Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

银联卡受理终端安全规范
配套文档
规范升级说明

Security Specifications for Terminal Accepting UnionPay Card
Supporting Documents
Specification Update Introduction

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》配套文档的规范升级说明。
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：中国银联技术部
本部分的主要起草人：吴水炯。

银联卡受理终端安全规范
配套文档
规范升级说明

1 范围

本部分对《银联卡受理终端安全规范》由UPTS 1.0升级到2.0版本的升级背景、工作原则、升级内容和形式、工作过程等进行说明，属于规范配套文档。

2 升级背景

随着银行卡产业整体发展，受理终端市场也出现了新的变化，对终端安全规范和标准化工作提出了新的要求。

首先，原有《银联卡受理终端安全规范》（以下简称“UPTS 1.0”）体系构成中缺乏层次性，标准以产品形态分布，但过分依赖产品，而核心安全基础的提炼和建立相对较为薄弱。

第二，以PIN输入设备安全为代表的终端核心安全部分自2010年起已有较长时间未有修订，随着技术的发展和社会环境的变化，终端开始面临新的安全挑战，威胁程度也有所提高，有必要对核心的安全内容进行一次全面补充和升级。

第三，UPTS 1.0要求内容的灵活性和适用性有待提高，在技术和产品创新日益加快的当下，给规范对市场的适应能力造成了一定影响，给制定和推广工作带来难度。

第四，UPTS 1.0各部分规范间存在内容重复冗余的现象，不利于规范的维护。

3 工作原则

3.1 标准工作基准

遵循技术标准工作基本准则：

——体现层次性和结构性；

——以支付交易信息安全为基础，体现全面性和可操作性；

——以支持、服务、引导市场的健康发展为根本；

——考虑市场现状，兼顾发展需要，力争先进性和前瞻性；

——内容简洁、重点突出，对现有国际、国家、行业、企业标准中已规定的内容、以及本系列规范其他卷、其他部分的内容，只做引用，不重复定义。

3.2 工作延续性

——保持标准主要内容的延续，以整合、补充和提升为主；

——保持认证工作的稳定，沿用UPTS 1.0分类，在升级后系列规范（UPTS 2.0）产品卷保留了原有产品形态并在认证工作中继续体现，对市场使用不产生影响；

——制定了科学的实施方案，明确对存量和新增产品的标准化要求，明确新老规范在时间上的适用性（详见《银联卡受理终端安全规范-配套文档：实施计划》），保证标准升级的平稳过渡。

4 升级内容

4.1 结构和内容调整

UPTS 1.0按产品类型划分为8个部分标准，UPTS 2.0划分为基础卷、产品卷、检测卷、辅助卷共四卷，形成层次化结构。

第1卷基础卷：经提炼和完善后，为终端安全提供基础性要求，包括术语、设备安全、管理安全、硬件要求等四个部分。

——术语：对UPTS 1.0分散在各部分的术语和缩略语进行整合和补充，形成统一的术语部分；

——设备安全：在UPTS 1.0的PIN输入设备安全的基础上进行了较大幅度补充和增强，成为终端设备的基础安全要求，并实现模块化；

——管理安全：以UPTS 1.0的PIN输入设备安全的管理要求内容为基础，进行完善；

——硬件要求：对UPTS 1.0分散在各部分的硬件要求进行整合。

第2卷产品卷：保持UPTS 1.0对产品的划分，各部分要求以基础卷模块组合为基础，附加产品特征性的安全要求，全卷目前包括POS终端、无人值守（自助）终端、个人支付终端、独立部件、电话支付终端、智能终端、mPOS通用技术安全等七个部分，核心的安全要求引用基础卷，各产品的硬件要求已在基础卷硬件要求部分统一说明。

——POS终端：对应UPTS 1.0第1部分《POS终端安全规范》；

——无人值守（自助）终端：对应UPTS 1.0第3部分《自助终端安全规范》；

——个人支付终端：对应UPTS 1.0第7部分《个人支付终端安全规范》；

——独立部件：针对装配到其他终端中，实现PIN输入、IC卡阅读、磁条卡阅读等功能的独立部件所设置的规范；

——电话支付终端：对应UPTS 1.0第5部分《电话支付终端安全规范》；

——智能终端：对应UPTS 1.0第8部分《智能销售点终端安全规范》；

——mPOS通用技术安全：对应UPTS 1.0第9部分《mPOS通用技术安全要求》。

第3卷检测卷：针对第1卷基础卷和第2卷产品卷的技术要求，给出对应的检测要求，供送检单位参考使用，分为基础安全检测、产品分类安全检测、硬件技术检测等三个部分。

——基础安全检测要求：针对本系列规范第1卷基础卷第2部分设备安全、第3部分管理安全所设定的要求，对应给出检测要求；

——产品分类安全检测要求：针对本系列规范第2卷产品卷所设定的要求，对应给出检测要求，基础部分引用基础安全检测部分，叠加各产品特殊要求；

——硬件技术检测要求：针对本系列规范第1卷基础卷第4部分硬件要求部分，对应给出检测要求。

第4卷辅助卷：非正式规范，主要包括重点终端安全领域技术实现方案和指引、以及行业性、个性化的支付安全技术指南或方案，属于辅助性文档，应对市场需求，仅供生产、使用单位参考，并根据实际情况不断补充。

——终端防切转网技术安全指南：针对机构防切机转网需求，所设计的技术方案和对应安全指引，建议有需求的机构按此方案进行部署实施；

——航空机上支付技术安全指南：针对航空行业机上支付场景的特殊性，所设计的技术安全指引，建议该行业的支付方案根据本指南进行部署实施；

——POS互联网接入系统部署方案：针对POS终端通过互联网方式接入收单系统，所设计的技术实施方案，供有需求的机构和生产企业参考使用；

——终端非法移机监控技术指南：针对终端非法移机现象和监控需求，所总结的技术方案和指引，供有需求的机构和生产企业参考使用。

原有UPTS 1.0第1部分《POS终端安全规范》补充文档《POS终端支持互联网接入的技术安全要求》由UPTS 2.0第1卷基础卷第2部分设备安全中的第8章模块六开放协议及各产品中的特定要求所替代。

原有UPTS 1.0第2部分《银联卡受理信息系统安全规范》保留成为独立规范，不再列入终端安全规范系列。

4.2 重点内容

4.2.1 基础安全较大升级

原有UPTS 1.0无基础安全层规范，仅在PIN安全要求上有《PIN输入设备安全规范》作为基础，且自编制之后尚未进行修订，在对新产生的安全需求的应对上有欠缺。

UPTS 2.0专门整合形成基础卷规范，为所有终端设备提供最基础、最核心的安全支撑，并以模块化形式展现，包括：物理安全模块、逻辑安全模块、联机PIN安全模块、脱机PIN安全模块、集成安全模块、开放协议模块、账户数据保护模块等共七个设备安全要求模块，以及管理安全模块。

——物理安全、逻辑安全、联机PIN安全、脱机PIN安全等四个设备安全模块以UPTS 1.0《PIN输入设备安全规范》为基础，强化了安全要求，对以分值评估的安全项改进了分值计算方法、提升了分值要求；

——新增集成安全、开放协议、账户数据保护等三个设备安全模块，其中集成安全主要针对自助类终端的设备集成提出安全要求；开放协议主要针对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的终端，提升数据传输安全性；账户数据保护主要针对终端账户数据的安全保护提出要求。

4.2.2 产品分类不变化

为保持标准升级和认证工作的平稳过渡，同时保持机构终端习惯和延续性，UPTS 1.0已有的7类产品均得到保留，并在第2卷产品卷中以7个部分的形式展示。

——除因基础卷的整合和升级导致的整体基础要求提升之外，各UPTS 1.0的产品要求基本保持不变，但针对部分功能要求满足基础卷升级中新引入的模块要求（集成安全、开放协议和账户数据保护）；

——对于有明确账户数据保护需求的终端（例如mPOS的受理终端），要求必须满足新增的账户数据保护模块要求；其余类型终端分别补充了增强的账户数据安全要求，账户数据保护模块不强制；

——对于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的终端，要求必须满足新增的开放协议安全要求；

——对于无人值守（自助）终端，要求必须满足集成安全要求。

4.2.3 硬件要求整合

硬件要求进行整合，形成第1卷基础卷第4部分硬件要求，统一基本硬件模块功能和性能的基础性要求，并对个别因产品类型和应用场景不同导致的硬件差别提出区分要求。

未来存在硬件要求与安全要求分离的标准化发展可能。

5 规范使用

UPTS 2.0建议按以下方式阅读和使用，特别是对于终端生产企业和使用机构：

——了解UPTS 2.0整体架构；

——阅读第2卷产品卷，了解具体产品类型的要求，内容包括：指明基础卷中哪些模块适用于本类型产品，说明适用的条件，列举在基本模块要求之外该类型特殊的要求，并提出辅助要求和建议；

——根据产品卷各部分内的要求，对于基础模块，参阅第1卷基础卷对应部分和章节；

——对于需了解检测工作的人员和单位（如生产企业等），可在了解以上内容后，阅读第3卷检测卷；

——对于具有其他安全技术、实施方案等类型需求的人员和单位，可在第4卷辅助卷寻找技术指南或部署方案以获得参考信息。

6 工作过程

第一阶段，2013年11月-2014年4月，研究和规划：了解市场实际情况，分析UPTS 1.0存在问题及对目前和今后标准、认证和产品工作的影响，分析规范升级的必要性和可行性，明确规范工作方向，规划升级后新的《银联卡受理终端安全规范》（以下简称“UPTS 2.0”）的架构组成和内容范围。

第二阶段，2014年5月-2014年7月，讨论和编写：就UPTS 2.0系列规范整体架构、内容组成、实施规划等组织检测机构、生产企业等进行反复讨论，形成具体工作思路，完成初稿编写。

第三阶段，2014年8月-10月，征求意见：组织银联内部相关部门、主要终端生产企业、非金融支付机构讨论，提交技管委工作组会、银联技术专题会评审，根据各方反馈意见对标准进行补充完善。

第四阶段，2014年11月，提交审议：技管委正式审议并发布。

7 其他事项

本标准的升级得到了银行卡检测中心、联迪、百富、新大陆、新国都、惠尔丰、升腾、瑞佰等单位专家的大力支持和帮助，在此表示感谢。