

附件

ICS 03.060

A 11

备案号:

JR

中华人民共和国金融行业标准

JR/T 0061—2011

银行卡名词术语

Bank card terminology

2011-06-10 发布

2011-06-10 实施

中国人民银行 发布

目 次

前言	I
1 范围	2
2 规范性引用文件	2
3 卡片术语	2
4 机构及人员术语	7
5 终端及设备术语	10
6 业务及应用术语	14
7 信息交换术语	27
8 安全及风险管理术语	35
附录 A（资料性附录） 银行卡名词术语中文索引	51
附录 B（资料性附录） 银行卡名词术语英文索引	66
参考文献	81

前 言

本标准依据GB/T 1.1《标准化工作导则 第1部分：标准的结构和编写》起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC180）归口。

本标准主要起草单位：中国人民银行、中国金融电子化公司。

本标准参加起草单位：中国工商银行、中国建设银行、中国银联、银行卡检测中心、国家电子计算机质量监督检验中心。

本标准主要起草人：姜云兵、李曙光、张雯华、李兴峰、张艳、赵志兰、吴藩、古炜旋、杜秉一、张永峰、沈涛、黄贵玲。

银行卡名词术语

1 范围

本标准规定了常用的银行卡名词术语，包括卡片术语、机构及人员术语、终端及设备术语、业务及应用术语、信息交换术语、安全及风险管理术语。附录A和附录B分别给出了银行卡名词术语的中文和英文索引。

本标准适用于与银行卡应用相关的卡片设计、管理、发行、受理以及应用系统的研制、开发、集成和维护等相关部门（单位）。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 14916 识别卡 物理特性
- GB/T 15120（所有部分） 识别卡 记录技术
- GB/T 15150 产生报文的银行卡 交换报文规范 金融交易内容
- GB/T 15694.1 识别卡 发卡者标识 第1部分：编号体系
- GB/T 17552 识别卡 金融交易卡
- GB/T 18789 自动柜员机（ATM）通用规范
- GB/T 19584 银行卡磁条信息格式和使用规范

3 卡片术语

3.1

识别卡 identification card

一种可识别其持卡人和发卡机构的卡，卡上载有其预期应用和有关交易所要求输入的数据。

3.2

银行卡 bank card

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

3.3

借记卡 debit card

没有透支功能，需先存款后才能进行消费、取现等行为的银行卡。

3.4

信用卡 credit card

持卡人凭其信用获得发卡机构授信，并在授信额度内从特定金融机构获得现金、转账存取或者从特约商户获得商品、服务等，并按照约定方式清偿账款所使用的电子支付卡片。信用卡按是否向发卡机构交存备用金分为贷记卡、准贷记卡两类。

3.5

贷记卡 credit card

发卡机构给予持卡人一定的信用额度，持卡人可在信用额度内先消费、后还款的信用卡。

3.6

准贷记卡 semi-credit card

持卡人须先按发卡机构要求交存一定金额的备用金，当备用金账户余额不足以支付时，可在发卡机构规定的信用额度内透支的信用卡。

3.7

主卡 main card

在同一账户下的多张银行卡的使用中起主导作用的银行卡，主卡持卡人需承担副卡项下全部债务。

3.8

副卡 supplementary card**附属卡** supplementary card

在同一账户下的多张银行卡的使用中处于附属地位的银行卡。

3.9

套卡 card family

一组相关联的银行卡，通常具有相同的标识，使用共有的支付系统进行交易。

3.10

未使用的卡 unused card

具有其预期目的所要求的所有部件、未进行过任何个人化和测试操作，并且被保存在洁净的环境中，在 5℃~30℃ 的温度和 10%~90% 的湿度条件下暴露在日光下的时间不超过 48 小时，也未遭受过热力冲击的卡。

3.11

错误制卡 misembossed card

压卡时包含错误信息的有效卡片。

3.12

编码错卡 misencoded card

在编码时包含错误信息的有效卡片。

3.13

过期卡 expired card

卡片凸印的、存储的、或是印制的有效期已经逾期的卡片。

3.14

ID-000 型卡 ID-000 card

标称尺寸为：宽度 25mm，高度 15mm，厚度 0.76mm 的识别卡。

3.15

ID-1 型卡 ID-1 card

标称尺寸为：宽度 85.60mm，高度 53.98mm，厚度 0.76mm 的识别卡。

3.16

ID-2 型卡 ID-2 card

标称尺寸为：宽度 105.00mm，高度 74.00mm，厚度 0.76mm 的识别卡。

3.17

ID-3 型卡 ID-3 card

标称尺寸为：宽度 125.00mm，高度 88.00mm，厚度 0.76mm 的识别卡。

3.18

磁条 magnetic stripe

包括磁编码信息的条状物。

3.19

磁条卡 magnetic stripe card

磁记录介质卡片，其有三条记载磁编码信息的磁道。

注：物理特性应符合 GB/T 14916 标准，磁条记录符合 GB/T 15120、GB/T 15694.1、GB/T 17552、GB/T 19584 标准。

3.20

磁道数据 track data

一磁、二磁和三磁定义的必备或可选的数据元。

注：磁道数据可以在物理卡的磁条上，也可以被包含在集成电路或者其他媒介上。

3.21

一磁 track 1

银行卡的第一条磁道，为只读属性，其数据元定义见 GB/T 19584 中。

3.22

二磁 track 2

银行卡的第二条磁道，为只读属性，其数据元定义见 GB/T 19584 中。

3.23

二磁等价数据 track 2 equivalent data

该数据依据 GB/T 19584，包含磁条二磁的数据元。这些数据包括：主账号（PAN）、域分隔符、有效期、服务代码和自定义数据域，但不包含开始和结束标识符以及纵向冗余检查。

3.24

三磁 track 3

银行卡的第三条磁道，为读写属性，其数据元定义见 GB/T 19584 中。

3.25

集成电路（IC） integrated circuit (IC)

具有处理和/或存储功能的电子器件。

3.26

集成电路卡（IC 卡） integrated circuit card (ICC)

芯片卡 chip 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。

3.27

存储卡 memory card

具有存储信息功能，但不具备高级计算能力（例如，不含微处理器）的一种集成电路卡。

3.28

逻辑加密卡 smart card with security logic

以可电擦除的可编程只读存储器和密码控制逻辑单元为核心器件，能多次重复使用的 IC 卡。

3.29

智能卡 smart card

CPU 卡 CPU card

配置有容量很大、类型不同的存储器，逻辑控制电路以及微处理器（CPU）电路，能多次重复使用的 IC 卡。

3.30

磁条芯片复合卡 combined IC and magnetic stripe card

兼具磁条卡和芯片卡两者功能的复合卡。

3.31

掩膜 mask

在制作过程中，将一组指令保存在永久的非易失存储器中（例如只读存储器），或存储在非易失可编程存储器中。

3.32

触点 contact

保持集成电路卡和外部接口设备之间电流连续性的导电元件。

3.33

TIM 卡 TIM card

用户初始化终端参数的接触式 IC 卡。

3.34

TKEY 卡 TKEY card

用于下载终端认证密钥的接触式 IC 卡。

3.35

TSAM 卡 TSAM card

用于终端安全控制的接触式 IC 卡。

3.36

无触点的 contactless

无需使用通电元件完成与卡交换信号和给卡供应能量（即不存在从外部接口设备到卡内所包含集成电路的欧姆性通道）。

3.37

非接触卡 contactless card

无触点的集成电路卡 contactless integrated circuit card

卡片与接口设备间不经接触，而是通过射频接口的高频传输技术导入能量从而传递信息的卡片。

3.38

邻近式 IC 卡 (VICC) vicinity IC card (VICC)

一种 ID-1 型卡，其中已装入集成电路和耦合电路，与集成电路的通信是通过与邻近式耦合设备中的电感耦合进行的。

3.39

接近式 IC 卡 (PICC) proximity IC card (PICC)

一种 ID-1 型卡，在它上面已装入集成电路和耦合电路，与集成电路的通信是通过与接近式耦合设备的电感耦合完成的。

3.40

发卡行标识域 issuer identification area

在卡面上不同于银行卡清算组织标识的地方，标注有发卡行名字、标识及所有设计元素的区域。发卡行也可能在此区域内印上卡种类名称，联名种类标识或合作卡种类的标识。

3.41

卡号 card number

主账号 (PAN) primary account number (PAN)

用于标识发卡机构及卡片的号码，由发卡机构标识代码、发卡机构自定义位和校验位组成，其应遵照 JR/T 0008 的规定。

3.42

主账号序列号 primary account number sequence number

用来确认和区分具有相同主账号 (PAN) 的卡片和持卡人的数据元。

3. 43

第一辅助账号 (SAN-1) first subsidiary account number (SAN-1)

除主账号之外的第一个可供选用的辅助账户标识。

3. 44

第二辅助账号 (SAN-2) second subsidiary account number (SAN-2)

除主账号和第一辅助账号之外的第二个可供选用的辅助账户标识。

3. 45

卡段 card range

卡号的一段范围。

3. 46

签名条 signature panel

卡上用于签名的特定区域。

3. 47

凸印 embossing

一种使字符从卡的正面显著地凸起的印刷方式。

3. 48

凸起区 raised area

在卡表面加上一些特征如全息图、签名条、磁条、照片、集成电路触点、凸印字符等而凸起的卡表面区域。

3. 49

(字符的) 凸印起伏高度 embossing relief height (of character)

凸印处理所产生的卡表面局部升起的高度。

3. 50

卡片有效期 expiration date

发卡机构规定的卡片有效使用时间。一般印制在卡片的正面左下方位置, 并与磁条或芯片内相应信息一致, 超过该时间后, 卡片将停止使用。

3. 51

可检测功能 testably function

经受了某些可能的破坏性作用后, 仍有以下功能: a) 卡上的任何磁条都给出了根据基本标准进行暴露前后信号幅度间的关系; b) 卡上的任何集成电路仍然给出了符合基本标准的复位应答响应; c) 与卡上的任何集成电路相关的任何触点仍然给出了符合基本标准的电阻和阻抗; d) 卡上的任何光存储器仍然给出了符合基本标准的光特性; e) 卡上的任何非接触集成电路仍然按其用途进行操作。

3. 52

矫顽力 coercivity

抗磁力 coercivity

持续作用的磁场从先前的饱和磁化状态, 沿相反方向把磁化减小到零时, 在与磁条纵轴平行的方向测量到的磁场强度。

3. 53

磁通翻转 flux transition

垂直于磁条表面最大磁通分量的位置。

3. 54

基准信号幅度 reference signal amplitude

校正到主标准的基准卡的最大平均信号幅度

3.55

平均信号幅度 average signal amplitude

当以规定的记录密度用测试记录电流记录时，在卡的全部记录区测出的读出电压峰—峰值的平均值。

3.56

基准电流 (IR) reference current (IR)

在给定的测试条件下，读出电压幅度等于密度为 8ftpmm (磁通翻转每毫米) 的最大幅度的 80% 时，基准卡上产生的最小记录电流幅度 (方波)。

3.57

剥离强度 peel strength

在构造方面，卡抵御相邻层材料分离的能力。

3.58

耐化学性 resistance to chemicals

暴露在通常遇到的化学制品之下，卡保持其性能和外观的能力。

3.59

粘连或并块 adhesion or blocking

将新卡堆积时的粘接性。

3.60

翘曲 warpage

相对平面的偏离。

3.61

弯曲韧性 bending stiffness

卡抗弯曲的能力。

3.62

动态弯曲应力 dynamic bending stress

以规定的大小和与卡相关的方向周期性施加的弯曲应力。

3.63

尺寸稳定性 dimensional stability

当暴露在规定的温度和湿度条件下，卡抵御尺寸变化的能力。

3.64

可燃性 flammability

一旦点燃，卡维持和扩散火焰的能力。

3.65

表面粗糙度 surface roughness

表面区域的拓扑结构，在国际标准中参照不同的分辨率和计算方法进行规定。

4 机构及人员术语

4.1

银行卡交易交换网络 exchange network for bank card transaction

由机构、银行卡跨行信息交换系统以及网络设备 (如路由器等) 构成的，用于承载银行卡跨行业务的专用网络。

4.2

ICA 号 ICA number

ICA号是由国际组织给银行分配的一组6位的数字号码，其分配与银行标识代码（BIN）或发卡行标识代码（IIN）相关，通常用于标识清算或结算的实体。

4.3

银联标识 CUP logo

银联标识是由象征银联网络的图案和字符组成，经商标局注册，用于银联网络成员机构开展银联卡相关发卡和收单业务的标识。

4.4

发卡行 issuer

发卡机构 issuer

发行银行卡，维护与卡关联的账户，并与持卡人在这两方面具有协议关系的机构。

4.5

发卡行标识代码（IIN） issuer identification number (IIN)

银行标识代码（BIN） bank identification number (BIN)

标识发卡机构的代码。

4.6

部分迁移的发卡机构 early issuer

无法接收芯片卡交易信息，也不具备联机卡片认证能力，仅能接收磁条交易报文并处理现有报文域的发卡机构。

4.7

完全迁移的发卡机构 full issuer

能接收芯片卡交易信息，同时也具备联机卡片认证能力和接收芯片卡交易报文并处理报文域的发卡机构。

4.8

EMV 机构 EMVCo

由Europay组织、Mastercard组织和Visa组织共同创立的以合作确定EMV芯片卡协同规范和相关的认可手续的合法机构。

4.9

通信方 communicating party

发送或接收公钥，用于与公钥所有者通信的一方。

4.10

发起方 initiator

开始某一过程的节点或实体。

4.11

响应方 respondent

对一过程的发起者作出响应的节点或实体。

4.12

文件接收方 file acceptor

在文件收发过程中，将文件接收进来的一方。

4.13

文件发送方 file sender

在文件收发过程中，将文件传送出去的一方。

4.14

可信第三方 trusted third party

被通信实体了解并信任的通常可访问的实体。

4. 15
认证中心 (CA) certification authority (CA)
证明公钥和其他相关信息同其拥有者相关联的可信的第三方机构。
4. 16
从属认证中心 subject CA
由CA认证的认证中心 (CA)，并遵照CA的证书策略。
4. 17
账户历史数据 account historical data
在一定时期内，账户的金融交易记录（例如账户使用的次数，逾期还款等）。
4. 18
电话支付中心 telephone payment centre
为实现电话支付功能与服务而与电话支付终端完成信息收发等处理功能的中心。
4. 19
应用提供商 application provider
将各种所需组件装载至卡片提供完整应用的实体。应用提供商与持卡人有着直接的商业关系并向持卡人提供各种基于卡片的服务。
4. 20
封装机构 embedder
进行IC封装工作的实体。
4. 21
集成电路厂商 integrated circuit manufacturer
制作配有特定只读存储器的芯片厂商。
4. 22
ADF 个人化机构 (ADF) personalizer (ADF)
为IC中ADF分配的空间初始装载安全性参数和有关操作参数的实体。
4. 23
持卡人 cardholder
卡的合法持有者。
4. 24
个人识别码 (PIN) personal identification number (PIN)
个人密码 personal password
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。
4. 25
持卡者标识 cardholder identification
标识持卡者的代码。
4. 26
合法用户 authorized customer
可以合法进行交易的持卡人。
4. 27
授权者 grantor
具有授予访问权利的实体。
4. 28
操作员 operator

可以在终端设备上上进行一般维护与设置的合法者。

5 终端及设备术语

5.1

金融业务专用机具 special machines and tools for financial bussiness

根据银行或其他金融机构业务处理的特殊需要而设计和生产的专用机器设备和工具的总称。

5.2

终端 terminal

在交易点安装,用于与银行卡配合共同完成金融交易的设备。它应包括接口设备,也可包括其他的部件和接口(如与主机的通讯)。

5.3

终端标识码 terminal identification number

用于标识每一台销售点终端的唯一号码。

5.4

读磁条终端 magnetic stripe terminal

能够读取卡片磁条信息的终端。

5.5

IC卡终端 integrated circuit card terminal

能够处理集成电路卡的读取、通讯及进行交易的交易点终端。

5.6

脱机终端 offline terminal

不能处理联机授权请求的终端,包括仅脱机终端和有联机能力但无法进行通讯的终端。

5.7

联机终端 online terminal

以联机方式转发交易到后台系统的交易点终端。

5.8

授权终端 authorization terminal

安装在商户处用于请求或接收授权以完成卡交易的一种终端,其并不需要采集交易数据到支付系统。

5.9

自助终端 self-service terminal

客户自助使用,提供金融服务功能、交付或购买商品功能的终端。

5.10

无人值守支付终端 unattended payment terminal

在无人值守的环境下,可读取、采集并传输卡片信息的持卡人自助操作设备,如自动柜员机、自动加油机、发卡机、圈存设备等自助设备。

5.11

持卡人自助终端(CAT) cardholder-activated terminal (CAT)

持卡人自主地在终端(通常为无人值守的)上通过读取银行卡信息而获得商品或服务的设备。

5.12

银行自助设备 bank self-service equipment

银行提供,由客户自行完成现金交易、转账交易、账户查询等业务的专用设备,如自动取款机、自动存款机、自动存取款机、货币兑换设施、自助存储保险柜等。

5. 13

离行式 off-bank mode

自助设备设置在非银行营业场所的应用模式。

5. 14

在行式 in-bank mode

自助设备设置在银行营业场所的应用模式。

5. 15

穿墙式 through-wall mode

自助设备设置在建筑实体内，设备操作面穿出墙体，客户在建筑实体外操作使用的应用模式。

5. 16

大堂式 in-lobby mode

自助设备设置在储蓄所大厅、商场、宾馆大厅等地的应用模式。

5. 17

银亭 kiosk bank

安装在室外，不依附于任何建筑实体的自助银行的一种应用模式。具有封闭的设备防护区和客户操作区，对自助设备有一定的防护能力。

5. 18

收银终端 cash register terminal

在商户内部网络内，接受银行卡信息，具有通讯功能，接受柜员的指令完成金融交易信息和有关信息交换的设备，如商用第三代收银机或普通PC。

5. 19

金融税控收款机 fiscal cash register with EFT (electronic fund transfer) function

具有银行卡受理和税控功能的电子收款机。

5. 20

销售点终端 point-of-sale terminal

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报文和有关报文交换的设备，银行卡销售点终端简称为POS终端。

5. 21

自动柜员机 (ATM) automatic teller machine (ATM)

一种组合了多种不同金融业务功能的自助服务设备，合法用户可利用该设备所提供的功能完成存款、取款、信息查询等金融服务。

5. 22

ATM 保险柜 ATM safe

ATM中用于存放出钞模块、存款模块、数据安全模块等部件，并满足GB/T 18789-2002要求的保护外壳。

5. 23

数据安全模块 (DSM) data security module (DSM)

采用加密算法，实现数据安全功能的软件和硬件部件单元。

5. 24

出钞模块 (CDM) cash teller module (CDM)

ATM中存放现金并为合法用户实现取款交易时提取现金的部件单元。

5. 25

存款模块 deposit module

用于实现合法用户存入现金的部件单元。

- 5.26
终端控制模块 (TCM) terminal control module (TCM)
 终端的主控处理机。
- 5.27
凭条打印模块 (RPM) receipt print module (RPM)
 终端中为合法用户打印交易凭证的打印部件单元。
- 5.28
日志打印模块 (JPM) journal print module (JPM)
 ATM等自助设备记录工作状态的打印部件单元。
- 5.29
ATM 安全监控模块 ATM safety monitor module
 ATM中用于实现保安监视的部件单元。
- 5.30
多媒体功能模块 (MFM) multimedia function module (MFM)
 ATM中实现语音、图像等多媒体功能的部件单元。
- 5.31
后台维护模块 (ODM) operator's display module (ODM)
 终端中由银行管理员和维修人员使用的,用于公共支付终端系统维护、维修、诊断等的单元部件。
- 5.32
集成电路模块 integrated circuit module
 嵌入在IC卡中包括集成电路、集成电路载体、连线和触点的子装置。
- 5.33
存折打印模块 (BBPM) bank book print module (BBPM)
 用于打印客户存折的打印部件单元。
- 5.34
客户输入模块 (CIM) customer input module (CIM)
 终端中用于实现输入客户交易数据和管理员 (操作员) 维护数据的输入部件单元。
- 5.35
密码模块 cryptographic module
 硬件、固件、软件或一些它们的组合集,用来实现加密逻辑、加密过程,或同时实现上述两个功能。
- 5.36
密钥生成模块 key generation module
 用来生成和导出密钥的一种密码设备。
- 5.37
密钥装载模块 key loading module
 至少能存储一个密钥,并能在请求时将密钥传送到如IC卡或安全存取模块 (SAM) 等密码设备独立的电子元件。
- 5.38
电子柜 electronic cabin
 用于存放出钞模块、存款模块、数据安全模块之外的电子部件的外壳。
- 5.39
电子锁 electronic lock
 具有电信号触发、电磁定位、吸合或释放功能的电磁装置。

5.40

机械密码锁 mechanical lock

具有三个或四个转向轮的机械密码锁。

5.41

自动售油机 automatic fuel vending machine

通过服务站的加油器，接受支付并输出汽油的系统。

5.42

自动售货机 automatic vending machine

由持卡人操作的一种自助设备，直接提供商品给消费者，例如自助加油机。

5.43

现金存款机（CDM） cash deposit machine (CDM)

自动柜员机中的一种，合法用户可利用该设备实现存款等金融服务。

5.44

公共支付终端 public payment terminal

能够接收银行磁条卡或者金融IC卡信息，具有通讯功能，采用字符界面实现用户接入。并接受持卡人的操作指令而完成金融交易信息的有关信息交换的设备。

5.45

多媒体公共支付终端 multimedia public payment terminal

一种组合了多种不同金融业务的自助服务设备，采用多媒体手段实现用户接入。持卡人可利用该设备所提供的功能完成余额查询、密码修改、中间业务等非现金业务。

5.46

电话支付终端 telephone payment terminal

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。

5.47

用户移动终端 user mobile terminal

用于移动支付应用的手机终端或其他设备。

5.48

银行卡前置设备 prepositive facility of bank card network

位于各内部网络与银行卡跨行信息交换系统连接的接口处，实现信息识别、格式转换的一种网络接口设备。

5.49

持卡人接入设备 cardholder access device

持卡人用以发起一笔金融交易的终端设备或个人电脑，或是其他设备。

5.50

卡片读写设备（CAD） card acceptor device (CAD)

一种用来在卡上读写信息的硬件设备。

5.51

磁条阅读器 magnetic stripe reader

能够读取卡片磁条信息的设备。

5.52

IC卡读写器 ICC reader and writer

用于对IC卡上的信息进行存取的设备。

5.53

PIN 输入设备 (PED) PIN entry device (PED)

对PIN进行加密处理以保护PIN安全的设备。PIN输入设备应具有明确的物理和逻辑定义,并具有抗攻击或防攻击特性的外壳。

5.54

密码键盘 (EPP) encrypting PIN pad (EPP)

用于保护PIN输入安全,并对PIN进行加密的设备。密码键盘应有明确的物理和逻辑定义,并具有抗攻击或防攻击特性的外壳。

5.55

安全加密设备 (SCD) secure cryptographic device (SCD)

能提供一系列安全加密服务,具备物理和逻辑保护的硬件设备。

5.56

防攻击设备 tamper-evident device

一种使用在 PIN 加密与密钥管理体系中防攻击的安全设备,通过该设备可以发现任何企图渗入的操作。通过该设备,渗透性攻击不能获得之前输入的任何 PIN 或保密密钥的信息。

5.57

硬件安全装置 (PSD) physically secure device (PSD)

一种用以保护存储在设备里的任何加密密钥或PIN不受渗透性攻击的安全模块。在受到渗透性攻击时,硬件安全装置将立即自动擦除设备中的所有PIN、加密密钥及它们的所有残余部分。只有其内部操作不能也不会被外部操作所修改的设备才被认为是硬件安全装置。

5.58

接口设备 (IFD) interface device (IFD)

终端上插入IC卡的部分,包括其中的机械和电气部分。

5.59

邻近式耦合设备 (VCD) vicinity coupling device (VCD)

用电感耦合给VICC提供功率并控制与VICC数据交换的读/写设备。

5.60

接近式耦合设备 (PCD) proximity coupling device (PCD)

用电感耦合给PICC提供能量并控制与PICC交换数据的读/写设备。

5.61

接近式支付设备 proximity payment device

使用无线接口访问账户的一种支付工具。要求具备明确的商标、制造商和技术要求规范,并能够支持完成接近式支付交易。包括非接触设备、移动电话和微感应器。

6 业务及应用术语

6.1

EMV 标准 EMV standard

EMVCo制定和维护的标准,简称为EMV标准。

6.2

IC 的封装 IC embedding

将IC组件封装入卡中,使之成为集成电路卡的处理过程。

6.3

IC 的组装 IC assembling

将一个或多个IC与外部通信元件组装成一个适合于IC嵌入模块的处理过程。

6.4

IC 组件 IC assembly

适合于IC嵌入的、包含一个或多个IC和外部通信元件的模块。

6.5

ADF 分配 AD Fallocation

对应用提供者后续使用IC空间的安全规定。

6.6

IIN 的块 block of IINs

发卡行标识代码（IIN）注册簿中保留的由两个或多个IIN组成的序列，以便管理的或卡模式的块持有者进行分配。

6.7

系统跟踪审计号 system trace audit number

由报文发送方定义的唯一标识交易号码，该号码在整个交易期的全部报文中都保持不变。

6.8

交易参考号 transaction reference number

由收单行分派的、用来查询交易并在随后的报表中跟踪该查询的一个唯一字符代码。

6.9

POS 参考号 POS reference number

POS中心为交易分配的流水号，在响应报文中下传给POS终端作为对账参考号，并用于事后查证。

6.10

POS 交易批次号 POS transaction batch number

POS从签到起至结算、签退为止的交易为一批次，一个交易批次号标识一批交易。签到时由POS中心为该POS产生新的批次号，在签到响应报文中下传给POS。

6.11

POS 流水号 POS trace number

POS为每一笔交易产生的顺序编号。POS每上送一次交易此号码增加1。POS流水号为6位数字，值从1至999999循环使用。

在自动冲正时，POS中心依据POS流水号作为确定被冲正交易的要素之一。

POS流水号也作为交易凭证号，在进行退货、撤销等交易时，输入原交易凭证号作为确定原交易的要素之一，并且应上送原交易的凭证号。

6.12

POS 输入方式 entry mode of POS

按业务要求，POS有挥卡、插卡、刷卡及手工输入方式。

6.13

金融交易 financial transaction

持卡人通过银行卡账户完成的消费、存款、取款、转账结算等行为。

6.14

通讯服务 communication service

一种在用户之间传送报文的的服务，包括用其他方式清算的资金转账交易。

6.15

单信息交易 single message transaction

一笔交易被发送一次，同时用于授权、清分和结算，此类交易也称“全金融交易”。授权、清分和结算全部在线发生。

6.16

双信息交易 dual message transaction

一笔交易被发送两次，第一次仅用于授权，第二次的附加信息用于清分和结算。即授权实时处理、清分和结算非实时处理。

6.17

国内交易 domestic transaction

同一国家内机构之间进行的交易。

6.18

本地交易 local transaction

发生在发卡行所在地区的交易。

6.19

本地交易凭证 local transaction receipt

用来标明本地交易的交易凭证。

6.20

本地结算 local settlement

在本地交易中进行的结算。

6.21

本地授权 local authorization

本地交易进行的授权。

6.22

本行交易 on-us transaction**本代本交易** on-us transaction

发卡行与收单行为同一家银行的交易。

6.23

跨地区交易 interregional settlement

发生在发卡行所在地区之外的交易。

6.24

跨地区结算 interregional interchange

在跨地区交易中进行的结算。

6.25

跨国交易 international transaction

发生在发卡行所在国家之外的交易。

6.26

跨行转账 inter bank transfer

不同银行发行的银行卡之间互相转移资金。

6.27

IC卡交易 ICC transaction

通过终端使用IC卡进行的交易。

6.28

接近式支付交易 proximity payment transaction

有卡环境下，通过交易点无线接口完成的支付交易，包括由非接触设备、移动电话或微感应器完成的交易。

6.29

完整的芯片卡交易 whole chip card transaction

芯片卡按照JR/T 0025借记/贷记交易的完整流程进行的交易。

6.30

联系发卡行交易 refer to issuer transaction

由发卡行或经由代授权处理发起的对一笔授权请求的响应，该交易要求收单行直接联系发卡行。

6.31

简化的芯片卡交易 simplified chip card transaction

应用选择后，仅执行初始化应用和读应用数据，在得到满足交易的信息后，按处理磁条的流程进行交易，而不进行后序芯片卡处理的交易。

6.32

降级使用交易 fallback

当芯片卡在具有芯片能力的终端上交易，由于芯片卡不能正常工作或芯片终端不能正常工作时，终端指使持卡人通过刷磁条进行的交易。降级使用的交易必须得到发卡机构的授权。

6.33

金融类撤销交易 financial transaction cancellation

对已成功的金融交易，在一定条件下可对其进行取消，在结算前退还原始交易金额。撤销交易必须是对原始金融交易的全额撤销。

6.34

建立/撤销委托关系交易 setup/cancellation clientage transaction

用于建立/撤销持卡人、发卡行和服务提供商之间针对某种服务项目的委托关系。

6.35

有卡环境 card-present environment

面对面交易或自助交易的环境。

6.36

无卡环境 card-absent environment

在持卡人及卡片都不在现场情况下完成交易的一种环境。该环境下的交易包括：电子商务交易、网购或电话订购交易、代收付、电话服务交易等，但不包括面对面交易。

6.37

代理业务 agent service

发卡机构受公用事业机构、商业机构、企事业单位等收付方委托，办理的收费、发放现金等交易业务，如代收公用事业费（水、电、煤气）、代发工资、代交电话费、售票、缴税、证券交易等。

6.38

代收交易 collection

发卡机构受公用事业机构、商业机构、企事业单位等收款方委托，从持卡人账户中扣款的交易。

6.39

代付交易 agency payment

发卡机构受公用事业机构、商业机构、企事业单位等付款方委托，向持卡人账户中存款的交易。

6.40

代授权 stand-in authorization

银行卡清算组织在与发卡机构签订的代授权协议约定条件下，代替发卡机构完成交易授权应答的业务处理过程。

6.41

请求类交易 request transaction

从交易的请求方（如：受理方）发送至接收方（如：发卡机构），告知对方有一笔交易正在进行，并且完成该交易后需要回送响应。接收方接收到交易请求后应直接给予交易批准或拒绝的应答。如果交易的接收方不是该交易的最终接收机构，则接收方负责将交易向下一机构转发。

6.42

贷记交易 credit transaction

持卡人贷记其账户的资金要求。同时，它提供代理方（和/或受卡方）确认的应支付给发卡机构资金的详细资料。

6.43

借记交易 debit transaction

持卡人对借记其账户的认可。同时，它提供代理方（和/或受卡方）向发卡机构索取资金的权利。

6.44

转账 transfer

其一个账户向另一个账户的资金转移。

6.45

转入确认 transfer-in confirmation

银行卡清算组织在限定时间内接收不到转入方对转入转账请求的应答或转入转账应答未通过合法性检查时，向转入方发送的请求确认的交易。

6.46

第三方转账 third-party transfer

受益人不是发送方或接收方的转账交易。

6.47

撤销转账 reversal transfer

撤销前一笔转账而引起的借记和贷记。

6.48

查询余额 balance inquiry

持卡人进行相关账户余额查询的交易。

6.49

查询明细 detail inquiry

持卡人查询交易明细记录的交易。

6.50

现金充值 cash replenishing

持卡人通过现金充值终端将现金存入IC卡电子钱包或电子现金账户的交易。

6.51

分期付款 installment

持卡人使用贷记卡购买商品或服务时，在发卡行提供的分期付款期数选择范围内，按照与发卡行协议商定的还款计划，将商品总价分成若干期，每月向发卡行支付当期应付货款，直至商品总价清偿完毕为止的一种交易。

6.52

延迟付款 delayed payment

为有效规避欺诈风险，收单机构暂时延迟支付其认为的可疑交易款项给特约商户。

6.53

授权 authorization

根据定义的操作准则，发卡行（或其代理）对一笔交易的批准，商户通过电话或是授权终端接收该批准并处理该笔交易。

6.54

授权交易 authorization transaction

在双信息交易中，由受理方引发向发卡机构索取付款承诺，发卡机构根据持卡人账户情况返回应答信息的过程。

6.55

授权参考 referral call

发卡行对收单行授权请求的一种回应，要求收单行致电发卡行以便于发卡行确认是否批准该交易。

6.56

授权参考号 authorization reference number**授权号 authorization number****授权码 authorization number**

由发卡行或是授权机构分派的一个6位的数字字母参考号，用以标识特定的授权交易。

6.57

授权撤销交易 authorization cancellation transaction

在双信息交易中，受理方由于持卡人取消交易、以其他方式支付或商户自身原因而通过POS或其他方式、经由银行卡清算组织通知发卡机构取消付款承诺的过程。

6.58

部分授权 partial authorization

发卡行发出的授权响应，其授权金额小于参与部分授权服务的商户所请求的金额。

6.59

授权请求 authorization request

收单行向发卡行发送的要求准予完成支付卡相关交易的请求。

6.60

授权日志 authorization log

每日或每周用来记录授权交易明细的日志。

6.61

授权响应 authorization response

授权请求的答复，通常为的一组代码，它能够告知收单行或者商户如何处理该笔交易。

6.62

预授权 pre-authorization

特约商户通过POS或其他方式，就持卡人预计支付金额向发卡行索取付款承诺的过程。

6.63

预授权撤销 pre-authorization cancellation

特约商户由于各种原因通过POS或其他方式通知发卡行取消付款承诺的过程。

6.64

预授权完成 pre-authorization completion

持卡人对已取得预授权的交易，在预授权金额或超出预授权金额一定比例的范围内，做支付结算的交易。

6.65

预授权完成（请求）交易 pre-authorization completion transaction (request)

特约商户对已取得预授权的交易，在预授权金额或超出预授权金额一定比例的范围内，通过POS终端将交易信息实时提交发卡机构完成持卡人付款的交易。

6.66

预授权完成（手工） pre-authorization completion (manual)

特约商户对已取得预授权交易，在预授权金额或超出预授权一定比例的范围内，通过手工方式完成持卡人付款的过程。受理方可以在差错处理平台上提交手工结算，银行卡清算组织在收到差错处理平台的预授权完成（手工）请求后会向发卡机构发送预授权完成（手工）通知报文。

6. 67

预授权完成（通知）交易 pre-authorization completion transaction (advice)

特约商户对已取得预授权的交易，在预授权金额或超出预授权金额一定比例的范围内，通过POS终端非实时提交发卡机构以完成持卡人付款的交易。

6. 68

预授权完成撤销 cancellation of pre-authorization completion

特约商户由于各种原因对已经成功的预授权完成交易，于当日当批主动发起的取消行为。

6. 69

追加预授权 supplementary pre-authorization

当前面的预授权已获批准，为达到在原预授权金额的基础上追加预授权金额的目的所发起的一个或多个后续预授权。

6. 70

ATM 查询 ATM inquiry

持卡人在ATM上做相关账户余额查询的行为。

6. 71

ATM 取现 ATM cash withdraw

持卡人在ATM上提取现金的行为。

6. 72

ATM 授权 ATM authorization

发卡行（或其代理机构）对收单行（或受理方）给予的认可或保证。

6. 73

加钞周期 cash replenishment period

现金托管机构对ATM进行两次加钞之间的时间定义为一个加钞周期。

6. 74

安全电子商务交易 secure electronic commercial transaction

通过一种认证模式鉴定的电子商务交易。

6. 75

批准 approved

发卡行（或其代理行）批准一笔交易的授权响应，此授权响应发送给收单行，由收单行转发给商户。

6. 76

冲正 reversal

一种特殊的交易。由报文的发送方发起，用于通知接收方先一笔授权类或金融类交易没有按预定流程完成，应该取消其处理结果。

6. 77

退货 refund

特约商户因商品退回或服务取消，将已扣款项退还持卡人原扣款账户的过程，包括全额和部分金额退货。

6. 78

托收 collection

由于提交程序或时间等问题，导致入网机构或商户不能将可确认的真实的跨行交易数据提交统一清算时，入网机构提请中国银联或其他入网机构协助进行的尝试收款。

6.79

分单 split transaction

同一张银行卡在同一家商户的同一终端，购买同一商品（或服务）为逃避发卡行授权管理等限制性条件而发生连续两次（含）以上交易的支付行为。

6.80

清分 clearing

对交易数据依据机构和交易类型进行分类汇总，并计算结算金额的过程。

6.81

清算 settlement

根据清分结果对交易数据进行净额轧差和提交并完成资金划拨的全过程。

6.82

自主清算 self-determination settlement

两个机构之间的一种清算约定，当清算由一方发起并以该方的数据为准时，该方称该类交易为自主清算。

6.83

非自主清算 unself-determination settlement

两个机构之间的一种清算约定，当清算由一方发起并以该方的数据为准时，另一方称该类交易为非自主清算。

6.84

清算日 settlement business date

清算系统处理相关机构提交交易的日期。

6.85

清算数据 settlement data

清分后用于资金划拨和对账的交易数据。

6.86

清算账户 clearing account

清算机构用来接收银行的网络结算借贷交易的账户。

6.87

清算滞纳金 settlement late fee

清算组织因其成员机构未能于限期内完成银行清算金额转账而向成员机构收取的费用。

6.88

货币清算服务 intracurrency settlement service

一种清算服务，允许在不同的国家或在同一个国家内协议单位以及转发代理机构根据相互认定的汇率来进行清算。

6.89

资金结算交易 settlement transaction

在日切后，银行卡清算组织根据当日日志计算各入网机构当天的借贷交易笔数、金额及手续费，将计算结果告知入网机构的通知类交易。

6.90

差错交易 adjustment

由于机具、通信线路、系统处理及终端操作等原因引起，需要进行账务调整的交易。

6.91

确认查询 confirmation inquiry

发卡行为解决持卡人确认原始交易的需要而提起的查询请求，属于差错处理的一种交易类型。

6.92

贷记调整 credit adjustment

收单行对确认的长款向发卡行主动提出退款的请求，属于差错处理的一种交易类型。

6.93

请款 presentment

收单机构对原始交易的短款和贷记调整失误而向发卡机构提出的索款请求，属于差错处理的一种交易类型。

6.94

一次请款 first presentment

收单行向发卡行发起的初次请款。

6.95

再请款 re-presentment

收单机构或商户对发卡机构一次退单交易有异议而向发卡机构提出的再次索款请求，属于差错处理的一种交易类型。

6.96

退单 chargeback

发卡机构由于对收单机构请款交易的拒绝或对原始交易的疑问而向收单机构提出的拒绝付款，属于差错处理的一种交易类型，包括一次退单和二次退单。

6.97

一次退单 first chargeback

发卡行由于对收单行请款交易的拒绝或对原始交易的疑问而向收单行提出的拒绝付款，属于差错处理的一种交易类型。

6.98

二次退单 second chargeback

发卡行由于对收单行的再请款交易的异议而向收单行再次提出的拒绝付款，属于差错处理的一种交易类型。发卡行对借记卡交易和信用卡ATM交易没有二次退单权。

6.99

争议 dispute

入网机构之间通过正常差错处理流程（交易双方除例外交易、确认查询以外的差错处理权利已全部行使完毕，或超过时限不得再行使）仍未解决，或入网机构一方证明另一方违反规定造成己方损失但无法通过差错处理解决的各种交易纠纷。

6.100

调单 retrieval

因持卡人或发卡机构对已被清算的交易有疑问，在规定的时间内由发卡机构向收单机构和商户提出调阅交易单据的过程，属于确认查询的一种。

6.101

调单回复 retrieval response

受理方对发卡机构调单请求的回复。

6.102

调单展期 retrieval postponement

因内部处理环节过多或其他原因，导致调单回复方无法在规定时限内完成的，可以在最后回复期满前发起延长回复期限请求。

6.103

协商解决 negotiated solutions

协商解决是争议的任何一方在提出争议前，向对方提出书面通知，双方协商、解决争议的过程。

6.104

例外处理 exception

差错例外处理 exception

差错双方利用差错处理平台专用渠道，协商、处理正常差错处理流程无法解决差错交易的过程。

6.105

例外协商交易 exception consultation

对无法通过正常差错处理流程解决或经过正常差错处理流程后仍有疑问的交易，差错处理双方利用差错处理平台提供的专用渠道，对该类差错的处理进行联络、沟通和协商，属于差错例外处理的步骤之一。

6.106

例外长款处理 exceptional surplus processing

对无法通过正常差错处理流程解决或经过正常差错处理流程后仍有疑问的交易，差错双方经协商后，长款一方统一并主动发起的付款行为，属差错例外处理的步骤之一。

6.107

例外协商回复 exception consultation response

例外协商交易适用于已经超过差错处理期限、交易未清算、处理中心无记录、差错流程已经结束的交易。由发现账务差错的一方提出例外协商，例外协商的接收方对该笔例外协商交易进行回复，表明是否同意协商的内容，若双方能够达成一致，则长款方可以通过差错例外交易付款。

6.108

裁判 arbitrage

通过差错处理或协商均不能解决的交易纠纷，联网入网机构向争议处理机构提出申请，争议处理机构裁定责任承担方的过程。

6.109

交易成功率 transaction success ratio

成功交易笔数占总交易笔数的百分比。

6.110

交易点 point of transaction

销售点 point of sale

服务点 point of service

商户或收单行（在面对面交易环境中）或自助终端（在自助环境中）完成交易的实际位置。

6.111

交易国家 transaction country

无论发生交易时持卡人的所在地在何处，进行交易商户所在的国家称之为交易国家。当交易在飞机或游轮航线上完成时，交易国家为交易商户存放交易收据保证金的国家。

6.112

动态币种转换 dynamic currency conversion

在持卡人和商户都同意的前提下，将购买的商品或服务从一个币种转换为另外一个币种。

6.113

交易计数器 transaction counter

用于记录卡片交易次数的计数器。

6.114

交易记录明细 transaction audit trail

特定结算日所有交易明细的列表。

- 6.115
交易金额 transaction amount
 在交易双方之间转账的资金数额。
- 6.116
交易类型代码 transaction type code
 确定交易的性质、目的和/或原因的代码。
- 6.117
交易日期 transaction date
 持卡人与商户发生交易的日期。
- 6.118
交易日志 transaction log
 记录最近交易的信息细节，从中可以了解交易历史。
- 6.119
交易信息文档 transaction information document
 交易信息的所有类型，包括各种表单、销货单、凭证、终端收据、费用记录和代用汇票等。
- 6.120
私有协议 private agreement
 适用于对内部交易进行授权、清算和结算的成员间双方协议或成员组操作规范。
- 6.121
凭证 receipt
凭条 voucher
 由终端生成的印有相关交易信息的凭证。
- 6.122
商户退单比率 merchant chargeback rate

$$\text{商户退单比率} = \frac{\sum \text{商户本月内收到的退单交易金额}}{\sum \text{商户本月的收单交易金额}}$$
- 6.123
电子存折 (ED) electronic deposit (ED)
 一种为持卡人进行消费、取现等交易而设计的支持个人识别码 (PIN) 保护的金融IC卡应用。它支持圈存、圈提、消费和取现等交易。
- 6.124
电子钱包 (EP) electronic purse (EP)
 一种为方便持卡人小额消费而设计的金融IC卡应用。它支持圈存、消费等交易。消费不支持个人识别码 (PIN) 保护。
- 6.125
电子现金 (EC) electronic cash (EC)
 基于借记/贷记应用上实现的小额支付功能。
- 6.126
电子资金转账 (EFT) electronic funds transfer (EFT)
 由终端、计算机、电话等设备发起的一种无纸化资金转账。
- 6.127
费用 charge
 与金融服务有关的各种手续费。

6.128

处理费 processing fee

在交易数据交换的过程中，由发卡行或收单行向该银行卡清算组织支付的费用，该费用由交易种类决定。

6.129

安全处理费用及酬劳 security handling fee and reward

发卡行因收单行截留丢失卡或被盗卡而支付给收单行的费用。

6.130

交易费 transaction fee

对交易行为收取的费用（例如，代理方收取的费用）。

6.131

可用资金 available fund

可用于消费、转账或提现的资金。

6.132

即用资金 immediate fund

清算和交易执行同时进行的同日资金。

6.133

风险备付金 risk reserve fund

为防范支付风险，未达到信用及清算风险标准的成员机构按银行卡清算组织要求缴纳，并存放于银行卡清算组织指定账户的资金。

6.134

占挂资金 held amount

在清算点，由于争议，商业决策或是政府限制而未被进行清算处理的资金。

6.135

信用额度 credit line

发卡行在批准发放贷记卡或者准贷记卡时给予的一个最高透支的限额。

6.136

信用卡透支 overdraft of credit card

发卡机构授予持卡人一定的信用额度，持卡人可在信用额度内进行支付或取现，从而获得银行短期信贷资金的行为。

6.137

免息期 interest-free period

享受免息服务的交易，在交易日（银行记账日）至到期还款日之间的时间。

6.138

持卡人折扣 cardholder discount

商户优惠给持卡人的消费折扣。

6.139

补充明细 supplementary details

提供给持卡人的对账单个别项目的附加信息。

6.140

超时限值 timeout value

从授权请求发起到响应之间最大的时间限值。如果超过了这个时间限值，交易请求将被自动取消。

6.141

测试方法 test method

为了证实识别卡和相关接口设备符合若干标准而对其特性进行测试的方法。

6.142

个人化 personalization

相关部门用意义的白卡变为具有个人特殊意义的可用卡的过程。

6.143

卡片复制 card reproduction

卡片的重新复制。

6.144

主应用 primary application

多应用卡中与卡面应用标识相一致的应用，一张卡片只能有一个主应用。

6.145

应用标签 application label

根据GB/T 16649.5标准中与应用标识（AID）相关联的名称，用于应用选择。应用标签在应用定义文件（ADF）的文件控制信息（FCI）中可选（推荐要求），在ADF目录入口中必须存在。

6.146

应用标识（AID） application identifier (AID)

由注册的应用提供商标识符（RID）以及扩展的专用应用标识符（PIX）组成。

6.147

注册的应用提供商标识（RID） registered application provider identifier (RID)

应用标识符的一部分，由国际标准组织注册管理组（ISO RMG）分配，其由5位16进制的字节组成。

6.148

应用首选名称 application preferred name

与应用标识（AID）相关联的应用名称。如果应用首选名称存在且终端支持发卡行代码表索引指示的语言，则应用选择过程中显示给持卡人的应用名称应采用应用首选名称，而不是应用标签。

6.149

圈存 load

金融IC卡持卡人将其在银行账户上的资金划转到卡片上的电子钱包、电子存折或电子现金中。

6.150

自动圈存 auto-load

发卡机构根据持卡人预先协议，在处理电子现金联机交易时，对符合条件的直接通过返回脚本方式将电子现金余额进行更新的交易。

6.151

关联圈存 linked load

提供电子钱包的账户和提供资金的账户为相同账户的一种电子钱包圈存交易。

注：仅发送一笔交易，用以认证电子钱包和对圈存金额进行担保。

6.152

非关联圈存 unlinked load

提供电子钱包的账户和提供资金的账户不是同一账户的一种电子钱包圈存交易。

6.153

指定账户圈存 specific account load

持卡人通过圈存终端主动发起，将预先与电子现金绑定的借记卡或贷记卡中资金（或额度）划入电子现金的交易。

6.154

非指定账户圈存 load on unspecified account

持卡人通过圈存终端主动发起，将任一借记卡中资金划入电子现金的交易。

6.155

圈存交易凭证 load transaction receipt

持卡人在自动柜员机（ATM）或圈存设备上充值而产生的交易凭证。

6.156

圈提 unload

持卡人将其在电子存折或电子现金中的部分或全部资金划回其在银行的相应账户上。

6.157

卡片“发卡后”应用更新 post-issuance updates

允许发卡行更新已发行的卡片信息的方式。通常有两种更新方式：“发卡后”应用修改和“发卡后”应用装载。

6.158

“发卡后”应用修改 post-issuance application change

允许发卡行修改或锁定已经存在于芯片中的应用的方式。

6.159

“发卡后”应用装载 post-issuance application load

允许发卡行在已发行的卡片中添加应用或服务内容的方式。

7 信息交换术语

7.1

保护时间 guard time

同一方向发送的前一个字符奇偶位下降沿和后一个字符起始位下降沿之间的最小时间。

7.2

短连接 transitory connect

通信双方每次通信时建立，通信结束后关闭的连接。

7.3

长连接 persistent connect

通信双方建立后不再关闭，在通信正常情况下一直保持连通状态，双方在收发数据时不再重新建立连接。

7.4

初始文本序列 initial text sequence

n位的二进制向量，可以作为报文前缀。

7.5

串联 concatenation

通过把第二个元素的字节添加到第一个元素的结尾将两个元素连接起来。每个元素中的字节在结果串中的顺序和原来从卡片发到终端时的顺序相同，即高位字节在前。在每个字节中位按由高到低的顺序排列。

7.6

磁条镜像 magnetic stripe image

用复制磁条信息处理IC卡兼容交易的最小芯片支付数据。

7.7

类型 ABC class ABC

卡片和终端支持的供电电压值类型。有三种可以支持的供电电压类型：类型A=5.0伏，类型B=3.0伏，类型C=1.8伏。卡片和终端可以支持其中的一种，也可以支持连续的两种或两种以上的供电电压，如AB、ABC。

7.8

热复位 warm reset

在时钟（CLK）和电源电压（VCC）处于激活状态的前提下，IC卡收到复位信号时产生的复位。

7.9

冷复位 cold reset

当提供给IC卡的电源电压和其他信号从静止状态中复苏且收到复位信号后，IC卡产生的复位。

7.10

位冲突检测协议 bit collision detection protocol

在帧内比特级使用冲突检测的防冲突方法。冲突出现在至少两个PICC把互补位模式发送给PCD时。在这种情况下，位模式被合并，在整个（100%）位持续时间内载波以副载波来调制。PCD检测出冲突位并按串联次序识别所有的PICC ID。

7.11

静止状态 inactive

当IC卡上的电源电压（VCC）和其他信号相对于地的电压值小于或等于0.5伏时，则称电源电压和这些信号处于静止状态。

7.12

时间槽协议 time slot protocol

PCD与一个或多个PICC建立逻辑通道的方法，该方法对于PICC响应使用时间槽定位，类似于slotted-Aloha方法。

7.13

直联 direct connection

银行卡受理终端设备直接接入中国银联前置系统加入银联网络的模式。

7.14

间联 indirect connection

银行卡受理终端设备通过入网机构系统接入银联网络的模式。

7.15

联机交易 online transaction

由受理方、交换中心和发卡机构通过报文实时转接并处理完成的交易。

7.16

联机方式 online mode

进行交易时需与主机（host）或系统发生直接联系（通过有线或无线等通信方式与其他设备和系统交换信息），为合法用户完成交易的一种工作方式。

7.17

脱机方式 offline mode

终端进行交易时不与主机（host）或系统发生直接联系（不通过有线或无线等通信方式与其他设备和系统交换信息），为合法用户完成交易的一种工作方式。

7.18

应用 application

卡片和终端之间的应用协议和相关的数据集。

7.19

响应 response

处理所接收到的命令后返送给发起方报文的动作。

7.20

响应时间 response time

由终端生成报文的最后一个字节到收到响应的第一个字节所花费的时间,包括终端和网络延时所花费的时间。

7.21

响应码 response code

应答码 response code

接收方接收到请求或通知后,返回给发送方表示处理结果的代码。

7.22

命令 command

一个发出动作的请求或通知的报文。

7.23

交换 exchange

两个或多个不同实体或机构之间在双方约定的基础上(卡所产生的或激活的)交易数据的互换。

7.24

金融报文 financial message

用于金融机构(或其代理)之间交换信息的数据元集合,该类报文不设定或标识任何通信(头或尾、协议或字符码)或与保密有关的内容。

7.25

报文类型代码 message type code

用于指明报文的作用和/或要求,采取行动的代码。

7.26

报文标识符(MID) message identifier (MID)

发送方用来唯一标识金融报文的数据。

7.27

报文功能 message function

对报文的目 的及其涉及活动的标识。

7.28

报文位图 message bit map

用于标识报文中每个数据元存在(用1表示)或不存在(用0表示)的一系列位。

7.29

报文摘要 message digest

数字指纹 digital fingerprint

哈希算法对原始报文进行运算,得到的一个固定长度的数字串。

7.30

交易报文 transaction message

用于传递相关金融交易信息的报文。

7.31

授权报文 authorization message

在支付系统中,受理方和发卡行之间传输的,确立发卡行是否允许交易批准的报文。

7.32

交互报文 interactive message

发生交易时所发送的、要求响应的报文。

7.33

通知报文 advice message

发送方将已采取的动作通知接收方的报文，不要求认可，但要求响应。

7.34

响应报文 response message

原始请求或通知报文的接收方告知发送方该请求报文或通知报文已收到的报文。

注：该响应表示接收方采取了什么样的动作来完成原始的请求或通知。

7.35

撤销 reverse

通知原始的报文发送者交易不能按指令处理，即不能发送、不可处理或被接受方取消的报文。

7.36

重复 repeat

在预计期限内未收到回复的请求和通知报文的再发送。

7.37

再提交 resubmission

重新提交一个以前被否定或拒绝的请求报文。

7.38

报文转发 message forwarding

从某一成员接收报文，将其路由至中央处理站点（如需要，该站点可存储并修改报文信息）并发送至其他成员的技术。

7.39

存储转发 store and forward

发送方将报文存放在存储转发队列中，在一定次数内每隔一段时间重复发送。

7.40

处理优先级 processing priority

发送方要求接收方处理报文的紧急等级。

7.41

处理优先级代码 processing priority code

规定请求处理优先级的代码。

7.42

校验码 check code

附加在本体码后，用来验证本体码在机器中生成、存储和传输过程正确性的代码。

7.43

商户类别代码 merchant category code

根据商户业务、贸易和服务类型对商户进行分类，标识每一类别的代码称为商户类别代码。

7.44

促销代码 promotion code

由发卡行指派的一个代码，用于标识发卡行所推出的鼓励银行卡使用的某类促销项目。

7.45

服务点输入方式码 point of service entry mode

持卡人数据（如主账号和个人识别码）输入方式的代码。

7.46

服务代码 service code

发卡机构用来指明卡片可允许交易参数的3位数字。

- 7.47
无法识别的服务代码 unrecognized service code
 不能被磁条终端设备或芯片读取设备识别的服务代码。
- 7.48
公共服务平台 public service platform
 面向入网机构的基于Internet的服务平台，该平台能够提供与转接业务相关的差错、报表服务等功能。
- 7.49
公共支付平台（PPP） public payment platform (PPP)
 进行联机交易处理时，与公共支付终端建立通信连接的通信前置机和业务主机，其能够接受、处理和转发公共支付终端的交易请求信息，并向公共支付终端回送交易结果信息。
- 7.50
差错处理平台 adjustment platform
 用于联网成员间提交差错交易以解决跨行交易差错及疑问的电子处理系统。
- 7.51
电子资金转账系统（EFTS） electronic fund transfer system (EFTS)
 无需纸质证明的，通常能够完成资金转账的电子系统。
- 7.52
交易点的电子资金转账 electronic fund transfer at point-of-transaction
 在销售商品及提供服务的地点通过电子资金转账（EFT）对所购买商品及服务进行支付交易的技术。
- 7.53
卡支付系统 card payment system
 能支持银行卡支付的支付系统。
- 7.54
单一 IC 系统 IC-only system
 仅依赖IC技术和相应的接口设备的卡系统。
- 7.55
ATM 前置处理系统（ATMP） automatic teller machine front-end processing system (ATMP)
 进行联机交易处理时，与ATM终端建立通信连接的通信前置机或业务主机，其能够接受、处理或转发ATM终端的交易请求信息，并向ATM终端回送交易结果信息。
- 7.56
销售点系统 point-of-sale system
 在零售点或接近零售点的地方，接收金融交易数据，并将数据传输至计算机或授权网络以通知交易行为、授权和交易日志记录的电子系统。
- 7.57
POS 前置处理系统（POSP） POS front-end processing system (POSP)
 接受、处理或转发银行卡的交易请求信息，并向终端回送交易结果信息的前置系统。
- 7.58
不良商户系统 system of delinquent merchant
 管理信用度低于联网联合基本要求的银行卡商户信息的计算机系统。
- 7.59
不良持卡人系统 system of delinquent cardholder
 管理信用度低于联网联合基本要求的银行卡持卡人信息的计算机系统。

- 7.60
止付名单系统 system of stop payment name list
管理应止付的银行卡信息系统。
- 7.61
数字签名系统 digital signature system
提供数字签名生成和验证的非对称密码系统。
- 7.62
系统成功率 success ratio of system
系统成功交易笔数占总交易笔数的百分比。
- 7.63
支付网关 payment gateway
在电子商务交易中为商户提供授权和清算的电子商务服务系统。
- 7.64
收单网关 acquiring gateway
在电子商务交易中，由收单机构或其处理器所使用的协议所指定的软件程序。收单网关的功能是将报文从安全电子交易（SET）协议转换成客户接口规范（GB/T 15150）或其他收单机构所要求的POS报文格式。
- 7.65
批准响应 approval response
批准交易的授权响应。
- 7.66
支付系统环境（PSE） payment system environment (PSE)
当符合JR/T 0025的支付系统应用被选择，或者用于支付系统应用目的的目录定义文件（DDF）被选择后，IC卡中所确立的逻辑条件集合。
- 7.67
标签、长度、数值（TLV） tag, length, value (TLV)
由国际标准组织（ISO）定义，用以标明和定义芯片卡中的数据的标准结构。这些结构包括：标签即数据对象标识符，长度即压缩字节的长度，数值即标签实际的数据标识符。
- 7.68
基本文件 elementary file
可包含数据和/或文件控制信息的文件。
- 7.69
主文件（MF） master file (MF)
描述根文件结构的唯一且强制的专用文件。
- 7.70
专用文件（DF） dedicated file (DF)
包含文件控制信息，并且可包含用来分配的存储空间的文件。它可以是EF和（或）DF的父文件。
- 7.71
目录定义文件 directory definition file
用来认定专用文件的文件名与关联目录的数据元。
- 7.72
应用基本文件（AEF） application elementary file (AEF)

在JR/T 0025芯片目录结构中，位于应用定义文件（ADF）下一层级的文件。这些文件包含应用所必需的用户数据。组成某一特殊应用的所有应用基本文件（AEF）共享相同的专用文件。一个应用基本文件（AEF）不能成为其他文件的父文件。

7.73

应用定义文件（ADF） application definition file (ADF)

提供指向一个或多个应用基本文件（AEFs）入口的文件。应用定义文件（ADF）标明了一个应用，并包含了在应用选择过程中，读取芯片终端所使用的重要数据。应用定义文件的树形结构提供以下功能：连接应用文件至一个应用中，隔离不同应用，允许通过应用定义文件（ADF）选择访问该应用的逻辑结构。

7.74

短文件标识符 short file identifier

用作缩略文件标识符的数据对象。其以二进制表示，高3位置为0。

7.75

应用优先指示器（API） application priority indicator (API)

位于JR/T 0025芯片卡中，在一个目录中用来指定应用优先级的数据元。

7.76

应用选择指示符（ASI） application selection indicator (ASI)

指示应用选择时终端上的应用标识（AID）与卡片中的应用标识（AID）是完全匹配（长度和内容都必须一样）还是部分匹配（卡片AID的前面部分与终端AID相同，长度可以更长）的指示符。终端支持的应用列表中的每个应用标识（AID）仅有一个应用选择指示符。

7.77

应用文件定位器（AFL） application file locator (AFL)

用于指出应用相关的文件位置和记录范围。

7.78

IC 卡动态数 ICC dynamic number

随时间变化的一组数字，由JR/T 0025芯片卡生成，并被终端获取。

7.79

终端国家代码 terminal country code

用来表示交易终端所在国家的代码。

7.80

应用参考货币代码 application reference currency code

当终端货币代码与应用货币代码不同时，使用的另外定义的1到4种货币代码，每个货币代码由3位数字组成。

7.81

应用货币指数 application currency exponent

在JR/T 0025芯片卡处理中，该指数用来标明交易金额从右数起的小数点的位置。

7.82

应用用途控制（AUC） application usage control (AUC)

一组标明发卡行卡片应用地域及服务限制的标识，用来限定该卡是用于国内还是国际间，或能否用于现金、购物或服务。

7.83

最低限额 floor limit

商户可进行脱机交易的最大值，当超过该金额时，商户必须通过从发卡行获得联机授权来完成交易。

7.84

连续脱机交易次数上限 (UCOL) upper consecutive offline limit (UCOL)

由发卡行设定的,在不具备联机能力的交易点终端, JR/T 0025芯片卡应用所能完成脱机交易的最多次数。

7.85

连续脱机交易次数下限 (LCOL) lower consecutive offline limit (LCOL)

由发卡行指定的,在具备联机能力的终端,使用JR/T 0025芯片卡连续进行脱机交易的最大次数,若超过此次数,终端将发起一笔联机交易。

7.86

累计脱机交易金额下限检查 lower cumulative offline transaction amount check

用来测定当前交易的金额加上之前连续累计的脱机交易金额,是否超过了发卡行预先设定的累计金额值的功能。

7.87

累计脱机交易金额上限 upper cumulative offline transaction amount

累计的脱机交易金额所能达到的最高金额上限。当交易金额超过该金额时,该交易将会请求联机授权。

7.88

应用交易计数器 application transaction counter

在JR/T 0025芯片卡中,由应用程序来维护的计数器。计数器的增加是由JR/T 0025芯片卡来管理。

7.89

应用交互特征 application interchange profile

表明卡片所支持的功能。

7.90

脚本 script

发卡行向终端发送的命令或命令序列,目的是向IC卡连续输入命令。

7.91

预个人化数据 pre-personalization data

在预个人化阶段写入的非个性化数据。

7.92

个人化数据 personalization data

在个人化阶段写入的个性化数据。

7.93

数据对象列表 (DOL) data object list (DOL)

在JR/T 0025借记/贷记应用交易流程中,终端能够根据卡片的要求建立可变的数据元列表,并通过相关命令发送给卡片。在JR/T 0025交易流程使用的DOL包括:通过获取处理选项(GET PROCESS OPTIONS)命令使用的PDOL;通过生成应用密文(GENERATE AC)命令使用的CDOL1和CDOL2;用来产生TC哈希值的TDOL和通过内部认证(INTERNAL AUTHENTICATE)命令使用的DDOL。

7.94

处理选项数据对象列表 processing options data object list

芯片卡在获取处理选项(GET PROCESSING OPTIONS)命令时所需的终端数据对象(名称及长度)的列表。

7.95

交易验证码待读标志 TAC unread flag

基于冗错考虑，当IC卡内部解扣操作已完成，而终端未读到TAC码时，交易中断，需要通过交易验证码待读标志的机制，通知下一个操作终端将这个未读TAC码取出，形成补充交易数据包上送主机。

7.96

解扣出错计数器 GMAC count

用于防止外界对IC卡进行恶意试探的计数器。在执行解扣指令时，IC卡都会先对命令报文中的GMAC进行验证，如果正确，则进行下一步的正常操作，并将出错计数器复位；连续出错3次时，IC卡自动将当前应用锁定。

7.97

冲突 collision

在同一时间周期内，在同一PCD的工作场中，有两张或两张以上的PICC进行数据传输，使得PCD不能辨别数据是从哪一张PICC发出的。

8 安全及风险管理术语

8.1

安全环境 security environment

对卡系统，为卡的特定应用，规定可用的安全功能给命令提供保护的一种机制。

8.2

安全状态 security status

由相关实体进行识别和认证过程后形成的结果。

8.3

安全审计踪迹 security audit trail

遵循约定的安全规程，用来验证正确性和完整性，并可发现在安全性上破坏行为的历史数据和信息。

8.4

安全印制 security printing

包含精密行数安全方式、填充印制方式、水印方式、五彩印制方式以及添加序列号等防伪手段的印制方式。为防止欺诈，卡片的安全印制必须在严格管控条件下执行。

8.5

地址验证 address verification

将对从服务点上获取的数据和发卡机构持有的数据进行对比，用于验证持卡人签单地址的过程。

8.6

生物特征验证 biometric verification

一种对被观察的生物特征和参考值相比较的持卡人确认形式。

8.7

卡片验证码（CVN） card verification number (CVN)

对磁条信息合法性进行验证的代码。

8.8

卡片验证码 2（CVN2） card verification number 2 (CVN2)

在邮购/电话订购等非面对面交易中对银行卡卡片合法性进行验证的代码。

8.9

加密校验数（CCD） crypto check digital (CCD)

利用加密算法计算出的数字，用于提供数据完整性的一种校验方式。

8.10

敏感数据（信息） sensitive data (information)

必须防止被非法泄露、修改或破坏的数据，特别是明文 PIN 和加密密钥以及包含设计特点、状态

信息的数据。

8.11

个人鉴别信息 (PAI) personal authenticating information (PAI)

用于鉴别用户身份的信息。信息源于用户知道的信息 (如密码)、用户拥有的特性 (如唯一占有的特定标识)、用户自身的信息 (如指纹), 或者是这三种信息的任意组合。

8.12

持卡人身份识别值 (CIV) cardholder identification value (CIV)

用来确认持卡人身份的值。

8.13

参考 CIV reference CIV

用来验证交易 CIV 的 CIV。

8.14

PIN 验证 PIN verification

授权请求使用 PIN 验证持卡人身份的过程。

8.15

联机 PIN 验证 online PIN verification

一种持卡人身份的验证方式, 该方式将加密后的 PIN 值通过授权请求报文发送至发卡行, 通过比较报文中 PIN 值与发卡行 PIN 值是否一致来验证持卡人身份。

8.16

脱机 PIN 验证 offline PIN verification

一种持卡人身份的验证方式, 该方式通过终端和 IC 卡的交互来比较持卡人输入的 PIN 与 IC 卡芯片内存储的 PIN 是否一致来验证持卡人身份。

8.17

初始密码 natural PIN

不同于客户可选择的密码, 初始密码由发卡行分派。发卡行利用某种算法对有效数据和验证密钥进行运算, 再对运算结果进行 (或不进行) 后续操作, 选出一组数字作为初始密码。

8.18

交易 PIN transaction PIN

在交易时由客户输入的 PIN。

8.19

参考 PIN reference PIN

用来验证交易 PIN 的 PIN 值。

8.20

加密 PIN 值 encrypted PIN data

持卡人输入的加密过的 PIN。

8.21

PIN 验证码 (PVN) PIN verification number (PVN)

对 PIN 进行验证的代码。

8.22

PIN 验证密钥 (PVK) PIN verification key (PVK)

用于产生 PVN 的加密密钥, 长度为 128 位。

8.23

密码修改/解锁 PIN change/unblock

发卡金融机构为持卡人修改或解锁 PIN 的操作。

8.24

数据完整性 data integrity

数据不受未经许可的方法变更或破坏的属性。

8.25

不可否认性 non-repudiation

可由第三方确认数据的完整性和来源，并能够提供确凿证据。

8.26

密钥 key

用于将明文转换成密文或者将密文转换成明文的算法中的一个数值。

8.27

密钥的不可逆转换 irreversible transformation of a key

由前一密钥产生新的密钥，使得即使掌握新密钥和转换方法的细节，也没有确定前一密钥的可行方法。

8.28

密钥粒度 key granularity

密钥代表的个体的数量。例如，最细的粒度是由一个密钥表示一个个体；而一个粗粒度是一个节点密钥。

8.29

密码链 cryptographic link

预先同意交换数据并具有密钥关系的两个逻辑实体（节点）。

8.30

密码节点 cryptographic node

密码链中的一个逻辑实体（节点）。

8.31

密钥同步 key synchronization

两个节点验证它们使用相同密钥进行通信的过程。

8.32

密码服务报文 cryptographic service message

一种传递密钥或用于控制密钥关系信息的报文。

8.33

静态密钥 static key

交易双方使用双控方式手工装载的一种工作密钥。静态密钥具有不定期限生命周期。

8.34

动态密钥 dynamic key

通过联机网络管理报文实现密钥的更改，而不需要手工干预的一种工作密钥。

8.35

一次一密 derived unique key per transaction

对每次交易都采用不同密钥的密钥管理方式，以防止以往交易中泄漏的密钥被继续使用。每次交易的密钥由该次交易相关的数据通过算法生成。

8.36

明文 plaintext

未被加密的信息。

8.37

待加密元素 encipherment element

待加密的连续明文字符组。

8.38

密钥要素 keying material

建立和维护密钥关系的必要数据。

8.39

初始化向量 (IV) initialization vector (IV)

作为数据序列的加密起点的数字。初始化向量通过引入附加的密码方差提高安全性，并有助于密码设备的同步。

8.40

密文 cryptogram

加密运算的结果。

8.41

密码计算 ciphering

在称为密钥的参数控制下，实现明文密文间转换的一对操作。

注：加密操作将数据（明文）转换成不可读的密文形式；解密操作将密文恢复成明文。

8.42

密码函数 cryptographic function

使用密码算法进行处理的过程（例如：加密、鉴别、认证）。

8.43

加密 encryption

用密码算法将明文数据变换成密文数据的过程。

8.44

可逆加密 reversible encipherment

由明文到密文的转换过程，并且转换过程中使用的方法能够恢复原始明文。

8.45

不可逆加密 irreversible encipherment

从明文到密文的一种转换，通过使用这种方法，使得即使掌握密钥也无法恢复出明文，除非进行穷举。

8.46

解密 decipherment

将密文转换成明文的过程。

8.47

密码系统 cryptosystem

用来加密和解密信息的系统。

8.48

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第三方篡改，也保护数据发送方发出的数据不被接收方篡改。

8.49

鉴别 authentication

认证 authentication

对用户、设备和其他实体的身份以及数据完整性的验证。

- 8.50
鉴别密钥 authentication key
认证密钥 authentication key
 用于鉴别的密钥。
- 8.51
实体鉴别 entity authentication
 确认实体（节点）的身份是其所声称的身份。
- 8.52
报文鉴别 message authentication
 用于报文发送方和接收方之间，保证报文来源、报文部分内容或全部内容有效性的技术。
- 8.53
报文鉴别码（MAC） message authentication code (MAC)
 对交易数据及其相关参数进行运算后产生的代码，主要用于验证报文的完整。
- 8.54
密钥有效期 cryptoperiod
密钥周期 cryptoperiod
 某个特定的密钥被授权可以使用的时间段，或者某个密钥在给定的系统中有效的时间段。
- 8.55
密钥生命周期 key life cycle
 密钥管理的所有阶段，包括计划、生成、回收、销毁和存档。
- 8.56
密码生成 PIN generation
 为防止欺诈，在严密的安全条件下，生成密码并分配给持卡人的过程。
- 8.57
密钥引入 key introduction
 产生、分发和开始使用密钥对的过程。
- 8.58
密钥更换 key replacement
 回收一个密钥，同时引入另外一个密钥来代替它的过程。
- 8.59
密钥回收 key revocation
 回收使用中的密钥以及处理其使用后的遗留问题的密钥管理过程。密钥回收可以按计划回收或提前回收。
- 8.60
按计划的回收 planned revocation
 按照公布的密钥失效日期进行的密钥回收。
- 8.61
提前回收 accelerated revocation
 在已公布的密钥失效日期到期前回收密钥。
- 8.62
潜在泄露 potential compromise
 密码分析技术和/或计算能力的提高达到了可能造成某个特定长度的密钥的泄露的情况。。
- 8.63
逻辑泄露 logical compromise

由于密码分析技术和/或计算能力的提高，对密钥造成的泄露。

8.64

物理泄露 physical compromise

由于没有安全的保护，或者硬件安全模块的被盗或被未经授权的人存取等事实对密钥造成的泄露。

8.65

主密钥 primary key

用于产生交易中其他密钥的密钥（例如以变形或变换的方式）。

8.66

根密钥 derivation key

用来生成导出密钥的密钥。

8.67

导出密钥 derived key

分散密钥 diversified key

由根密钥和非保密可变数据生成的对称密钥。

注：根密钥用来生成大量密钥（导出密钥）

8.68

分散参数（DP） derivation parameter (DP)

用于从种子密钥中分散应用密钥值的数据元（或者几个数据元的组合）。

8.69

工作密钥（WK） working key (WK)

数据密钥（DK） data key (DK)

在终端正常情况下，对 PIN 加密、参与 MAC 计算的密钥。工作密钥应经常更新。在联机更新的报文中，使用密钥加密密钥对工作密钥加密，形成密文后进行传输。

8.70

MAC 密钥（MAK） message authentication code key (MAK)

用于生成交易 MAC 的密钥。

8.71

PIN 加密密钥（PIK） PIN key (PIK)

用于加解密 PIN 的密钥。

8.72

终端主密钥（TMK） terminal master key (TMK)

用于加密终端工作密钥（TPK、TAK）的密钥。

8.73

终端 MAC 密钥（TAK） terminal MAC key (TAK)

用于终端上对报文进行 MAC 生成和检验的密钥。

8.74

终端 PIN 密钥（TPK） terminal PIN key (TPK)

终端加密持卡人 PIN 的密钥。

8.75

会话密钥 session key

由密码管理协议生成的密钥，提供在多个实体间传输数据的安全服务。单个协议的执行可能产生多个会话密钥，例如一个加密密钥和一个 MAC 密钥。

8.76

密钥加密密钥（KEK） key encryption key (KEK)

只用于对其他密钥进行加密的密钥。通常，密钥加密密钥常用于在电子密钥交换和存档过程中对数据、PIN 或 MAC 相关密钥进行加密。

8.77

硬件加密 hardware encryption

用来加密敏感数据的物理安全设备。敏感数据除了在接入点和最终点外都不以明文形式出现，在每一个信息文件中，物理安全设备都会解密并重新加密文本。

8.78

硬件加密机 (HSM) hardware and security module (HSM)

对传输的数据进行加密的外围硬件设备，用于 PIN 的加密和解密、验证报文和文件来源的正确性以及存储密钥。

8.79

加密设备 cryptographic equipment

执行加密功能（如加密、鉴别、密钥生成）的设备

8.80

安全加密设备界面 security cryptographic device interface

安全加密设备和运行环境交互的界面（比如：命令、控制面板、锁等）。

8.81

设备安全性 device security

与特定操作环境无关，仅依赖于自身特性的安全加密设备安全性。

8.82

逻辑安全性 logical security

设备在功能上抵御攻击的能力。

8.83

物理安全性 physical security

设备在物理构造上抵御攻击的能力。

8.84

安全符合性检测清单 security compliance check list

按照设备类型建立的审计要求的列表。

8.85

安全应用模块 secure application module

包含算法、相关密钥、安全程序及信息，用来防止对应用程序未授权访问的物理模块。

注：为实现此目的，该模块应受物理和逻辑保护。

8.86

主机安全模块 host security module

用来支持密码功能和在主机系统上实现安全存取模块（SAM）功能的物理安全设备。

8.87

PASM 卡 PSAM card

金融 IC 卡终端设备的安全存取模块。

8.88

软件加密 software encryption

使用软件加密信息文件的敏感数据。

8.89

密码学 cryptography

一门包含数据转换原则、途径和方法的学科。旨在隐藏数据转换中的信息内容，防止未察觉的篡改

以及非授权的使用。

8.90

加密算法 cryptographic algorithm

为了隐藏或恢复信息内容，在密钥的控制下，对数据进行变换的算法。

8.91

数据加密标准 (DES) data encryption standard (DES)

美国国家标准局采用的加密规则。为保证安全传输，该标准以打乱 PIN 和交易数据进行加密。

8.92

数据加密算法 (DEA) data encryption algorithm (DEA)

美国国家标准协会的对称加密算法标准，其被广泛使用的为 DES，自发布以来，已被广泛研究，并为世界范围内认可和使用的对称算法。

8.93

n 位分组密码 n-bit block cipher

明文分组和密文分组在长度上都是 n 位的分组密码。

8.94

安全哈希算法-1 (SHA-1) secure hash algorithm-1 (SHA-1)

一个单向的加密函数，对于长度小于 264 位的任意长度的输入信息，会生成一条 160 位的报文摘要。

8.95

哈希函数 hash function

将位串映射为定长位串的函数，它满足以下两个条件：

——对于一个给定的输出，不可能推导出与之相对应的输入数据；

——对于一个给定的输入，不可能通过计算得到具有相同的输出的另一个输入。

另外，如果要求哈希函数具备防冲突功能，则还应满足以下条件：

——不可能通过计算找到两个不同的输入具有相同的输出。

8.96

哈希算法标识符 hash algorithm indicator

在签名数据前用来压缩静态或动态数据的算法标识符。

8.97

哈希结果 hash result

哈希函数输出的位串。

8.98

RSA 加密算法 (RSA) Rivest Shamir Adleman (RSA)

由麻省理工学院 (MIT) 的三位数学家：Rivest、Shamir 和 Adelman 发明的公钥加密算法，是最常用的加密和验证算法。

8.99

持卡人证书 cardholder certificate

在安全的电子商务交易中，用来认证持卡人身份的电子文本。

8.100

CUPSecure China UnionPay secure

中国银联制定的互联网电子商务领域银行卡交易的安全体系。

8.101

中国银联安全输入模式 China UnionPay secure information collection mode

由中国银联代为收集安全信息并转发给发卡机构，由发卡机构认证并完成相应支付交易的安全认证模式。

8.102

对称算法 symmetric algorithm

用相同的保密密钥进行加密和解密的一种密码算法。

8.103

对称加密技术 symmetric cryptographic technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

8.104

对称密码 symmetric cipher

使用相同的密钥进行加密和解密的密码方法。

8.105

保密密钥 secret key

对称加密技术中仅供指定实体所用的密钥。

8.106

双重控制 dual control

利用两个或更多的单独实体（通常是人），协同操作以保护敏感功能或信息的过程。单独的实体不能存取和使用这些功能或信息（如：密钥）。

8.107

伪随机 pseudo-random

由算法生成但在统计上是随机的且本质上是不可预测的过程。

8.108

伪随机数 pseudo-random number

在统计上具有随机性，并且即使通过某种算法程序生成也不可预测的数。

8.109

时间变量参数（TVP） time variant parameter (TVP)

在密钥的有效期内不能故意重复的随机或伪随机值。

8.110

密钥分割 split knowledge

两个或更多的实体分别地拥有密钥片断，仅通过单个密钥片段不能合成密钥信息。

8.111

密钥空间 key space

某一密码的所有可用密钥的集合。

8.112

密钥信封 key mailer

用于向已获授权人员传送密钥组件的信封。

8.113

密钥组件 key component

与密码密钥相关的参数之一（参数至少 2 个），在生成该密码密钥时，只有当参数的数量达到阈值时才能组合形成密钥，若参数数量小于阈值，则不能提供有关该密钥的任何信息。这些参数结合形成一个密钥的密钥特征（如格式、随机性），例如，通过模 2 加法形成密钥。

8.114

密钥偏移量 key offset

偏移量 offset

密钥和计数器使用模 2 加法相加的结果。

8.115

私钥 private key

一个实体的非对称密钥对中含有的供实体自身使用的密钥，在数字签名方案中，私钥用于签名。

8.116

公钥 public key

一个实体使用的非对称密钥对中可以公开的密钥。在数字签名方案中，公钥用于验证。

8.117

非对称算法 asymmetric algorithm

一种加密密钥和解密密钥不同的算法，并且对于该算法不能由一个密钥计算推导出另一个密钥。

8.118

非对称密码体系 asymmetric cryptosystem

公钥密码体系 public key cryptosystem

该密码体系由两个互补的操作组成，每一个操作利用不同但相关的密钥即公钥和私钥之一进行加密或解密，并且从加密密钥推导出解密密钥在计算上不可行。

8.119

公钥分配体系 public key distribution system

允许两个通信实体共同创建一个密钥的公钥密码体系。

8.120

非对称加密技术 asymmetric cryptographic technique

采用两种相关变换进行加密的技术，一种是公开变换（由公钥定义）；另一种是私有变换（由私钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

8.121

非对称密钥对 asymmetric key pair

在公钥体系中生成及使用的公钥及其相关私钥。

8.122

密钥对的所有者 key pair owner

拥有密钥对的一方。

8.123

非对称密码 asymmetric cipher

加密密钥和解密密钥不同的密码，并且从加密密钥推导出解密密钥在计算上不可行。

8.124

非对称密钥对生成器 asymmetric key pair generator

用于生成非对称密钥对的安全密码设备。

8.125

证书 certificate

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

8.126

证书标识符 certificate identifier

能够正确验证密钥证书的证书信息。

8.127

证书链 certificate link

包括根证书在内的一组排序的数字证书，其中根证书位于证书层次结构的最高层。

- 8.128
中间证书 intermediate certificate
证书链中除起始证书和末端证书之外的证书。
- 8.129
末端证书 end certificate
证书链中的最后证书。
- 8.130
CA 证书 CA certificate
主体为 CA 的证书，其相关的私钥用来对证书进行签名。
- 8.131
认证 certification
为一个实体创建公钥或属性证书的过程。
- 8.132
交叉认证 cross certification
两个 CA 相互对对方的公钥认证的过程。
- 8.133
策略映射 policy mapping
当一个域中的认证机构（CA）对另一个域中的 CA 认证时，第二个域中的特定证书策略可被第一个域中的机构看作是与第一个域中的特定证书策略等同的（但没有必要在任何方面都相同）策略。
- 8.134
策略限定符 policy qualifier
由策略决定的信息，在 X.509 证书中附有证书策略标识符。
- 8.135
认证业务申明（CPS） certification practice statement (CPS)
认证中心在发布证书时使用的业务申明。
- 8.136
证书使用系统 certificate-using system
由证书使用者使用的功能实现系统。
- 8.137
证书挂起 certificate hold
证书的暂时失效。
- 8.138
证书回收 certificate revocation
由发行证书的实体废除一个有效证书的过程。
- 8.139
证书回收列表（CRL） certificate revocation list (CRL)
被回收的证书列表。
- 8.140
CRL 分发点 CRL distribution point
CRL 的目录项或其他分发源。
- 8.141
IC 卡私钥 ICC private key
用来生成签名的动态应用数据的密钥。

- 8.142
持卡人验证方法列表 CVM list
用来标记持卡人验证方法的列表（例如签名、联机 PIN 和脱机 PIN 等）。
- 8.143
持卡人验证方法结果 CVM result
用来指明 CVM 执行结果的数据元。
- 8.144
卡片验证结果（CVR） card verification result (CVR)
JR/T 0025 芯片卡用来存储卡片风险管理结果的一组私有数据元。
- 8.145
卡片行为分析 card action analysis
根据CVR和应用缺省行为（ADA）来决定返回给终端的密文类型。
- 8.146
终端验证结果（TVR） terminal verification results (TVR)
在 JR/T 0025 借记/贷记应用交易流程中，用于标识终端执行脱机数据认证、处理限制、持卡人验证、终端风险管理、发卡行认证、发卡行脚本处理等各步骤的结果，终端和卡片将参考 TVR 的值对当前交易做出脱机拒绝、联机交易或脱机批准的决定。
- 8.147
发卡行行为代码（IAC） issuer action code (IAC)
发卡行根据TVR的内容选择的动作识别码。
- 8.148
终端行为代码（TAC） terminal action code (TAC)
收单行根据 TVR 的内容选择的动作识别码。
- 8.149
卡片风险管理（CRM） card risk management (CRM)
JR/T 0025 芯片卡用来决定如何响应终端请求的应用密文的过程。
- 8.150
终端风险管理 terminal risk management
终端风险管理可包括终端异常文件检查、最低限额检查、随机交易选择、终端频度检查、新卡检查。
- 8.151
静态数据认证（SDA） static data authentication (SDA)
终端验证卡片固定的加密签名的过程。
- 8.152
签名的静态应用数据 signed static application data
用于静态数据认证的关键应用参数数字签名。
- 8.153
静态数据认证标签 static data authentication (SDA) tag for signing
用于签名的静态数据认证标签。
- 8.154
动态数据认证（DDA） dynamic data authentication (DDA)
为保证交易安全，卡片在脱机环境下使用交易指定数据元生成签名，由芯片读卡设备验证该签名的过程。
- 8.155
签名的动态应用数据 signed dynamic application data

用于动态数据认证的关键应用参数数字签名。

8.156

动态数据认证数据对象列表 (DDOL) dynamic data authentication data object list (DDOL)

用于在内部认证 (Internal Authenticate) 命令中向 JR/T 0025 芯片卡传输的数据对象 (标签及长度) 列表。

8.157

交易证书 (TC) transaction certificate (TC)

在 JR/T 0025 借记/贷记应用交易流程中, 由 IC 卡生成表示批准交易的应用密文。

8.158

交易证书数据对象列表 (TDOL) transaction certificate data object list (TDOL)

终端生成交易证书 (TC) 哈希值所使用的数据对象 (标签及长度) 列表。

8.159

卡片认证方法 (CAM) card authentication methodology (CAM)

用来认定卡真伪的方法, 例如 CVN、CVN2、芯片 (集成电路) 和磁条的验证。

8.160

动态联机卡片认证方法 dynamic online

一般来说使用对称密码技术 (例如 DES)。对称密码技术要求 JR/T 0025 芯片卡和发卡行拥有相同的保密密钥。对于每一笔交易, JR/T 0025 芯片卡会计算出一个新的数字签名, 供发卡行来验证。因此, 每次验证都会产生一个唯一的结果。

8.161

PIN 尝试次数计数器 (PTC) PIN try counter (PTC)

芯片卡的一种功能, 是由发卡行指定的用以计算持卡人连续输错脱机密码的次数。每输错一次密码, 该值都会减 1, 当该值变为零时, 密码将被锁定, 并且芯片卡不再响应“验证”命令。

8.162

PIN 尝试限制 (PTL) PIN try limit (PTL)

发卡行指定的用来标明连续输错密码的最多次数的数据参数。当持卡人输入密码错误次数超过该限制值时, 密码将被锁定。

8.163

交易验证码 (TAC) transaction authorization cryptogram (TAC)

卡片对交易的确认信息, 在脱机消费交易中 TAC 正确即表示发卡机构认可这笔交易。

8.164

应用密文 (AC) application cryptogram (AC)

JR/T 0025 芯片卡响应生成应用密文 (GENERATE AC) 命令返回的密文。共有 3 类密文, 包括交易证书 (TC)、授权请求密文 (ARQC) 和应用认证密文 (AAC)。

8.165

应用授权参考 application authorization referral

芯片卡在第一次生成应用密文 (GENERATE AC) 时生成的响应, 用以标明卡片已经向发卡行主机系统发起参考请求。

8.166

授权请求密文 (ARQC) authorization request cryptogram (ARQC)

IC 卡为联机处理交易生成的应用密文, 发卡行在联机卡片认证过程中通过验证 ARQC 来认证当前交易中卡片的有效性。

8.167

授权响应密文 (ARPC) authorization response cryptogram (ARPC)

由发卡行生成并在联机授权报文中返回给终端的应用密文，用于 IC 卡验证联机授权响应是否来自真正的发卡行。

8.168

应用认证密文 (AAC) application authentication cryptogram (AAC)

在 JR/T 0025 借记/贷记应用交易流程中，由 IC 卡生成的，表示拒绝交易的应用密文。

8.169

联机卡片认证密文 online card authentication cryptogram

确认卡片和授权请求信息合法性的密文。

8.170

发卡行直接认证授权模式 issuer secure authentication and authorization mode

在发卡行直接认证模式中，由持卡人安全认证授权系统 (SAA) 提供界面供持卡人输入身份认证安全信息并完成相应支付交易的安全认证模式。

8.171

安全报文交换 secure messaging

在命令期间为数据交换的密码保护提供的一种方法。

8.172

发卡行加密主密钥 (ENC MDK) issuer master data encipherment DEA key (ENC MDK)

发卡行的一个主密钥，使用一些分散参数，产生 JR/T 0025 芯片卡安全报文密钥。分散参数一般为应用主账号 (PAN) 和应用主账号 (PAN) 序列号。

8.173

发卡行 mac 主密钥 (MAC MDK) issuer master message authentication code key (MAC MDK)

发卡行的一个双倍长主密钥，使用一些分散参数，产生 JR/T 0025 芯片卡 MAC 密钥。分散参数一般为应用主账号 (PAN) 和应用主账号 (PAN) 序列号。

8.174

发卡行应用数据 issuer application data

在联机交易中传输给发卡行的包含私有应用数据的数据元。

8.175

发卡行认证数据 issuer authentication data

联机交易中传输给 JR/T 0025 芯片卡的，用来验证发卡行真实性的数据。

8.176

认证中心公钥索引 certification authority public key index

包含一个二进制数值的单字节数据元。用来决定 JR/T 0025 芯片卡使用的认证中心的公钥，其相关的算法设置在终端上。

8.177

发卡行公钥指数 issuer public key exponent

用来验证静态应用数据和 JR/T 0025 芯片卡公钥证书的指数。

8.178

发卡行公钥余数 issuer public key remainder

发卡行公钥模的余数。

8.179

发卡行公钥证书 issuer public key certificate

通过认证中心签署的用于 SDA 或 DDA 的密钥。

8.180

发卡行私钥 issuer private key

用来生成签名的静态应用数据，并可签署 JR/T 0025 芯片卡公钥证书的密钥。

8.181

账户数据泄露事件 (ADCE) account data compromise event (ADCE)

由于账户数据被窃取而导致持卡人的账户被非法使用的事件。账户数据被窃取表示该账户的数据已经被不正当地泄露或使用。

8.182

攻击 tampering

对设备内部的探查或修改，或通过主动或被动的去探查或记录秘密数据的行为。

8.183

设陷盗取存款 trapping for deposit

将某种设备、材料用于 ATM 等设备中以避免合法用户察觉，阻止用户所存现金到达存款箱。存款在用户离开后可被获取。

8.184

设陷盗取出钞 trapping for cash

将某种设备、材料用于 ATM 等设备中以避免合法用户察觉，阻止用户拿到发出的现金。发出的现金在用户离开后可被获取。

8.185

钓盗现金 fishing

将任何形式的带有一个或多个钩子或其他装置的绳索、金属线或类似物品作用于 ATM，以获取现金。

8.186

暴力取现 forcing

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

8.187

泄露 compromise

一种对系统安全的侵害，该侵害有可能导致敏感数据被非法获得。

8.188

穿透 penetrate

主动攻击的一种，它使用物理的穿孔技术或者未经授权打开设备来获取其中的敏感数据，穿透是一种针对设备的物理特性的攻击。

8.189

监视 spy

一种被动的攻击，它可能包括诸如监视电磁辐射来发现设备中的敏感信息，或者通过视觉、听觉、或电子监视输入到设备里面的敏感数据。监视是一种针对设备物理特性的攻击。

8.190

操纵 manipulate

在未经授权的情况下，向设备发送一串输入信息，导致设备中敏感信息的泄露，或者以未经授权的方法获得服务，比如：让设备进入“测试状态”，以泄漏其敏感信息或者操纵设备的完整性。操纵是一种针对设备逻辑特性的攻击。

8.191

洗单 factoring

商户将其他未签约商户的交易在本商户的 POS 机或压印机上刷卡或压卡，或是通过网络交易，假冒本店交易与收单机构清算。

8.192

侧录 skimming

因商户默许、纵容、与不法分子共谋、商户管理不善、银行管理不善等原因导致银行卡机具上装载侧录仪器而造成的持卡人信息被盗录的行为。

8.193

替换 replace

未经授权而把一个设备替换为另一个。

8.194

字典攻击 dictionary attack

一种攻击，这种攻击中攻击者建立一个明文和相应密文的字典，当截获的密文和字典中存储的密文匹配时，对应的明文就可立即从字典中获得。

8.195

反射攻击 reflection attack

由假冒响应者发起的攻击，由此攻击者在一单独的对话中，用相同的随机值向发起者发起质询，该随机值与在并发的会话中发起者已经发出用来鉴别真实响应者的值相同。

8.196

抗攻击性 tamper-resistant characteristic

提供物理保护以抵御攻击的特性。

8.197

防攻击性 tamper-evident characteristic

能提供曾受到攻击企图的证据的特性。

8.198

反击性 tamper-responsive characteristic

针对已检测到的攻击，主动反应以阻止攻击的特性。

附录 A
(资料性附录)
银行卡名词术语中文索引

A		
ADF 分配	ADFFallocation	6.5
ADF 个人化机构	personalizer	4.22
ATM 安全监控模块	ATM safety monitor module	5.29
ATM 保险柜	ATM safe	5.22
ATM 查询	ATM inquiry	6.70
ATM 前置处理系统	automatic teller machine front-end processing system	7.55
ATM 取现	ATM cash withdraw	6.71
ATM 授权	ATM authorization	6.72
安全报文交换	secure messaging	8.171
安全处理费用及酬劳	security handling fee and reward	6.129
安全电子商务交易	secure electronic commercial transaction	6.74
安全符合性检测清单	security compliance check list	8.84
安全哈希算法-1	secure hash algorithm-1	8.94
安全环境	security environment	8.1
安全加密设备	secure cryptographic device	5.55
安全加密设备界面	security crytograhoic device interface	8.80
安全审计踪迹	security audit trail	8.3
安全印制	security printing	8.4
安全应用模块	secure application module	8.85
安全状态	security status	8.2
按计划的回收	planned revocation	8.60
B		
保护时间	guard time	7.1
保密密钥	secret key	8.105
报文标识符	message identifier	7.26
报文功能	message function	7.27
报文鉴别	message authentication	8.52
报文鉴别码	message authentication code	8.53
报文类型代码	message type code	7.25
报文位图	message bit map	7.28
报文摘要	message digest	7.29
报文转发	message forwarding	7.38
暴力取现	forcing	8.186
本地交易	local transaction	6.18
本地交易凭证	local transaction receipt	6.19
本地结算	local settlement	6.20
本地授权	local authorization	6.21

本行交易	on-us transaction	6.22
编码错卡	misencoded card	3.12
标签、长度、数值	tag, length, value	7.67
表面粗糙度	surface roughness	3.65
剥离强度	peel strength	3.57
补充明细	supplementary details	6.139
不可否认性	non-repudiation	8.25
不可逆加密	irreversible encipherment	8.45
不良持卡人系统	system of delinquent cardholder	7.59
不良商户系统	system of delinquent merchant	7.58
部分迁移的发卡机构	early issuer	4.6
部分授权	partial authorization	6.58
C		
CA 证书	CA certificate	8.130
CRL 分发点	CRL distribution point	8.140
CUPSecure	China UnionPay secure	8.100
裁判	arbitrage	6.108
参考 CIV	reference CIV	8.13
参考 PIN	reference PIN	8.19
操纵	manipulate	8.190
操作员	operator	4.28
侧录	skimming	8.192
测试方法	test method	6.141
策略限定符	policy qualifier	8.134
策略映射	policy mapping	8.133
查询明细	detail inquiry	6.49
查询余额	balance inquiry	6.48
差错处理平台	adjustment platform	7.50
差错交易	adjustment	6.90
长连接	persistent connect	7.3
超时限值	timeout value	6.140
撤销	reverse	7.35
撤销转账	reversal transfer	6.47
持卡人	cardholder	4.23
持卡人接入设备	cardholder access device	5.49
持卡人身份识别值	cardholder identification value	8.12
持卡人验证方法结果	CVM result	8.143
持卡人验证方法列表	CVM list	8.142
持卡人折扣	cardholder discount	6.138
持卡人证书	cardholder certificate	8.99
持卡人自助终端	cardholder-activated terminal	5.11
持卡者标识	cardholder identification	4.25
尺寸稳定性	dimensional stability	3.63
冲突	collision	7.97

冲正	reversal	6.76
出钞模块	cash teller module	5.24
初始化向量	initialization vector	8.39
初始密码	natural PIN	8.17
初始文本序列	initial text sequence	7.4
处理费	processing fee	6.128
处理选项数据对象列表	processing options data object list	7.94
处理优先级	processing priority	7.40
处理优先级代码	processing priority code	7.41
触点	contact	3.32
穿墙式	through-wall mode	5.15
穿透	penetrate	8.188
串联	concatenation	7.5
磁道数据	track data	3.20
磁条	magnetic stripe	3.18
磁条镜像	magnetic stripe image	7.6
磁条卡	magnetic stripe card	3.19
磁条芯片复合卡	combined IC and magnetic stripe card	3.30
磁条阅读器	magnetic stripe reader	5.51
磁通翻转	flux transition	3.53
从属认证中心	subject CA	4.16
促销代码	promotion code	7.44
存储卡	memory card	3.27
存储转发	store and forward	7.39
存款模块	deposit module	5.25
存折打印模块	bank book print module	5.33
错误制卡	misembossed card	3.11
D		
大堂式	in-lobby mode	5.16
代付交易	agency payment	6.39
代理业务	agent service	6.37
代收交易	collection	6.38
代授权	stand-in authorization	6.40
待加密元素	encipherment element	8.37
贷记调整	credit adjustment	6.92
贷记交易	credit transaction	6.42
贷记卡	credit card	3.5
单信息交易	single message transaction	6.15
单一 IC 系统	IC-only system	7.54
导出密钥	derived key	8.67
地址验证	address verification	8.5
第二辅助账号	second subsidiary account number	3.44
第三方转账	third-party transfer	6.46
第一辅助账号	first subsidiary account number	3.43

电话支付中心	telephone payment centre	4.18
电话支付终端	telephone payment terminal	5.46
电子存折	electronic deposit	6.123
电子柜	electronic cabin	5.38
电子钱包	electronic purse	6.124
电子锁	electronic lock	5.39
电子现金	electronic cash	6.125
电子资金转账	electronic funds transfer	6.126
电子资金转账系统	electronic fund transfer system	7.51
钓鱼现金	fishing	8.185
调单	retrieval	6.100
调单回复	retrieval response	6.101
调单展期	retrieval postponement	6.102
动态币种转换	dynamic currency conversion	6.112
动态联机卡片认证方法	dynamic online	8.160
动态密钥	dynamic key	8.34
动态数据认证	dynamic data authentication	8.154
动态数据认证数据对象列表	dynamic data authentication data object list	8.156
动态弯曲应力	dynamic bending stress	3.62
读磁条终端	magnetic stripe terminal	5.4
短连接	transitory connect	7.2
短文件标识符	short file identifier	7.74
对称加密技术	symmetric cryptographic technique	8.103
对称密码	symmetric cipher	8.104
对称算法	symmetric algorithm	8.102
多媒体公共支付终端	multimedia public payment terminal	5.45
多媒体功能模块	multimedia function module	5.30
E		
EMV 标准	EMV standard	6.1
EMV 机构	EMVCo	4.8
二磁	track 2	3.22
二磁等价数据	track 2 equivalent data	3.23
二次退单	second chargeback	6.98
F		
发卡后应用修改	post-issuance application change	6.158
发卡后应用装载	post-issuance application load	6.159
发卡行	issuer	4.4
发卡行 mac 主密钥	issuer master message authentication code key	8.173
发卡行标识代码	issuer identification number	4.5
发卡行标识域	issuer identification area	3.40
发卡行公钥余数	issuer public key remainder	8.178
发卡行公钥证书	issuer public key certificate	8.179
发卡行公钥指数	issuer public key exponent	8.177

发卡行加密主密钥	issuer master data encipherment DEA key	8.172
发卡行认证数据	issuer authentication data	8.175
发卡行私钥	issuer private key	8.180
发卡行行为代码	issuer action code	8.147
发卡行应用数据	issuer application data	8.174
发卡行直接认证授权模式	issuer secure authentication and authorization mode	8.170
发起方	initiator	4.10
反攻击性	tamper-responsive characteristic	8.198
反射攻击	reflection attack	8.195
防攻击设备	tamper-evident device	5.56
防攻击性	tamper-evident characteristic	8.197
非对称加密技术	asymmetric cryptographic technique	8.120
非对称密码	asymmetric cipher	8.123
非对称密码体系	asymmetric cryptosystem	8.118
非对称密钥对	asymmetric key pair	8.121
非对称密钥对生成器	asymmetric key pair generator	8.124
非对称算法	asymmetric algorithm	8.117
非关联圈存	unlinked load	6.152
非接触卡	contactless card	3.37
非指定账户圈存	load on unspecified account	6.154
非自主清算	unself-determination settlement	6.83
费用	charge	6.127
分单	split transaction	6.79
分期付款	installment	6.51
分散参数	derivation parameter	8.68
风险备付金	risk reserve fund	6.133
封装机构	embedder	4.20
服务代码	service code	7.46
服务点输入方式码	point of service entry mode	7.45
副卡	supplementary card	3.8
G		
个人化	personalization	6.142
个人化数据	personalization data	7.92
个人鉴别信息	personal authenticating information	8.11
个人识别码	personal identification number	4.24
根密钥	derivation key	8.66
工作密钥	working key	8.69
公共服务平台	public service platform	7.48
公共支付平台	public payment platform	7.49
公共支付终端	public payment terminal	5.44
公钥	public key	8.116
公钥分配体系	public key distribution system	8.119
攻击	tampering	8.182
关联圈存	linked load	6.151

国内交易	domestic transaction	6.17
过期卡	expired card	3.13
H		
哈希函数	hash function	8.95
哈希结果	hash result	8.97
哈希算法标识符	hash algorithm indicator	8.96
合法用户	authorized customer	4.26
后台维护模块	operator's display module	5.31
会话密钥	session key	8.75
货币清算服务	intracurrency settlement service	6.88
I		
ICA 号	ICA number	4.2
IC 的封装	IC embedding	6.2
IC 的组装	IC assembling	6.3
IC 卡动态数	ICC dynamic number	7.78
IC 卡读写器	ICC reader and writer	5.52
IC 卡交易	ICC transaction	6.27
IC 卡私钥	ICC private key	8.141
IC 卡终端	integrated circuit card terminal	5.5
IC 组件	IC assembly	6.4
ID-000 型卡	ID-000 card	3.14
ID-1 型卡	ID-1 card	3.15
ID-2 型卡	ID-2 card	3.16
ID-3 型卡	ID-3 card	3.17
IIN 的块	block of IINs	6.6
J		
机械密码锁	mechanical lock	5.40
基本文件	elementary file	7.68
基准电流	reference current	3.56
基准信号幅度	reference signal amplitude	3.54
即用资金	immediate fund	6.132
集成电路	integrated circuit	3.25
集成电路厂商	integrated circuit manufacturer	4.21
集成电路卡	integrated circuit card	3.26
集成电路模块	integrated circuit module	5.32
加钞周期	cash replenishment period	6.73
加密	encryption	8.43
加密 PIN 值	encrypted PIN data	8.20
加密设备	cryptographic equipment	8.79
加密算法	cryptographic algorithm	8.90
加密校验数	crypto check digital	8.9
间联	indirect connection	7.14
监视	spy	8.189
简化的芯片卡交易	simplified chip card transaction	6.31

建立/撤销委托关系交易	setup/cancellation clientage transaction	6.34
鉴别	authentication	8.49
鉴别密钥	authentication key	8.50
降级使用交易	fallback	6.32
交叉认证	cross certification	8.132
交互报文	interactive message	7.32
交换	exchange	7.23
交易 PIN	transaction PIN	8.18
交易报文	transaction message	7.30
交易参考号	transaction reference number	6.8
交易成功率	transaction success ratio	6.109
交易点	point of transaction	6.100
交易点的电子资金转账	electronic fund transfer at point-of-transaction	7.52
交易费	transaction fee	6.130
交易国家	transaction country	6.111
交易计数器	transaction counter	6.113
交易记录明细	transaction audit trail	6.114
交易金额	transaction amount	6.115
交易类型代码	transaction type code	6.116
交易日期	transaction date	6.117
交易日志	transaction log	6.118
交易信息文档	transaction information document	6.119
交易验证码	transaction authorization cryptogram	8.163
交易验证码待读标志	TAC unread flag	7.95
交易证书	transaction certificate	8.157
交易证书数据对象列表	transaction certificate data object list	8.158
矫顽力	coercivity	3.52
脚本	script	7.90
接近式 IC 卡	proximity IC card	3.39
接近式耦合设备	proximity coupling device	5.60
接近式支付交易	proximity payment transaction	6.28
接近式支付设备	proximity payment device	5.61
接口设备	interface device	5.58
解扣出错计数器	GMAC count	7.96
解密	decipherment	8.46
借记交易	debit transaction	6.43
借记卡	debit card	3.3
金融报文	financial message	7.24
金融交易	financial transaction	6.13
金融类撤销交易	financial transaction cancellation	6.33
金融税控收款机	fiscal cash register with EFT (electronic fund transfer) function	5.19
金融业务专用机具	special machines and tools for financial bussiness	5.1
静态密钥	static key	8.33

静态数据认证	static data authentication	8.151
静态数据认证标签	static data authentication (SDA) tag for signing	8.153
静止状态	inactive	7.11
K		
卡段	card range	3.45
卡号	card number	3.41
卡片的"发卡后"应用更新	post-issuance updates	6.157
卡片读写设备	card acceptor device	5.50
卡片风险管理	card risk management	8.149
卡片复制	card reproduction	6.143
卡片认证方法	card authentication methodology	8.159
卡片行为分析	card action analysis	8.145
卡片验证结果	card verification result	8.144
卡片验证码	card verification number	8.7
卡片验证码 2	card verification number 2	8.8
卡片有效期	expiration date	3.50
卡支付系统	card payment system	7.53
抗攻击性	tamper-resistant characteristic	8.196
可检测功能	testably function	3.51
可逆加密	reversible encipherment	8.44
可燃性	flammability	3.64
可信第三方	trusted third party	4.14
可用资金	available fund	6.131
客户输入模块	customer input module	5.34
跨地区交易	interregional settlement	6.23
跨地区结算	interregional interchange	6.24
跨国交易	international transaction	6.25
跨行转账	inter bank transfer	6.26
L		
类型 ABC	class ABC	7.7
累计脱机交易金额上限	upper cumulative offline transaction amount	7.87
累计脱机交易金额下限检查	lower cumulative offline transaction amount check	7.86
冷复位	cold reset	7.9
离行式	off-bank mode	5.13
例外长款处理	exceptional surplus processing	6.106
例外处理	exception	6.104
例外协商回复	exception consultation response	6.107
例外协商交易	exception consultation	6.105
连续脱机交易次数上限	upper consecutive offline limit	7.84
连续脱机交易次数下限	lower consecutive offline limit	7.85
联机 PIN 验证	online PIN verification	8.15
联机方式	online mode	7.16
联机交易	online transaction	7.15

联机卡片认证密文	online card authentication cryptogram	8.169
联机终端	online terminal	5.7
联系发卡行交易	refer to issuer transaction	6.30
邻近式 IC 卡	vicinity IC card	3.38
邻近式耦合设备	vicinity coupling device	5.59
逻辑安全性	logical security	8.82
逻辑加密卡	smart card with security logic	3.28
逻辑泄露	logical compromise	8.63
M		
MAC 密钥	message authentication code key	8.70
密码服务报文	cryptographic service message	8.32
密码函数	cryptographic function	8.42
密码计算	ciphering	8.41
密码键盘	encrypting PIN pad	5.54
密码节点	cryptographic node	8.30
密码链	cryptographic link	8.29
密码模块	cryptographic module	5.35
密码生成	PIN generation	8.56
密码系统	cryptosystem	8.47
密码修改/解锁	PIN change/unblock	8.23
密码学	cryptography	8.89
密文	cryptogram	8.40
密钥	key	8.26
密钥的不可逆转换	irreversible transformation of a key	8.27
密钥对的所有者	key pair owner	8.122
密钥分割	split knowledge	8.110
密钥更换	key replacement	8.58
密钥回收	key revocation	8.59
密钥加密密钥	key encryption key	8.76
密钥空间	key space	8.111
密钥粒度	key granularity	8.28
密钥偏移量	key offset	8.114
密钥生成模块	key generation module	5.36
密钥生命周期	key life cycle	8.55
密钥同步	key synchronization	8.31
密钥信封	key mailer	8.112
密钥要素	keying material	8.38
密钥引入	key introduction	8.57
密钥有效期	cryptoperiod	8.54
密钥装载模块	key loading module	5.37
密钥组件	key component	8.113
免息期	interest-free period	6.137
敏感数据 (信息)	sensitive data (information)	8.10
明文	plaintext	8.36

命令	command	7.22
末端证书	end certificate	8.129
目录定义文件	directory definition file	7.71
N		
n 位分组密码	n-bit block cipher	8.93
耐化学性	resistance to chemicals	3.58
P		
PASM 卡	PSAM card	8.87
PIN 尝试次数计数器	PIN try counter	8.161
PIN 尝试限制	PIN try limit	8.162
PIN 加密密钥	PIN key	8.71
PIN 输入设备	PIN entry device	5.53
PIN 验证	PIN verification	8.14
PIN 验证码	PIN verification number	8.21
PIN 验证密钥	PIN verification key	8.22
POS 参考号	POS reference number	6.9
POS 交易批次号	POS transaction batch number	6.10
POS 流水号	POS trace number	6.11
POS 前置处理系统	POS front-end processing system	7.57
POS 输入方式	entry mode of POS	6.12
批准	approved	6.75
批准响应	approval response	7.65
平均信号幅度	average signal amplitude	3.55
凭条打印模块	receipt print module	5.27
凭证	receipt	6.121
Q		
签名的动态应用数据	signed dynamic application data	8.155
签名的静态应用数据	signed static application data	8.152
签名条	signature panel	3.46
潜在泄露	potential compromise	8.62
翘曲	warpage	3.60
清分	clearing	6.80
清算	settlement	6.81
清算日	settlement business date	6.84
清算数据	settlement data	6.85
清算账户	clearing account	6.86
清算滞纳金	settlement late fee	6.87
请款	presentment	6.93
请求类交易	request transaction	6.41
圈存	load	6.149
圈存交易凭证	load transaction receipt	6.155
圈提	unload	6.156
确认查询	confirmation inquiry	6.91
R		

RSA 加密算法	Rivest Shamir Adleman	8.98
热复位	warm reset	7.8
认证	certification	8.131
认证业务申明	certification practice statement	8.135
认证中心	certification authority	4.15
认证中心公钥索引	certification authority public key index	8.176
日志打印模块	journal print module	5.28
软件加密	software encryption	8.88
S		
三磁	track 3	3.24
商户类别代码	merchant category code	7.43
商户退单比率	merchant chargeback rate	6.122
设备安全性	device security	8.81
设陷盗取出钞	trapping for cash	8.184
设陷盗取存款	trapping for deposit	8.183
生物特征验证	biometric verification	8.6
时间变量参数	time variant parameter	8.109
时间槽协议	time slot protocol	7.12
识别卡	identification card	3.1
实体鉴别	entity authentication	8.51
收单网关	acquiring gateway	7.64
收银终端	cash register terminal	5.18
授权	authorization	6.53
授权报文	authorization message	7.31
授权参考	referral call	6.55
授权参考号	authorization reference number	6.56
授权撤销交易	authorization cancellation transaction	6.57
授权交易	authorization transaction	6.54
授权请求	authorization request	6.59
授权请求密文	authorization request cryptogram	8.166
授权日志	authorization log	6.60
授权响应	authorization response	6.61
授权响应密文	authorization response cryptogram	8.167
授权者	grantor	4.27
授权终端	authorization terminal	5.8
数据安全模块	data security module	5.23
数据对象列表	data object list	7.93
数据加密标准	data encryption standard	8.91
数据加密算法	data encryption algorithm	8.92
数据完整性	data integrity	8.24
数字签名	digital signature	8.48
数字签名系统	digital signature system	7.61
双信息交易	dual message transaction	6.16
双重控制	dual control	8.106

私有协议	private agreement	6.120
私钥	private key	8.115
T		
TIM 卡	TIM card	3.33
TKEY 卡	TKEY card	3.34
TSAM 卡	TSAM card	3.35
套卡	card family	3.9
提前回收	accelerated revocation	8.61
替换	replace	8.193
通信方	communicating party	4.9
通讯服务	communication service	6.14
通知报文	advice message	7.33
凸起区	raised area	3.48
凸印	embossing	3.47
退单	chargeback	6.96
退货	refund	6.77
托收	collection	6.78
脱机 PIN 验证	offline PIN verification	8.16
脱机方式	offline mode	7.17
脱机终端	offline terminal	5.6
W		
弯曲韧性	bending stiffness	3.61
完全迁移的发卡机构	full issuer	4.7
完整的芯片卡交易	whole chip card transaction	6.29
伪随机	pseudo-random	8.107
伪随机数	pseudo-random number	8.108
未使用的卡	unused card	3.10
位冲突检测协议	bit collision detection protocol	7.10
文件发送方	file sender	4.13
文件接收方	file acceptor	4.12
无触点的	contactless	3.36
无法识别的服务代码	unrecognized service code	7.47
无卡环境	card-absent environment	6.36
无人值守支付终端	unattended payment terminal	5.10
物理安全性	physical security	8.83
物理泄露	physical compromise	8.64
X		
洗单	factoring	8.191
系统成功率	success ratio of system	7.62
系统跟踪审计号	system trace audit number	6.7
现金充值	cash replenishing	6.50
现金存款机	cash deposit machine	5.43
响应	response	7.19
响应报文	response message	7.34

响应方	respondent	4.11
响应码	response code	7.21
响应时间	response time	7.20
销售点系统	point-of-sale system	7.56
销售点终端	point-of-sale terminal	5.20
校验码	check code	7.42
协商解决	negotiated solutions	6.103
泄露	compromise	8.187
信用额度	credit line	6.135
信用卡	credit card	3.4
信用卡透支	overdraft of credit card	6.136
Y		
延迟付款	delayed payment	6.52
掩膜	mask	3.31
一磁	track 1	3.21
一次请款	first presentment	6.94
一次退单	first chargeback	6.97
一次一密	derived unique key per transaction	8.35
银联标识	CUP logo	4.3
银亭	kiosk bank	5.17
银行卡	bank card	3.2
银行卡交易交换网络	exchange network for bank card transaction	4.1
银行卡前置设备	prepositive facility of bank card network	5.48
银行自助设备	bank self-service equipment	5.12
应用	application	7.18
应用标签	application label	6.145
应用标识	application identifier	6.146
应用参考货币代码	application reference currency code	7.80
应用定义文件	application definition file	7.73
应用货币指数	application currency exponent	7.81
应用基本文件	application elementary file	7.72
应用交互特征	application interchange profile	7.89
应用交易计数器	application transaction counter	7.88
应用密文	application cryptogram	8.164
应用认证密文	application authentication cryptogram	8.168
应用首选名称	application preferred name	6.148
应用授权参考	application authorization referral	8.165
应用提供商	application provider	4.19
应用文件定位器	application file locator	7.77
应用选择指示符	application selection indicator	7.76
应用用途控制	application usage control	7.82
应用优先指示器	application priority indicator	7.75
硬件安全装置	physically secure device	5.57
硬件加密	hardware encryption	8.77

硬件加密机	hardware and security module	8.78
用户移动终端	user mobile terminal	5.47
有卡环境	card-present environment	6.35
预个人化数据	pre-personalization data	7.91
预授权	pre-authorization	6.62
预授权撤销	pre-authorization cancellation	6.63
预授权完成	pre-authorization completion	6.64
预授权完成（请求）交易	pre-authorization completion transaction (request)	6.65
预授权完成（手工）	pre-authorization completion (manual)	6.66
预授权完成（通知）交易	pre-authorization completion transaction (advice)	6.67
预授权完成撤销	cancellation of pre-authorization completion	6.68
Z		
再请款	re-presentment	6.95
再提交	resubmission	7.37
在行式	in-bank mode	5.14
粘连或并块	adhesion or blocking	3.59
占挂资金	held amount	6.134
账户历史数据	account historical data	4.17
账户数据泄露事件	account data compromise event	8.181
争议	dispute	6.99
证书	certificate	8.125
证书标识符	certificate identifier	8.126
证书挂起	certificate hold	8.137
证书回收	certificate revocation	8.138
证书回收列表	certificate revocation list	8.139
证书链	certificate link	8.127
证书使用系统	certificate-using system	8.136
支付网关	payment gateway	7.63
支付系统环境	payment system environment	7.66
直联	direct connection	7.13
止付名单系统	system of stop payment name list	7.60
指定账户圈存	specific account load	6.153
智能卡	smart card	3.29
中国银联安全输入模式	China UnionPay secure information collection mode	8.101
中间证书	intermediate certificate	8.128
终端	terminal	5.2
终端 MAC 密钥	terminal MAC key	8.73
终端 PIN 密钥	terminal PIN key	8.74
终端标识码	terminal identification number	5.3
终端风险管理	terminal risk management	8.150
终端国家代码	terminal country code	7.79
终端控制模块	terminal control module	5.26
终端行为代码	terminal action code	8.148
终端验证结果	terminal verification results	8.146

终端主密钥	terminal master key	8.72
重复	repeat	7.36
主机安全模块	host security module	8.86
主卡	main card	3.7
主密钥	primary key	8.65
主文件	master file	7.69
主应用	primary application	6.144
主账号序列号	primary account number sequence number	3.42
注册的应用提供商标识	registered application provider identifier	6.147
专用文件	dedicated file	7.70
转入确认	transfer-in confirmation	6.45
转账	transfer	6.44
追加预授权	supplementary pre-authorization	6.69
准贷记卡	semi-credit card	3.6
资金结算交易	settlement transaction	6.89
字典攻击	dictionary attack	8.194
（字符的）凸印起伏高度	embossing relief height (of character)	3.49
自动柜员机	automatic teller machine	5.21
自动圈存	auto-load	6.150
自动售货机	automatic vending machine	5.42
自动售油机	automatic fuel vending machine	5.41
自主清算	self-determination settlement	6.82
自助终端	self-service terminal	5.9
最低限额	floor limit	7.83

附录 B
(资料性附录)
银行卡名词术语英文索引

A

accelerated revocation	提前回收	8.61
account data compromise event	账户数据泄露事件	8.181
account historical data	账户历史数据	4.17
acquiring gateway	收单网关	7.64
address verification	地址验证	8.5
ADFAallocation	ADF 分配	6.5
adhesion or blocking	粘连或并块	3.59
adjustment	差错交易	6.90
adjustment platform	差错处理平台	7.50
advice message	通知报文	7.33
agency payment	代付交易	6.39
agent service	代理业务	6.37
application	应用	7.18
application authentication cryptogram	应用认证密文	8.168
application authorization referral	应用授权参考	8.165
application cryptogram	应用密文	8.164
application currency exponent	应用货币指数	7.81
application definition file	应用定义文件	7.73
application elementary file	应用基本文件	7.72
application file locator	应用文件定位器	7.77
application identifier	应用标识	6.146
application interchange profile	应用交互特征	7.89
application label	应用标签	6.145
application preferred name	应用首选名称	6.148
application priority indicator	应用优先指示器	7.75
application provider	应用提供商	4.19
application reference currency code	应用参考货币代码	7.80
application selection indicator	应用选择指示符	7.76
application transaction counter	应用交易计数器	7.88
application usage control	应用用途控制	7.82
approval response	批准响应	7.65
approved	批准	6.75
arbitrage	裁判	6.108
asymmetric algorithm	非对称算法	8.117
asymmetric cipher	非对称密码	8.123
asymmetric cryptographic technique	非对称加密技术	8.120
asymmetric cryptosystem	非对称密码体系	8.118

asymmetric key pair	非对称密钥对	8.121
asymmetric key pair generator	非对称密钥对生成器	8.124
ATM authorization	ATM 授权	6.72
ATM cash withdraw	ATM 取现	6.71
ATM inquiry	ATM 查询	6.70
ATM safe	ATM 保险柜	5.22
ATM safety monitor module	ATM 安全监控模块	5.29
authentication	鉴别	8.49
authentication key	鉴别密钥	8.50
authorization	授权	6.53
authorization cancellation transaction	授权撤销交易	6.57
authorization log	授权日志	6.60
authorization message	授权报文	7.31
authorization reference number	授权参考号	6.56
authorization request	授权请求	6.59
authorization request cryptogram	授权请求密文	8.166
authorization response	授权响应	6.61
authorization response cryptogram	授权响应密文	8.167
authorization terminal	授权终端	5.8
authorization transaction	授权交易	6.54
authorized customer	合法用户	4.26
auto-load	自动圈存	6.150
automatic fuel vending machine	自动售油机	5.41
automatic teller machine	自动柜员机	5.21
automatic teller machine front-end processing system	ATM 前置处理系统	7.55
automatic vending machine	自动售货机	5.42
available fund	可用资金	6.131
average signal amplitude	平均信号幅度	3.55
B		
balance inquiry	查询余额	6.48
bank book print module	存折打印模块	5.33
bank card	银行卡	3.2
bank self-service equipment	银行自助设备	5.12
bending stiffness	弯曲韧性	3.61
biometric verification	生物特征验证	8.6
bit collision detection protocol	位冲突检测协议	7.10
block of IINs	IIN 的块	6.6
C		
CA certificate	CA 证书	8.130
cancellation of pre-authorization completion	预授权完成撤销	6.68
card acceptor device	卡片读写设备	5.50
card action analysis	卡片行为分析	8.145
card authentication methodology	卡片认证方法	8.159
card family	套卡	3.9

card number	卡号	3.41
card payment system	卡支付系统	7.53
card range	卡段	3.45
card reproduction	卡片复制	6.143
card risk management	卡片风险管理	8.149
card verification number	卡片验证码	8.7
card verification number 2	卡片验证码 2	8.8
card verification result	卡片验证结果	8.144
card-absent environment	无卡环境	6.36
cardholder	持卡人	4.23
cardholder access device	持卡人接入设备	5.49
cardholder certificate	持卡人证书	8.99
cardholder discount	持卡人折扣	6.138
cardholder identification	持卡者标识	4.25
cardholder identification value	持卡人身份识别值	8.12
cardholder-activated terminal	持卡人自助终端	5.11
card-present environment	有卡环境	6.35
cash deposit machine	现金存款机	5.43
cash register terminal	收银终端	5.18
cash replenishing	现金充值	6.50
cash replenishment period	加钞周期	6.73
cash teller module	出钞模块	5.24
certificate	证书	8.125
certificate hold	证书挂起	8.137
certificate identifier	证书标识符	8.126
certificate link	证书链	8.127
certificate revocation	证书回收	8.138
certificate revocation list	证书回收列表	8.139
certificate-using system	证书使用系统	8.136
certification	认证	8.131
certification authority	认证中心	4.15
certification authority public key index	认证中心公钥索引	8.176
certification practice statement	认证业务申明	8.135
charge	费用	6.127
chargeback	退单	6.96
check code	校验码	7.42
China UnionPay secure	CUPSecure	8.100
China UnionPay secure information collection mode	中国银联安全输入模式	8.101
ciphering	密码计算	8.41
class ABC	类型 ABC	7.7
clearing	清分	6.80
clearing account	清算账户	6.86
coercivity	矫顽力	3.52
cold reset	冷复位	7.9

collection	代收交易	6.38
collection	托收	6.78
collision	冲突	7.97
combined IC and magnetic stripe card	磁条芯片复合卡	3.30
command	命令	7.22
communicating party	通信方	4.9
communication service	通讯服务	6.14
compromise	泄露	8.187
concatenation	串联	7.5
confirmation inquiry	确认查询	6.91
contact	触点	3.32
contactless	无触点的	3.36
contactless card	非接触卡	3.37
credit adjustment	贷记调整	6.92
credit card	贷记卡	3.5
credit card	信用卡	3.4
credit line	信用额度	6.135
credit transaction	贷记交易	6.42
CRL distribution point	CRL 分发点	8.140
cross certification	交叉认证	8.132
crypto check digital	加密校验数	8.9
cryptogram	密文	8.40
cryptographic equipment	加密设备	8.79
cryptographic function	密码函数	8.42
cryptographic link	密码链	8.29
cryptographic module	密码模块	5.35
cryptographic node	密码节点	8.30
cryptographic service message	密码服务报文	8.32
cryptology	密码学	8.89
cryptoperiod	密钥有效期	8.54
cryptosystem	密码系统	8.47
cryptographic algorithm	加密算法	8.90
CUP logo	银联标识	4.3
customer input module	客户输入模块	5.34
CVM list	持卡人验证方法列表	8.142
CVM result	持卡人验证方法结果	8.143
D		
data encryption algorithm	数据加密算法	8.92
data encryption standard	数据加密标准	8.91
data integrity	数据完整性	8.24
data object list	数据对象列表	7.93
data security module	数据安全模块	5.23
debit card	借记卡	3.3
debit transaction	借记交易	6.43

decipherment	解密	8.46
dedicated file	专用文件	7.70
delayed payment	延迟付款	6.52
deposit module	存款模块	5.25
derivation key	根密钥	8.66
derivation parameter	分散参数	8.68
derived key	导出密钥	8.67
derived unique key per transaction	一次一密	8.35
detail inquiry	查询明细	6.49
device security	设备安全性	8.81
dictionary attack	字典攻击	8.194
digital signature	数字签名	8.48
digital signature system	数字签名系统	7.61
dimensional stability	尺寸稳定性	3.63
direct connection	直联	7.13
directory definition file	目录定义文件	7.71
dispute	争议	6.99
domestic transaction	国内交易	6.17
dual control	双重控制	8.106
dual message transaction	双信息交易	6.16
dynamic bending stress	动态弯曲应力	3.62
dynamic currency conversion	动态币种转换	6.112
dynamic data authentication	动态数据认证	8.154
dynamic data authentication data object list	动态数据认证数据对象列表	8.156
dynamic key	动态密钥	8.34
dynamic online	动态联机卡片认证方法	8.160
E		
early issuer	部分迁移的发卡机构	4.6
electronic cabin	电子柜	5.38
electronic cash	电子现金	6.125
electronic deposit	电子存折	6.123
electronic fund transfer at point-of-transaction	交易点的电子资金转账	7.52
electronic fund transfer system	电子资金转账系统	7.51
electronic funds transfer	电子资金转账	6.126
electronic lock	电子锁	5.39
electronic purse	电子钱包	6.124
elementary file	基本文件	7.68
embedder	封装机构	4.20
embossing	凸印	3.47
embossing relief height (of character)	(字符的)凸印起伏高度	3.49
EMV standard	EMV 标准	6.1
EMVCo	EMV 机构	4.8
encipherment element	待加密元素	8.37

encrypted PIN data	加密 PIN 值	8.20
encrypting PIN pad	密码键盘	5.54
encryption	加密	8.43
end certificate	末端证书	8.129
entity authentication	实体鉴别	8.51
entry mode of POS	POS 输入方式	6.12
exception	例外处理	6.104
exception consultation	例外协商交易	6.105
exception consultation response	例外协商回复	6.107
exceptional surplus processing	例外长款处理	6.106
exchange	交换	7.23
exchange network for bank card transaction	银行卡交易交换网络	4.1
expiration date	卡片有效期	3.50
expired card	过期卡	3.13
F		
factoring	洗单	8.191
fallback	降级使用交易	6.32
file acceptor	文件接收方	4.12
file sender	文件发送方	4.13
financial message	金融报文	7.24
financial transaction	金融交易	6.13
financial transaction cancellation	金融类撤销交易	6.33
first chargeback	一次退单	6.97
first presentment	一次请款	6.94
first subsidiary account number	第一辅助账号	3.43
fiscal cash register with EFT (electronic fund transfer)	金融税控收款机	5.19
function		
fishing	钓盗现金	8.185
flammability	可燃性	3.64
floor limit	最低限额	7.83
flux transition	磁通翻转	3.53
forcing	暴力取现	8.186
full issuer	完全迁移的发卡机构	4.7
G		
GMAC count	解扣出错计数器	7.96
grantor	授权者	4.27
guard time	保护时间	7.1
H		
hardware and security module	硬件加密机	8.78
hardware encryption	硬件加密	8.77
hash algorithm indicator	哈希算法标识符	8.96
hash function	哈希函数	8.95
hash result	哈希结果	8.97
held amount	占挂资金	6.134

host security module	主机安全模块	8.86
I		
IC assembling	IC 的组装	6.3
IC assembly	IC 组件	6.4
IC embedding	IC 的封装	6.2
ICA number	ICA 号	4.2
ICC dynamic number	IC 卡动态数	7.78
ICC private key	IC 卡私钥	8.141
ICC reader and writer	IC 卡读写器	5.52
ICC transaction	IC 卡交易	6.27
IC-only system	单一 IC 系统	7.54
ID-000 card	ID-000 型卡	3.14
ID-1 card	ID-1 型卡	3.15
ID-2 card	ID-2 型卡	3.16
ID-3 card	ID-3 型卡	3.17
identification card	识别卡	3.1
immediate fund	即用资金	6.132
inactive	静止状态	7.11
in-bank mode	在行式	5.14
indirect connection	间联	7.14
initial text sequence	初始文本序列	7.4
initialization vector	初始化向量	8.39
initiator	发起方	4.10
in-lobby mode	大堂式	5.16
installment	分期付款	6.51
integrated circuit	集成电路	3.25
integrated circuit card	集成电路卡	3.26
integrated circuit card terminal	IC 卡终端	5.5
integrated circuit manufacturer	集成电路厂商	4.21
integrated circuit module	集成电路模块	5.32
inter bank transfer	跨行转账	6.26
interactive message	交互报文	7.32
interest-free period	免息期	6.137
interface device	接口设备	5.58
intermediate certificate	中间证书	8.128
international transaction	跨国交易	6.25
interregional interchange	跨地区结算	6.24
interregional settlement	跨地区交易	6.23
intracurrency settlement service	货币清算服务	6.88
irreversible encipherment	不可逆加密	8.45
irreversible transformation of a key	密钥的不可逆转换	8.27
issuer	发卡行	4.4
issuer action code	发卡行行为代码	8.147
issuer application data	发卡行应用数据	8.174

issuer authentication data	发卡行认证数据	8.175
issuer identification area	发卡行标识域	3.40
issuer identification number	发卡行标识代码	4.5
issuer master data encipherment DEA key	发卡行加密主密钥	8.172
issuer master message authentication code key	发卡行 mac 主密钥	8.173
issuer private key	发卡行私钥	8.180
issuer public key certificate	发卡行公钥证书	8.179
issuer public key exponent	发卡行公钥指数	8.177
issuer public key remainder	发卡行公钥余数	8.178
issuer secure authentication and authorization mode	发卡行直接认证授权模式	8.170
J		
journal print module	日志打印模块	5.28
K		
key	密钥	8.26
key component	密钥组件	8.113
key encryption key	密钥加密密钥	8.76
key generation module	密钥生成模块	5.36
key granularity	密钥粒度	8.28
key introduction	密钥引入	8.57
key life cycle	密钥生命周期	8.55
key loading module	密钥装载模块	5.37
key mailer	密钥信封	8.112
key offset	密钥偏移量	8.114
key pair owner	密钥对的所有者	8.122
key replacement	密钥更换	8.58
key revocation	密钥回收	8.59
key space	密钥空间	8.111
key synchronization	密钥同步	8.31
keying material	密钥要素	8.38
kiosk bank	银亭	5.17
L		
linked load	关联圈存	6.151
load	圈存	6.149
load on unspecific account	非指定账户圈存	6.154
load transaction receipt	圈存交易凭证	6.155
local authorization	本地授权	6.21
local settlement	本地结算	6.20
local transaction	本地交易	6.18
local transaction receipt	本地交易凭证	6.19
logical compromise	逻辑泄露	8.63
logical security	逻辑安全性	8.82
lower consecutive offline limit	连续脱机交易次数下限	7.85
lower cumulative offline transaction amount check	累计脱机交易金额下限	7.86

		检查	
M			
magnetic stripe		磁条	3.18
magnetic stripe card		磁条卡	3.19
magnetic stripe image		磁条镜像	7.6
magnetic stripe reader		磁条阅读器	5.51
magnetic stripe terminal		读磁条终端	5.4
main card		主卡	3.7
manipulate		操纵	8.190
mask		掩膜	3.31
master file		主文件	7.69
mechanical lock		机械密码锁	5.40
memory card		存储卡	3.27
merchant category code		商户类别代码	7.43
merchant chargeback rate		商户退单比率	6.122
message authentication		报文鉴别	8.52
message authentication code		报文鉴别码	8.53
message authentication code key		MAC 密钥	8.70
message bit map		报文位图	7.28
message digest		报文摘要	7.29
message forwarding		报文转发	7.38
message function		报文功能	7.27
message identifier		报文标识符	7.26
message type code		报文类型代码	7.25
misembossed card		错误制卡	3.11
misencoded card		编码错卡	3.12
multimedia function module		多媒体功能模块	5.30
multimedia public payment terminal		多媒体公共支付终端	5.45
N			
natural PIN		初始密码	8.17
n-bit block cipher		n 位分组密码	8.93
negotiated solutions		协商解决	6.103
non-repudiation		不可否认性	8.25
O			
off-bank mode		离行式	5.13
offline mode		脱机方式	7.17
offline PIN verification		脱机 PIN 验证	8.16
offline terminal		脱机终端	5.6
online card authentication cryptogram		联机卡片认证密文	8.169
online mode		联机方式	7.16
online PIN verification		联机 PIN 验证	8.15
online terminal		联机终端	5.7
online transaction		联机交易	7.15
on-us transaction		本行交易	6.22

operator	操作员	4.28
operator's display module	后台维护模块	5.31
overdraft of credit card	信用卡透支	6.136
P		
partial authorization	部分授权	6.58
payment gateway	支付网关	7.63
payment system environment	支付系统环境	7.66
peel strength	剥离强度	3.57
penetrate	穿透	8.188
persistent connect	长连接	7.3
personal authenticating information	个人鉴别信息	8.11
personal identification number	个人识别码	4.24
personalization	个人化	6.142
personalization data	个人化数据	7.92
personalizer	ADF 个人化机构	4.22
physical compromise	物理泄露	8.64
physical security	物理安全性	8.83
physically secure device	硬件安全装置	5.57
PIN change/unblock	密码修改/解锁	8.23
PIN entry device	PIN 输入设备	5.53
PIN generation	密码生成	8.56
PIN key	PIN 加密密钥	8.71
PIN try counter	PIN 尝试次数计数器	8.161
PIN try limit	PIN 尝试限制	8.162
PIN verification	PIN 验证	8.14
PIN verification key	PIN 验证密钥	8.22
PIN verification number	PIN 验证码	8.21
plaintext	明文	8.36
planned revocation	按计划的回收	8.60
point of service entry mode	服务点输入方式码	7.45
point of transaction	交易点	6.100
point-of-sale system	销售点系统	7.56
point-of-sale terminal	销售点终端	5.20
policy mapping	策略映射	8.133
policy qualifier	策略限定符	8.134
POS front-end processing system	POS 前置处理系统	7.57
POS reference number	POS 参考号	6.9
POS trace number	POS 流水号	6.11
POS transaction batch number	POS 交易批次号	6.10
post-issuance application change	发卡后应用修改	6.158
post-issuance application load	发卡后应用装载	6.159
post-issuance updates	卡片的"发卡后"应用更新	6.157
potential compromise	潜在泄露	8.62

pre-authorization	预授权	6.62
pre-authorization cancellation	预授权撤销	6.63
pre-authorization completion	预授权完成	6.64
pre-authorization completion (manual)	预授权完成（手工）	6.66
pre-authorization completion transaction (advice)	预授权完成（通知）交易	6.67
pre-authorization completion transaction (request)	预授权完成（请求）交易	6.65
pre-personalization data	预个人化数据	7.91
prepositive facility of bank card network	银行卡前置设备	5.48
presentment	请款	6.93
primary account number sequence number	主账号序列号	3.42
primary application	主应用	6.144
primary key	主密钥	8.65
private agreement	私有协议	6.120
private key	私钥	8.115
processing fee	处理费	6.128
processing options data object list	处理选项数据对象列表	7.94
processing priority	处理优先级	7.40
processing priority code	处理优先级代码	7.41
promotion code	促销代码	7.44
proximity coupling device	接近式耦合设备	5.60
proximity IC card	接近式 IC 卡	3.39
proximity payment device	接近式支付设备	5.61
proximity payment transaction	接近式支付交易	6.28
PSAM card	PASM 卡	8.87
pseudo-random	伪随机	8.107
pseudo-random number	伪随机数	8.108
public key	公钥	8.116
public key distribution system	公钥分配体系	8.119
public payment platform	公共支付平台	7.49
public payment terminal	公共支付终端	5.44
public service platform	公共服务平台	7.48
R		
raised area	凸起区	3.48
receipt	凭证	6.121
receipt print module	凭条打印模块	5.27
refer to issuer transaction	联系发卡行交易	6.30
reference CIV	参考 CIV	8.13
reference current	基准电流	3.56
reference PIN	参考 PIN	8.19
reference signal amplitude	基准信号幅度	3.54
referral call	授权参考	6.55
reflection attack	反射攻击	8.195
refund	退货	6.77
registered application provider identifier	注册的应用提供商标识	6.147

repeat	重复	7.36
replace	替换	8.193
re-presentment	再请款	6.95
request transaction	请求类交易	6.41
resistance to chemicals	耐化学性	3.58
respondent	响应方	4.11
response	响应	7.19
response code	响应码	7.21
response message	响应报文	7.34
response time	响应时间	7.20
resubmission	再提交	7.37
retrieval	调单	6.100
retrieval postponement	调单展期	6.102
retrieval response	调单回复	6.101
reversal	冲正	6.76
reversal transfer	撤销转账	6.47
reverse	撤销	7.35
reversible encipherment	可逆加密	8.44
risk reserve fund	风险备付金	6.133
Rivest Shamir Adleman	RSA 加密算法	8.98
S		
script	脚本	7.90
second chargeback	二次退单	6.98
second subsidiary account number	第二辅助账号	3.44
secret key	保密密钥	8.105
secure application module	安全应用模块	8.85
secure cryptographic device	安全加密设备	5.55
secure electronic commercial transaction	安全电子商务交易	6.74
secure hash algorithm-1	安全哈希算法-1	8.94
secure messaging	安全报文交换	8.171
security audit trail	安全审计踪迹	8.3
security compliance check list	安全符合性检测清单	8.84
security cryptographic device interface	安全加密设备界面	8.80
security environment	安全环境	8.1
security handling fee and reward	安全处理费用及酬劳	6.129
security printing	安全印制	8.4
security status	安全状态	8.2
self-determination settlement	自主清算	6.82
self-service terminal	自助终端	5.9
semi-credit card	准贷记卡	3.6
sensitive data (information)	敏感数据 (信息)	8.10
service code	服务代码	7.46
session key	会话密钥	8.75
settlement	清算	6.81

settlement business date	清算日	6.84
settlement data	清算数据	6.85
settlement late fee	清算滞纳金	6.87
settlement transaction	资金结算交易	6.89
setup/cancellation clientage transaction	建立/撤销委托关系交易	6.34
short file identifier	短文件标识符	7.74
signature panel	签名条	3.46
signed dynamic application data	签名的动态应用数据	8.155
signed static application data	签名的静态应用数据	8.152
simplified chip card transaction	简化的芯片卡交易	6.31
single message transaction	单信息交易	6.15
skimming	侧录	8.192
smart card	智能卡	3.29
smart card with security logic	逻辑加密卡	3.28
software encryption	软件加密	8.88
special machines and tools for financial bussiness	金融业务专用机具	5.1
specific account load	指定账户圈存	6.153
split knowledge	密钥分割	8.110
split transaction	分单	6.79
spy	监视	8.189
stand-in authorization	代授权	6.40
static data authentication	静态数据认证	8.151
static data authentication (SDA) tag for signing	静态数据认证标签	8.153
static key	静态密钥	8.33
store and forward	存储转发	7.39
subject CA	从属认证中心	4.16
success ratio of system	系统成功率	7.62
supplementary card	副卡	3.8
supplementary details	补充明细	6.139
supplementary pre-authorization	追加预授权	6.69
surface roughness	表面粗糙度	3.65
symmetric algorithm	对称算法	8.102
symmetric cipher	对称密码	8.104
symmetric cryptographic technique	对称加密技术	8.103
system of delinquent cardholder	不良持卡人系统	7.59
system of delinquent merchant	不良商户系统	7.58
system of stop payment name list	止付名单系统	7.60
system trace audit number	系统跟踪审计号	6.7
T		
TAC unread flag	交易验证码待读标志	7.95
tag, length, value	标签、长度、数值	7.67
tamper-evident characteristic	防攻击性	8.197
tamper-evident device	防攻击设备	5.56
tampering	攻击	8.182

tamper-resistant characteristic	抗攻击性	8.196
tamper-responsive characteristic	反攻击性	8.198
telephone payment centre	电话支付中心	4.18
telephone payment terminal	电话支付终端	5.46
terminal	终端	5.2
terminal action code	终端行为代码	8.148
terminal control module	终端控制模块	5.26
terminal country code	终端国家代码	7.79
terminal identification number	终端标识码	5.3
terminal MAC key	终端 MAC 密钥	8.73
terminal master key	终端主密钥	8.72
terminal PIN key	终端 PIN 密钥	8.74
terminal risk management	终端风险管理	8.150
terminal verification results	终端验证结果	8.146
test method	测试方法	6.141
testably function	可检测功能	3.51
third-party transfer	第三方转账	6.46
through-wall mode	穿墙式	5.15
TIM card	TIM 卡	3.33
time slot protocol	时间槽协议	7.12
time variant parameter	时间变量参数	8.109
timeout value	超时限值	6.140
TKEY card	TKEY 卡	3.34
track 1	一磁	3.21
track 2	二磁	3.22
track 2 equivalent data	二磁等价数据	3.23
track 3	三磁	3.24
track data	磁道数据	3.20
transaction amount	交易金额	6.115
transaction audit trail	交易记录明细	6.114
transaction authorization cryptogram	交易验证码	8.163
transaction certificate	交易证书	8.157
transaction certificate data object list	交易证书数据对象列表	8.158
transaction counter	交易计数器	6.113
transaction country	交易国家	6.111
transaction date	交易日期	6.117
transaction fee	交易费	6.130
transaction information document	交易信息文档	6.119
transaction log	交易日志	6.118
transaction message	交易报文	7.30
transaction PIN	交易 PIN	8.18
transaction reference number	交易参考号	6.8
transaction success ratio	交易成功率	6.109
transaction type code	交易类型代码	6.116

transfer	转账	6.44
transfer-in confirmation	转入确认	6.45
transitory connect	短连接	7.2
trapping for cash	设陷盗取出钞	8.184
trapping for deposit	设陷盗取存款	8.183
trusted third party	可信第三方	4.14
TSAM card	TSAM 卡	3.35
unattended payment terminal	无人值守支付终端	5.10
unlinked load	非关联圈存	6.152
unload	圈提	6.156
	U	
unrecognized service code	无法识别的服务代码	7.47
unself-determination settlement	非自主清算	6.83
unused card	未使用的卡	3.10
upper consecutive offline limit	连续脱机交易次数上限	7.84
upper cumulative offline transaction amount	累计脱机交易金额上限	7.87
user mobile terminal	用户移动终端	5.47
	V	
vicinity coupling device	邻近式耦合设备	5.59
vicinity IC card	邻近式 IC 卡	3.38
	W	
warm reset	热复位	7.8
warpage	翘曲	3.60
whole chip card transaction	完整的芯片卡交易	6.29
working key	工作密钥	8.69

参考文献

- [1] GB/T 10112—1999 术语工作 原则与方法 (ISO/DIS 704:1997, NEQ)
- [2] GB/T 15237.1—2000 术语工作 词汇 第1部分:理论与应用 (ISO 1087-1:2000, EQV)
- [3] GB/T 15694.2—2002 识别卡 发卡者的标识 第2部分:应用和注册规程 (ISO/IEC 7812-2:2000, IDT)
- [4] GB/T 15733—1995 金融电子化基本术语
- [5] GB/T 15948.1—2007 转账报文 第1部分:电子资金转账报文数据段和数据元术语及通用集 (ISO 7982-1:1998, IDT)
- [6] GB/T 16649.8-2002 识别卡 带触点的集成电路卡 第8部分:与安全相关的行业间命令 (ISO/IEC 7816-8:1999, IDT)
- [7] GB/T 16785—1997 术语工作 概念与术语的协调 (ISO 860:1996, EQV)
- [8] GB/T 16790.1—1997 金融交易卡 使用集成电路卡的金融交易系统的安全结构 第1部分:卡的生命周期 (ISO 10202-1:1991, IDT)
- [9] GB/T 16790.5—2006 金融交易卡 使用集成电路卡的金融交易系统的安全体系 第5部分:算法应用 (ISO 10202-5:1998, IDT)
- [10] GB/T 16790.6—2006 金融交易卡 使用集成电路卡的金融交易系统的安全体系 第6部分:持卡人身份验证 (ISO 10202-6:1994, IDT)
- [11] GB/T 16790.7—2006 金融交易卡 使用集成电路卡的金融交易系统的安全体系 第7部分:密钥管理 (ISO 10202-7:1998, IDT)
- [12] GB/T 16791.1—1997 金融交易卡 集成电路卡与卡接受设备之间的报文 第1部分:概念与结构 (ISO 9992-1:1990, IDT)
- [13] GB/T 17552—2008 识别卡 金融交易卡 (ISO/IEC 7813:2006, IDT)
- [14] GB/T 17554.1—2006 识别卡 测试方法 第1部分:一般特性测试 (ISO/IEC 10373-1:1998, MOD)
- [15] GB/T 17554.3—2006 识别卡 测试方法 第3部分:带触点的集成电路卡及其相关接口设备 (ISO/IEC 10373-3:2001, MOD)
- [16] GB 18240.1—2003 税控收款机 第1部分:机器规范
- [17] GB 18240.4—2004 税控收款机 第4部分:银行卡受理设备规范
- [18] GB 18240.6—2004 税控收款机 第6部分:设备编码规则
- [19] GB/T 18460.2—2001 IC卡预付售电系统 第2部分:IC卡及其管理
- [20] GB/T 19558—2004 集成电路 (IC) 卡公用付费电话系统总技术要求
- [21] GB/T 20001.1—2001 标准编写规则 第1部分:术语 (ISO 10241:1992, NEQ)
- [22] GB/T 20276—2006 信息安全技术 智能卡嵌入式软件安全技术要求 (EAL4增强级)
- [23] GB/T 20544—2006 银行业务 报文加密程序 (批发) 一般原则 (ISO 10126-1:1991, MOD)
- [24] GB/T 20547.2—2006 银行业务 安全加密设备 (零售) 第2部分:金融交易中设备安全符合性检测清单 (ISO 13491-2:2005, MOD)
- [25] GB/T 21077.2—2007 银行业务 证书管理 第2部分:证书扩展项 (ISO 15782-2:2001, MOD)
- [26] GB/T 21078.1—2007 银行业务 个人识别码的管理与安全 第1部分:ATM和POS系统中联机PIN处理的基本原则和要求 (ISO 9564-1:2002, MOD)
- [27] GB/T 21079.1—2007 银行业务 安全加密设备 (零售) 第1部分:概念、要求和评估方法 (ISO 13491-1:1998, MOD)

- [28] GB/T 21080—2007 银行业务和相关金融服务 基于对称算法的签名鉴别(ISO 11131:1992, IDT)
- [29] GB/T 21081—2007 银行业务 密钥管理相关数据元(零售)(ISO 13492:1998, IDT)
- [30] GB/T 21082.4—2007 银行业务 密钥管理(零售) 第4部分:使用公开密钥密码的密钥管理技术(ISO 11568-4:1998, MOD)
- [31] GB/T 21082.5—2007 银行业务 密钥管理(零售) 第5部分:公开密钥密码系统的密钥生命周期(ISO 11568-5:1998, IDT)
- [32] GA 745—2008 银行自助设备 自助银行安全防范的规定
- [33] JR/T 0001—2009 银行卡销售点(POS)终端规范
- [34] JR/T 0002—2009 银行卡自动柜员机(ATM)终端规范
- [35] JR/T 0003—2003 银行卡联网联合安全规范
- [36] JR/T 0025.1—2010 中国金融集成电路(IC)卡规范 第1部分:电子钱包/电子存折应用卡片规范
- [37] JR/T 0025.2—2010 中国金融集成电路(IC)卡规范 第2部分:电子钱包/电子存折应用规范
- [38] JR/T 0025.3—2010 中国金融集成电路(IC)卡规范 第3部分:与应用无关的IC卡与终端接口规范
- [39] JR/T 0025.4—2010 中国金融集成电路(IC)卡规范 第4部分:借记/贷记应用规范
- [40] JR/T 0025.5—2010 中国金融集成电路(IC)卡规范 第5部分:借记/贷记应用卡片规范
- [41] JR/T 0025.6—2010 中国金融集成电路(IC)卡规范 第6部分:借记/贷记应用终端规范
- [42] JR/T 0025.7—2010 中国金融集成电路(IC)卡规范 第7部分:借记/贷记应用安全规范
- [43] JR/T 0025.8—2010 中国金融集成电路(IC)卡规范 第8部分:与应用无关的非接触式规范
- [44] JR/T 0025.9—2010 中国金融集成电路(IC)卡规范 第9部分:电子钱包扩展应用指南
- [45] JR/T 0025.10—2010 中国金融集成电路(IC)卡规范 第10部分:借记/贷记应用个人化指南
- [46] JR/T 0025.11—2010 中国金融集成电路(IC)卡规范 第11部分:非接触式IC卡通讯规范
- [47] JR/T 0025.12—2010 中国金融集成电路(IC)卡规范 第12部分:非接触式IC卡支付规范
- [48] JR/T 0025.13—2010 中国金融集成电路(IC)卡规范 第13部分:基于借记/贷记应用的小额支付规范
- [49] JR/T 0045.1—2008 中国金融集成电路(IC)卡检测规范 第1部分:借记/贷记应用卡片检测规范
- [50] JR/T 0045.2—2008 中国金融集成电路(IC)卡检测规范 第2部分:借记/贷记应用终端检测规范
- [51] JR/T 0052—2009 银行卡卡片规范
- [52] JR/T 0055.1—2009 银行卡联网联合技术规范 第1部分:交易处理
- [53] JR/T 0055.2—2009 银行卡联网联合技术规范 第2部分:报文交换
- [54] JR/T 0055.3—2009 银行卡联网联合技术规范 第3部分:文件数据格式
- [55] JR/T 0055.4—2009 银行卡联网联合技术规范 第4部分:数据安全传输控制
- [56] JR/T 0055.5—2009 银行卡联网联合技术规范 第5部分:通信接口
- [57] ISO 8583-1:2003 产生报文的金融交易卡 交换报文规范 第1部分:报文、数据元和代码值
- [58] ISO 8583-2:1998 产生报文的金融交易卡 交换报文规范 第2部分:机构标识代码(IIC)的申请及注册规程

- [59] ISO 9992-2:1998 金融交易卡 集成电路卡与卡接受设备之间的报文 第2部分：功能、报文（命令和响应）、数据元和结构
- [60] ISO/TR 9564—4:2004 银行业务 个人识别码的管理与安全 第4部分：开放网络中PIN处理指南
- [61] ISO 11568-1:1994 银行业务 密钥管理（零售） 第1部分：密钥管理介绍
- [62] ISO 11568-2:2005 银行业务 密钥管理（零售） 第2部分：对称密码及其密钥管理和生命周期
- [63] ISO 11568-3:1994 银行业务 密钥管理（零售） 第3部分：对称密码的密钥生命周期
- [64] 关于银行外币卡管理有关问题的通知 国家外汇管理局，2003年5月12日
- [65] 刑法1997 全国人民代表大会，1997年
- [66] 银行卡业务管理办法 中国人民银行办公厅，2003年
- [67] 全国银行IC卡密钥管理规则（暂行） 中国人民银行办公厅，2000年6月23日
- [68] 银行卡联网联合业务规范 中国人民银行，2001年
- [69] 中央预算单位公务卡管理暂行办法 财政部网站，2007年7月12日
- [70] 程启芬，房军. 银行卡你认识吗 [M]. 北京：群众出版社，2009：13-19
- [71] 戴相龙，黄达主编. 中华金融辞库 [M]. 北京：中国金融出版社，1998:390-392
- [72] 阮莉萍，徐雷. 银行卡业务处理. 高等教育出版社，2007年1月1日
- [73] 王爱英. 智能卡技术——IC卡（第二版）[M]. 北京：清华大学出版社，2003年5月
- [74] PIN输入设备安全评估指南，中国银联，2005年11月17日
- [75] 中国银联代理业务ATM终端技术规范 中国银联，2006年
- [76] 中国银联电话支付终端规范 中国银联
- [77] 中国银联公共支付终端技术规范 中国银联
- [78] 中国银联借记/贷记应用IC卡检测规范 中国银联，2008年
- [79] 银行卡信息交换术语 中国银联，2004年
- [80] 银联卡业务运作规章 中国银联
- [81] 银联卡磁条卡物理性能检测标准 中国银联，2008年
- [82] MasterCard术语 MasterCard，2008年9月
- [83] Visa国际业务运作规则 Visa
-