Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

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

Security Specifications for Terminal Accepting UnionPay Card
Volume 1: Fundamental Specifications
Part 2: Device Security

中国银联 版权所有

2014-11-30 发布　　2014-12-01 实施

中国银联股份有限公司 发布

中国银联股份有限公司（以下简称“中国银联”）对该规范文档保留全部知识产权权利，包括但不限于版权、专利、商标、商业秘密等。任何人对该规范文档的任何使用都要受限于在中国银联成员机构服务平台（http://member.unionpay.com/）与中国银联签署的协议之规定。中国银联不对该规范文档的错误或疏漏以及由此导致的任何损失负任何责任。中国银联针对该规范文档放弃所有明示或暗示的保证,包括但不限于不侵犯第三方知识产权。

未经中国银联书面同意，您不得将该规范文档用于与中国银联合作事项之外的用途和目的。未经中国银联书面同意，不得下载、转发、公开或以其它任何形式向第三方提供该规范文档。如果您通过非法渠道获得该规范文档，请立即删除，并通过合法渠道向中国银联申请。

中国银联对该规范文档或与其相关的文档是否涉及第三方的知识产权（如加密算法可能在某些国家受专利保护）不做任何声明和担保，中国银联对于该规范文档的使用是否侵犯第三方权利不承担任何责任，包括但不限于对该规范文档的部分或全部使用。

目　　次

中国银联
版权所有

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1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：中国银联、银行卡检测中心、福建联迪商用设备有限公司、百富计算机技术有限公司、深圳新国都技术股份有限公司。

本部分的主要起草人：李伟、吴水炯、谭颖、张志波、周皓、杜磊、王建新、安焘、蒋利兵、倪国荣、孟陆强、姚承勇、杨超杰、黎景阳、万籁民、朱秋云、郭鸿志、陈乐。

中国银联
版权所有

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

1 范围

本部分对终端设备的安全提出要求。

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。

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 模块一：物理安全

3.1 入侵检测机制

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可被恢复。

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。

IC卡读卡器不适用本项。

3.2 独立安全机制

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。

3.3 环境和操作条件改变适应性

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。

3.4 敏感功能或信息保护

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。

IC卡读卡器不适用本项。

3.5 PIN 输入过程监控

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。

IC卡读卡器不适用本项。

3.6 密钥识别分析

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。

3.7 设备显示的物理安全

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。

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。

3.8 防偷窥保护

设备提供防止持卡人在输入PIN时被窥视的方法。

3.9 磁条读卡器保护

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。

3.10 无人值守（自助）支付终端设备防移除

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。

3.11 PIN 输入音调

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。

3.12 IC 卡读写器结构

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。

4 模块二：逻辑安全

中国银联 版权所有

4.1 自检测试

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。

4.2 逻辑异常

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。

4.3 固件和应用软件的认证及更新

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和非法的功能。

——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。验证要求遵循5.3节第二项要求。

4.4 输入 PIN 区别

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。

4.5 内存清除

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。

4.6 敏感服务

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。

4.7 随机数

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。

中国银联 版权所有

4.8 PIN 防穷举

设备应具有防止利用穷举探测PIN值的能力。

4.9 密钥管理技术

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）。

4.10 PIN 加密算法

设备采用的PIN加密技术必须遵循ISO 9564。

4.11 数据加解密

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。

4.12 明文密钥安全

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。

4.13 交易控制

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。

4.14 设备显示的逻辑安全

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）。

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。

4.15 应用隔离

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。

4.16 操作系统最小配置

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。

4.17 组件集成文档

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。

4.18 安全策略

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。

4.19 远程密钥发布

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。

5 模块三：联机 PIN 安全

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。

6 模块四：脱机 PIN 安全

6.1 防渗透保护

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。

6.2 IC 卡读写器结构

IC卡读写器结构要求应与3.12一致。

6.3 PIN 传输保护

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。

7 模块五：集成安全

中国银联 版权所有

7.1 配置管理

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。

7.2 PIN 输入功能集成

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。

7.3 终端集成

7.3.1 安全等级保持

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。

7.3.2 防卡片盗取

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

7.3.3 组件隔离

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。

7.3.4 设备显示安全

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3.7和4.14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。

7.3.5 密码输入接口控制

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。

7.3.6 设备移除要求

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。

8 模块六：开放协议

8.1 协议和接口声明和定义

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。

8.2 漏洞评估

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

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。

8.4 运行测试

8.4.1 安全协议声明

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

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。

8.4.3 数据完整性保护

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。

8.4.4 服务器身份鉴别

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。

8.4.5 异常监测

设备能够监测信息重放，并对异常进行处理。

8.4.6 随机数

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

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。

中国银联 版权所有

8.5 管理和维护

8.5.1 配置管理安全指南

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。

8.5.2 安全维护指南

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。

8.5.3 更新机制

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。

9 模块七：账户数据保护

9.1 概述

本章对持卡人账户数据的安全读取和安全交换进行规定。主要适用于账户信息读取设备，即读卡器组件。

9.2 账户数据处理

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。

9.2.1 账户数据处理的安全要求

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分，同时攻击阶段分值至少8分。

——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。

9.2.2 独立安全机制

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。

9.3 集成条件下的账户数据保护

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。

中国银联 版权所有

9.4 密钥保护

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。

9.5 加密机制

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。

9.6 远程密钥发布

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。

9.7 数据源认证

设备支持对已加密信息来源的验证。

9.8 密钥唯一性

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。

9.9 加解密数据对象控制

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。

9.10 远程访问

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。

9.11 固件审查

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。

9.12 应用真实性

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。

9.13 应用指引

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。

9.14 固件更新

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。

中国银联 版权所有

9.15 逻辑异常

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。

9.16 开放协议和服务

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。

9.17 明文数据保护

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。

9.18 主账号值替代

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。

9.19 密钥管理

设备中密钥管理技术应符合4.9节要求。

9.20 主账号防穷举

设备应具备主账号（PAN）防穷举机制。

9.21 环境和操作条件改变适应性

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。

9.22 应用隔离

要求与 4.15节相一致。

9.23 操作系统安全配置

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）；

中国银联 版权所有

——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）。

9.24 敏感服务保护

要求与 4.6节相一致。

中国银联
版权所有