Q/CUP

中 国 银 联 股 份 有 限 公 司 企 业 标 准

Q/CUP 007.1.1—2014

银联卡受理终端安全规范
第 1 卷：基础卷
第 1 部分：术语

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

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 III
1 范围 1
2 术语和定义 1
3 缩略语 4

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：中国银联技术部
本部分的主要起草人：吴水炯、谭颖、李伟。

银联卡受理终端安全规范
第 1 卷：基础卷
第 1 部分：术语

1 范围

本部分对《银联卡受理终端安全规范》系列各卷、各部分规范中涉及的术语和缩略语进行集中解释。

2 术语和定义

2.1

银行卡 bank card

商业银行等金融机构及邮政储汇机构向社会发行的，具有消费信用、转账结算、存取现金等全部或部分功能的信用支付工具。

2.2

持卡人 card holder

银行卡的合法持有人，即与卡对应的银行账户相联系的客户。

2.3

磁条卡 magnetic stripe card

物理特性符合GB/T 14916标准，磁条记录符合GB/T 15120、GB/T 15694-1、ISO 7812-2、GB/T17552标准的银行卡片。

2.4

集成电路（IC）卡 integrated circuit card

内部封装一个或多个集成电路用于执行处理和存储功能的卡片。

2.5

个人标识码 personal identification number；PIN

即个人密码，是在交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中任何环节都不允许PIN以明文的方式出现。

2.6

敏感数据（信息） sensitive data（information）

指磁道信息、PIN和加密密钥等终端或持卡人独有的数据或信息，敏感数据进行有效保护，防止泄露、被修改或被破坏。

2.7

固件 firmware

在终端内部与设备安全性相关所有程序代码称为固件，固件必须符合本规范的各项安全要求。

2.8

销售点终端 point of sale；POS

能够接受银行卡信息，具有通讯功能，并接受柜员的指令而完成金融交易信息和有关信息交换的设备。

2.9

自助服务 self-service

通过人机交互自主选择并获得所需服务的方式。

2.10

无人值守（自助） 支付终端 unattended payment terminal（UPT）

简称“自助终端”，由持卡人操作的设备或装置，它在无人值守的环境中读取、捕捉和传输卡中的信息，提供自助服务功能。

2.11

钓现 fishing

将任何形式的带有一个或多个钩子或其它装置的绳索、金属线或类似物品作用于自助服务终端，以非法获取现金。

2.12

暴力取现 forcing

用撬棍、螺丝起子、扳手、或其它类似工具扩大缝隙，或通过打破一个部件或使一个部件变形以获取现金。

2.13

加密密码键盘 encrypt PIN pad, EPP

用于自动PIN受理装置中安全输入PIN码和加密的装置。EPP可以带有一个内置显示屏或读卡器，或者采用自动装置中安装的外部显示屏或读卡器。EPP一般用在ATM机中（或自动加油器中），用于输入PIN码，通过装置控制器控制。EPP具有明确的物理和逻辑界限以及一个防篡改功能或者能够显示篡改迹象的外壳。

2.14

个人支付终端 personal payment terminal, PPT

持卡人个人在支付及认证过程中使用的一种终端设备，该设备可连接个人计算机、移动电话等个人设备联接后台。个人支付终端具备读取银行卡数据的能力，能加密保护卡片数据，部分终端也具有PIN信息保护能力。

2.15

电话支付终端 telephone payment terminal

简称电话终端。在传统电话设备基础上发展起来的一种新型终端设备，电话支付终端通过与电话支付中心进行信息交互、由后台定制交易完成基于银行卡的各种业务功能。以其适用的环境及功能不同分为I型终端II型终端。I型终端建议用于家庭等私有场所。II型终端建议用于有人值守的小区和便民点、单位办公室和无集中收银的商品批发市场。

2.16

TSAM 卡

I型终端中用于终端安全控制的接触式IC卡。

2.17

TKEY 卡

I型终端中用于下载终端认证密钥的接触式IC卡。

2.18

FSK

频移键控，英文全拼是Frequency Shift Keying。

2.19

HDLC

高速数据链路控制，英文全拼是High Level Data Link Control。

2.20

DTMF

双音多频，英文全拼是Dual Tone Multi-frequency。

2.21

智能销售点终端 smart POS

商户在支付及认证过程中使用的一种智能终端设备，该设备支持磁条卡、IC卡等银行卡数据的读取，能实现卡片及PIN信息的加密保护，可通过互联网接入智能销售点终端后台系统，与后台系统共同实现银行卡交易受理。本规范以下简称“智能终端”。

2.22

智能销售点终端操作系统 smart POS operating system

在智能销售点终端搭载并运行的操作系统，能实现应用的加载和运行、资源的调用、以及安全防护等功能。本规范以下简称“智能终端操作系统”。

2.23

银联卡支付客户端 unionpay payment client

运行于智能终端的支付客户端，提供银行卡的受理入口。

2.24

银联卡智能销售点终端后台系统 unionpay cloud payment background system

银联卡支付客户端的后台系统，具有银行卡交易处理、终端管理等功能。本规范以下简称“智能终端后台系统”。

2.25

应用管理客户端 AppStore client

运行于智能终端的多应用管理客户端，其提供的功能包括但不限于应用下载、应用发现、应用搜索、应用安装、应用卸载等功能。

2.26

应用管理后台系统 AppStore background system

作为应用管理客户端的后台系统，其提供的功能包括但不限于多应用的生命周期管理等功能。

2.27

密钥 key

加密转换中控制操作的一组符号。

2.28

对称密钥 symmetric key

又称专用密钥加密，即发送和接收数据的双方必须使用相同的密钥对明文进行加密和解密运算。对称密钥加密算法主要包括：DES、3DES、IDEA、FEAL、BLOWFISH等。

2.29

工作密钥 working key; WK

对通信各方首发的数据进行加密的密钥，在终端中主要包括PIN加密密钥（PIK）、MAC计算密钥（MAK）和磁道数据密钥（TDK）等，存储于设备的硬件安全存储区域中。工作密钥应经常更新。在联机更新的报文中对工作密钥必须用密钥加密密钥（KEK）加密，形成密文后进行传输。

2.30

非对称密钥 asymmetric keys

非对称密钥，需要使用一对密钥来分别完成加密和解密操作，一个公开发布，即公开密钥，另一个由使用者秘密保存，即私用密钥。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。

2.31

公钥 public key

在一个实体使用的非对称密钥对中可以被公众使用的密钥。在数字签名方案中，公钥定义验证函数。

2.32

私钥 private key

在一个实体使用的非对称密钥对中仅被该实体使用的密钥。在数字签名方案中，私钥定义签名函数。

2.33

数字证书 digital certificate

由发行证书的认证中心使用其私钥对实体的公钥、身份信息以及其它相关信息进行签名，形成的不可伪造的数据。

2.34

数字签名 digital signature

对数据的一种非对称加密变换。该变换可以使数据接收方确认数据的来源和完整性，保护数据发送方发出和接收方收到的数据不被篡改。

2.35

认证中心 certificate authority; CA

CA是证书的签发机构，是负责签发证书、认证证书、管理已颁发证书的机关。它负责制定政策和具体步骤来验证、识别用户身份，并对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权。

2.36

SSL 和 TLS

安全套接层协议（Secure Sockets Layer，SSL）和传输层安全协议（Transport Layer Security，TLS）对网络连接实现加密，是为网络通信提供安全及数据完整性的一种安全协议。

2.37

IPSEC

IPSEC（Internet Protocol Security），是通过对IP协议（互联网协议）的分组进行加密和认证来保护IP协议的网络传输协议族（一些相互关联的协议的集合）。

3 缩略语

IC	Integrated Circuit	集成电路
PIN	Personal Identification Number	个人识别码
POS	Point of Sale	销售点终端
UPT	Unattended Payment Terminal	无人值守（自助）支付终端
EPP	Encrypt PIN Pad	加密密码键盘
HDLC	High Level Data Link Control	高速数据链路控制
DTMF	Dual Tone Multi-Frequency	双音多频
CA	Certificate Authority	认证中心
SSL	Secure Sockets Layer	安全套接字层协议
TLS	Transport Layer Security	传输层安全协议
IPSEC	Internet Protocol Security	互联网协议安全协议