Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.4.1—2014

银联卡受理终端安全规范
第 4 卷：辅助卷
第 1 部分：终端防切转网技术安全指南

Security Specifications for Terminal Accepting UnionPay Card
Volume 4: Auxiliary Requirements
Part 1: Technical Security Guideline for Terminal Anti-Refurbishment

中国银联股份有限公司

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4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：中国银联、福建联迪商用设备有限公司。
本部分的主要起草人：吴水炯、倪国荣、姚承勇。

中国银联
版权所有

银联卡受理终端安全规范
第 4 卷：辅助卷
第 1 部分：终端防切转网技术安全指南

1 范围

本部分为终端防切机转网（刷机）提供技术安全指南，供收单机构和生产企业参考使用。

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 058 银联卡密码算法使用与密钥管理规范》

3 背景

切机转网，指部分金融收单机构、代理商或商户未经终端原收单机构授权，在原收单机构所拥有、且已经布放到商户的终端中下载非原收单机构授权的应用程序，或者替换终端原收单机构的应用程序，从而以较低的成本代价实现改变终端收单业务接入方的目的，使原收单机构商户拓展的利益受损。

本文中的原收单机构指对终端拥有所有权的收单机构。

针对上述现象，提出终端防切机转网技术指南，为具有相应需求的机构提供参考。

4 功能定义

防切机转网的核心是保障收单机构合法程序运行，防止未经授权的程序运行，包含两个层面功能：

——利用电子签名技术，阻止非法程序（包括非法开发和篡改的程序）运行，避免未经检验的应用程序流通到市场上，造成收单安全隐患；

——利用厂商的软硬件技术保障手段，保护收单机构合法商业利益诉求，阻止合法开发和检验、但属于其他机构的应用程序在未经原收单机构授权的情况下装载到终端并运行。

在终端安全体系中，签名技术可以有效鉴别程序合法性，即实现上述第一个层面的功能，并在《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）中已明确要求。本指南以电子签名技术为基础，主要针对收单机构商业利益保护，即实现上述第二个层面的功能。

5 手段分析

切机转网存在多种形式，相应代价不同，在现有技术和管理条件下具有不同的对应方案。

表1 现有主要切机转网手段分析

切机转网方式	切机代价	应对方案
通过安装工具，在终端下载未经原收单机构授权的应用程序	低	在终端布放前安装并固化特定的“机构根证书”，终端只能下载和运行该“机构根证书”授权认证的应用程序
窃取终端厂商所使用的PC工具，将终端恢复成出厂默认状态，抹除购买方（原收单机构）的机构根证书，并重新下载未经授权的应用程序或机构根证书	中等	加强厂商工具管控。 使用操作员授权卡等方式防止非厂商人员和非授权人员的操作。启用激活操作，使终端在该切机行为下需要授权激活才能运行应用程序。
绕开厂商的固件保护措施，通过拆解终端，从目标终端中通过镜像拷贝的方式，或通过第三方工具直接编辑FLASH内容的方式，替换原有固件及机构根证书。	较高	识别硬件拆机行为并促发激活操作。 通过激活操作，恢复至初始机构根证书。
直接替换终端中关键芯片。	高	切机成本高，跟踪但暂不处理。

上表分析现有主要切机转网手段，随着技术发展，不排除未来出现新的手段和方式。应对方案不存在绝对有效性和永久有效性，只有不断提高切机成本，使非法切机者无法因此获取足够的商业利益或无法弥补付出成本，进而放弃采取非法行为。这也与终端安全乃至整个安全领域的基本认识相一致。

6 技术方案

6.1 概述

本指南所述防切转网方案包括以下三个方面：

——终端应用程序签名认证：保证终端只能安装和运行合法签名的应用程序；

——机构根证书保护：保证签名认证功能所需的原收单机构根证书不被非法篡改或者替换；

——授权激活操作：终端由异常状态（一般指受到外部攻击，例如本指南所述的对机构根证书或其他敏感信息的更改等）转换到正常状态时由授权操作员进行的授权确认操作。

执行安全操作的固件代码应通过其他手段进行真实性和完整性的保护，本指南不再展开。

6.2 数字签名和证书体系

6.2.1 多级证书体系

以三级证书体系为例对数字证书体系及其安全机制进行说明。

表2 数字证书体系范例（三级证书）

层级	证书	作用	备注
第一级	终端根证书	验证机构根证书合法性	出厂固化
第二级	机构根证书	验证工作证书合法性	由终端根证书对应私钥签发，不可篡改和替换
第三级	工作证书	验证目标文件(终端应用程序文件或更新）签名数据合法性	由机构根证书对应私钥签发

其中，机构根证书表明该终端对应的收单机构身份，也是收单机构终端所有权的保证，不可被篡改和替换。

工作证书由收单机构根证书对应私钥签发，保存于定制签名设备（如签名卡）中，对应私钥无法导出到签名设备之外。签名设备对目标文件进行签名，该签名数据将与目标文件、工作证书一并下载到终端，供终端验证。

收单机构根据自身管理需求，选择是否设置工作证书。如不设置工作证书，则由机构根证书对应私钥对应用程序文件直接进行签名。

机构也可以基于机构根证书，建立自身的多级证书机制满足实际管理需求。

6.2.2 终端应用程序认证

终端应用程序文件由工作证书对应的私钥签名。

终端下载或更新应用程序时，机构根证书对一同下载的工作证书进行合法性验证。验证通过后用工作证书对应用程序签名数据进行合法性验证，通过后应用程序才能被正常安装和运行。

6.2.3 机构根证书保护

机构根证书一般在出厂时预置。该证书的安全保护应满足以下要求：

——机构根证书由终端根证书对应私钥签发，终端根证书对机构根证书签名数据验证通过后，机构根证书才能被装载于终端内。

——终端固件应设置有效的逻辑安全机制，判断终端是否已经装载机构根证书，如已装载，则其不应被修改和替换。

——任何对机构根证书的攻击行为应导致终端进入异常状态，仅当完成授权激活操作才能使终端进入正常状态。

——每次上电，终端应对机构根证书进行自检验证，确保其完整性，并确保其未被其他根证书替换。如自检未通过，终端应进入异常状态，需授权激活才能正常使用。

6.2.4 终端根证书保护

终端根证书及其对应私钥是方切转网安全方案的基础，应满足以下要求：

——终端根证书对应私钥应保存于厂商安全房加密机内。

——终端根证书应固化于终端硬件安全区内，任何对其进行的修改、替换等操作均应使终端进入异常状态。

6.2.5 终端授权激活

终端受到攻击时应促发安全机制，使终端进入异常状态，应用程序和安全功能无法运行。仅当完成授权激活后，终端才能返回正常状态。

授权激活应由授权人员持专用设备（如授权激活卡）进行操作，并具备相应的安全认证，包括：

——授权人员身份认证，可通过专用设备识别叠加后台联机认证等方式实现。

——机构根证书一致性检查，验证当前终端内机构根证书是否与正常配置相一致。

厂商应提供有效且可行的管理手段保证授权激活操作的安全性，防止不受控制或单一人员违背授权激活管理意志的行为。

6.3 加密算法要求

数字签名所采用的加密算法和参数应符合《银联卡密码算法使用与密钥管理规范》（Q/CUP 058）要求，如非对称加密采用2048位及以上长度RSA算法，哈希计算采用SHA-256及以上算法等。

7 数字签名工具管理

收单机构应采取有效手段对机构根证书对应的数字签名工具进行安全管理，包括但不限于以下要求：

——应妥善保管数字签名工具及其密码口令。

——应设置严格的安全管理制度，控制签名工具对应用程序的签名操作。

——工具及其密码口令保管、签名操作等应设置安全专员实施，其人员设置和变更应在第一时间内通知终端厂商，并建立联系人机制。

——非安全专员进行的签名操作应获得安全专员授权，并采取必要管理手段保证操作的可追溯性和操作信息（操作人员、操作时间、目标应用程序等）的完整性。

——当发生工具丢失或口令泄露，应在第一时间通知终端厂商，进行应急处理，例如重新发布新的签名工具和机构根证书，应用程序采用新的签名后才被发布等。

——应用程序签名操作应在受控环境下进行，确保签名工具的正确使用。

中国银联
版权所有