有效期、卡片验证码等交易信息（参见银联风管委【2013】9号和【2006】6号相关风险要求）之外，还应保证交易金额、交易类型、货币类型、商户号、终端号等关键交易信息在处理和传输过程中不被篡改。

检测范围：mPOS

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。
- 对交易信息安全保护的有效性进行验证

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。
- 必须保证交易金额、交易类型、货币类型、商户号、终端号等关键交易信息在处理和传输过程中不被篡改。

9.1.3 安全提示

检测目的：终端应提供相关机制，确保交易过程中流程关键环节（如：交易金额及交易类型确认，密码输入等）和交易结果能安全、有效地向持卡人和收银员进行强制提示，确认后才可进行下一步操作。

检测范围：mPOS

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。
- 对安全提示的有效性进行验证

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。
- 终端必须提供相关机制，确保交易过程中流程关键环节（如：交易金额及交易类型确认，密码输入等）和交易结果能安全、有效地向持卡人和收银员进行强制提示，确认后才可进行下一步操作。

9.1.4 交易真实性

检测目的：对交易报文的来源进行鉴别，保证交易真实性，防止信息伪造和重放攻击。

检测范围：mPOS

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。
- 对交易真实性进行验证

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。
- 对交易报文的来源进行鉴别，必须保证交易真实性，防止信息伪造和重放攻击。

9.2 受理终端安全要求

9.2.1 基础安全要求

检测目的：受理终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第3章模块一物理安全、第4章模块二逻辑安全、第5章模块三联机PIN安全、第6章模块四脱机PIN安全的要求。受理终端应满足《银联卡受理终端安全规范-第1卷：基础卷-第3部分：管理安全》（Q/CUP 007.1.3-2014）的要求。受理终端宜实现DUKPT或等效的一次一密机制，建议实施标准DUKPT机制。

检测范围：mPOS受理终端

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。
- 按照《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》（Q/CUP 007.3.1-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的检测案例进行测试。
- 按照《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的检测案例进行测试。

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。
- 受理终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 3 章模块一物理安全、第 4 章模块二逻辑安全、第 5 章模块三联机 PIN 安全、第 6 章模块四脱机 PIN 安全的要求。
- 受理终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 3 部分：管理安全》（Q/CUP 007.1.3-2014）的要求。
- 如果终端支持 DUKPT 或等效的一次一密机制，对其机制进行检查。

9.2.2 终端功能限制

检测目的：受理终端不应向上位机提供单独、直接的PIN和磁道等敏感数据加密计算功能，防止被用于伪造交易、密钥穷举破解等。若受理终端向上位机提供MAC计算功能，则应对交易金额等4.3节所述交易信息进行强制校验或填充，防止交易信息被篡改后骗取合法MAC。

检测范围：mPOS受理终端

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。
- 对终端功能限制进行有效性验证。

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。
- 受理终端不能向上位机提供单独、直接的 PIN 和磁道等敏感数据加密计算功能
- 如果受理终端支持向上位机提供 MAC 计算功能，则必须对交易金额等 4.3 节所述交易信息进行强制校验或填充，防止交易信息被篡改后骗取合法 MAC。

9.2.3 传输安全要求

检测目的：若受理终端使用开放安全协议和传输协议通过公共网络进行数据传输，则应满足《银联卡受理终端安全规范-第1卷：基础卷-第2部分：设备安全》（Q/CUP 007.1.2-2014）中第8章模块六开放协议的要求。受理终端应保证能有效鉴别后台发送数据的真实性、完整性。终端输出数据的保护见账户信息保护和交易信息保护要求。

检测范围：mPOS受理终端

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。
- 按照《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》（Q/CUP 007.3.1-2014）中第8章模块六开放协议的检测案例进行测试。

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。
- 受理终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 8 章模块六开放协议的要求。
- 受理终端应保证能有效鉴别后台发送数据的真实性、完整性。终端输出数据的保护见账户信息保护和交易信息保护要求。。

9.2.4 账户数据保护

检测目的：终端对账户数据（包括磁条卡和 IC 卡）的保护应满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求。

检测范围：mPOS受理终端

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。
- 按照《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》（Q/CUP 007.3.1-2014）中第9章模块七账户数据保护的检测案例进行测试。

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。
- 受理终端满足《银联卡受理终端安全规范-第 1 卷：基础卷-第 2 部分：设备安全》（Q/CUP 007.1.2-2014）中第 9 章模块七账户数据保护的要求。

9.2.5 交易信息安全要求

检测目的：终端应保证所获得的交易金额、交易类型、货币类型、商户号、终端号、交易结果等关键交易信息在后续处理和传输过程中不被篡改。

检测范围：mPOS受理终端

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。
- 对终端交易信息安全要求进行有效性验证。

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。
- 终端应保证所获得的交易金额、交易类型、货币类型、商户号、终端号、交易结果等关键交易信息在后续处理和传输过程中不被篡改。

9.2.6 终端唯一性和真实性要求

检测目的：受理终端应保证具有唯一性，满足一机一密要求（例如：在主密钥和工作密钥组成的二级密钥体系中，应保证每台受理终端分配唯一主密钥；在 DUKPT 中，应保证每台受理终端分配唯一初始密钥序列号 KSN）。若涉及受理终端远程启用，终端与后台处理系统应进行联机认证，并上送受理终端设备序列号等信息，未通过联机认证不应进行支付交易。

检测范围：mPOS受理终端

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。
• 对终端唯一性和真实性要求进行有效性验证。

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。
• 受理终端必须保证具有唯一性，满足一机一密要求（例如：在主密钥和工作密钥组成的二级密钥体系中，必须保证每台受理终端分配唯一主密钥；在 DUKPT 中，必须保证每台受理终端分配唯一初始密钥序列号 KSN）。
• 若涉及受理终端远程启用，终端与后台处理系统应进行联机认证，并上送受理终端设备序列号等信息，未通过联机认证不应进行支付交易。

9.3 上位机支付应用软件安全要求

9.3.1 基础安全要求

检测目的：上位机安装的支付应用软件应符合《银联卡支付应用软件安全规范》（Q/CUP 056）的要求。

检测范围：上位机支付应用软件

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。
• 对上位机安装的支付应用软件进行有效性验证。

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。
• 上位机安装的支付应用软件必须符合《银联卡支付应用软件安全规范》（Q/CUP 056）的要求。

9.3.2 辅助信息要求

检测目的：软件应具备地理位置信息获取和上送能力，且对所获取的地理位置信息进行保护，防止处理或传输过程中被篡改。如软件可获取当前上位机唯一特征码（如 IMEI 号、设备 MAC 地址等），则应上传作为平台安全评估的辅助参考手段。

检测范围：上位机支付应用软件

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。
• 对辅助信息要求进行有效性验证。

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。
• 软件必须具备地理位置信息获取和上送能力，且对所获取的地理位置信息进行保护，防止处理或传输过程中被篡改。
• 如果软件支持获取当前上位机唯一特征码（如 IMEI 号、设备 MAC 地址等），则必须上传作为平台安全评估的辅助参考手段。

9.3.3 软件功能限制

检测目的：IC 卡应用处理内核（UICS Level 2、PBOC Level 2 等）内核不应部署于上位机。

检测范围：上位机支付应用软件

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。
• 对软件功能限制进行有效性验证。

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。
• IC 卡应用处理内核（UICS Level 2、PBOC Level 2 等）内核必须不部署于上位机。

9.4 辅助安全要求

9.4.1 防切机转网

检测目的：终端可根据管理机构要求支持防切转网功能，具体参照《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）要求。

检测范围：mPOS

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。
• 按照《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）的检测案例进行测试。

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。
• 终端可根据管理机构要求支持防切转网功能，满足《银联卡受理终端安全规范-第 4 卷：辅助卷-第 1 部分：终端防切机转网技术安全指南》（Q/CUP 007.4.1-2014）的要求。