Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.2.6—2014

银联卡受理终端安全规范
第 2 卷：产品卷
第 6 部分：智能销售点终端

Security Specifications for Terminal Accepting UnionPay Card
Volume 2: Product Requirements
Part 6: Smart Point of Sale Terminal

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2卷第6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：中国银联电子支付研究院、中国银联技术部。
本部分的主要起草人：李伟、程志强、吴水炯、才华、王海冰、李洁、周皓、汪毅。

银联卡受理终端安全规范
第 2 卷：产品卷
第 6 部分：智能销售点终端

1 范围

本部分对智能销售点终端（以下简称“智能终端”）提出安全要求。

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。

Q/CUP 007.1 银联卡受理终端安全规范-第1卷：基础卷

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

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 基础安全要求

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。

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。

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。

4 传输安全要求

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。

5 账户数据保护

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（下文中最终的账户数据加密设备，指对第6章所述加密磁道信息的工作密钥进行存储并完成加密运算的模块，例如密码键盘等）：

——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。

6 其他要求

6.1 操作系统安全

6.1.1 系统内核加载安全

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。

6.1.2 系统更新与升级安全

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。

6.1.3 资源访问权限控制

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（安全模块功能见附录B）

——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。

6.1.4 应用间数据交换

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。

6.1.5 应用软件管理

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。

6.2 证书管理与加密运算模块安全

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：

- 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；
- 应具备程序执行异常检测处理机制；
- 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。

7 辅助安全要求

7.1 地理位置信息

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。

7.2 防切机转网

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。

7.3 应用软件安全

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。

附 录 A
（规范性附录）密钥体系

A.1 对称密钥

交易密钥通常采用对称密钥，一般分为二级：终端主密钥(TMK)和工作密钥(WK)。

A.1.1 终端主密钥

主密钥用于对工作密钥(WK)进行加密保护，终端管理系统为每台终端分配唯一的TMK，TMK应至少采用双倍长密钥。TMK必须要有安全保护措施，只能写入并参与运算，不能被读取。TMK应安全存储于终端和终端管理系统中。

A.1.2 工作密钥

工作密钥（WK）由终端管理系统的加密机产生，在终端每次签到时从终端管理系统利用TMK加密后下载，并由TMK加密存储。终端工作密钥在下载时必须以密文传送，严禁明文传送。

智能终端使用的工作密钥通常包括用于对个人标识码(PIN)加密的PIK、进行磁道加密的TDK（磁道数据密钥）和计算报文鉴别码的MAK（报文鉴别计算密钥）。

A.2 非对称密钥

A.2.1 操作系统内核安全加载的证书和密钥

运行于智能终端之上的操作系统内核受管理方（银行卡组织及其授权机构，或其他智能终端支付系统管理运营方及其授权机构）签名保护。其中涉及的证书和密钥包括：系统内核私钥、系统内核公钥证书、操作系统管理方公钥等。

——操作系统内核应由系统内核私钥签名，操作系统管理方应将该签名数据、系统内核公钥证书（由管理方私钥签名）及签名后的操作系统内核一同发布；

——操作系统管理方公钥存储于证书管理与加密运算模块中，用于验证系统内核公钥证书并获取内核公钥；

——加载操作系统时，应使用内核公钥对签名后的操作系统进行验证，仅当验证通过条件下操作系统才可被成功加载。

A.2.2 系统通信链路安全证书和密钥

运行于智能终端之上的银联卡支付客户端与银联卡支付后台系统间的通信应由管理方（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）采用SSL/TLS双向认证机制进行保护，要求智能终端认证后台系统，且后台系统认证智能终端。其中涉及的证书和密钥包括：终端私钥、终端公钥证书、终端管理方公钥、支付后台系统私钥、支付后台系统公钥证书、支付后台系统管理方公钥等。

——终端私钥用于终端向支付后台系统的传输加密，该密钥存储于证书管理与加密运算模块中；

——终端公钥证书（由终端管理方私钥签名）存储于证书管理与加密运算模块中，在建立通信连接时由终端发送给后台系统，后台系统使用管理方公钥对其进行验证并获取终端公钥，并使用该公钥验证终端发送信息的签名；

——支付后台系统私钥用于对后台向终端的传输加密，存储于后台系统；

——支付后台系统公钥证书（由支付后台系统管理方私钥签名）存储于后台系统，在建立通信连接时由后台系统发送给终端，终端使用管理方公钥对其进行验证并获取支付后台系统公钥，并使用该公钥验证后台发送信息的签名。

A.2.3 应用软件安全证书和密钥

运行于智能终端之上的应用应经过管理方（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）重签名。其中涉及的证书和密钥包括：应用软件私钥、应用软件公钥证书、应用软件管理方公钥等。

——应用软件应由应用软件私钥签名，应用软件管理方应将该签名数据、应用软件公钥证书（由管理方私钥签名）及签名后的应用软件一同发布；

——应用软件管理方公钥存储于证书管理与加密运算模块中，用于验证应用软件公钥证书并获取应用软件公钥；

——安装应用时，应使用应用软件公钥对签名后的应用软件进行验证，仅当验证通过条件下应用软件才可被成功安装。