

金融标准化系列丛书-1

银行卡

名词术语及标准规范

© 主编 李东荣

BANK CARD
TERMINOLOGY AND STANDARDS



 中国金融出版社

金融标准化系列丛书-1

银行卡

名词术语及标准规范

常州大学图书馆藏
李东策主编

BANK CARD

TERMINOLOGY AND STANDARDS

责任编辑：吕楠

责任校对：孙蕊

责任印制：毛春明

图书在版编目 (CIP) 数据

银行卡名词术语及标准规范 (Yinhangka Mingci Shuyu ji Biaozhun Guifan) / 李东荣主编. —北京: 中国金融出版社, 2011. 1

(金融标准化系列丛书-1)

ISBN 978-7-5049-5715-3

I. ①银… II. ①李… III. ①信用卡—名词术语—规范
IV. ①F830.46-61

中国版本图书馆 CIP 数据核字 (2010) 第 208499 号

出版

发行

中国金融出版社

社址 北京市丰台区益泽路 2 号

市场开发部 (010)63266347, 63805472, 63439533 (传真)

网上书店 <http://www.chinafph.com>

(010)63286832, 63365686 (传真)

读者服务部 (010)66070833, 62568380

邮编 100071

经销 新华书店

印刷 保利达印务有限公司

尺寸 169 毫米×239 毫米

印张 22.25

字数 347 千

版次 2011 年 1 月第 1 版

印次 2011 年 1 月第 1 次印刷

定价 49.00 元

ISBN 978-7-5049-5715-3/F.5275

如出现印装错误本社负责调换 联系电话 (010)63263947

序 言

标准化是为在一定范围内获得最佳秩序，对现实问题或潜在问题制定共同使用和重复使用的条款的活动。在现代经济发展过程中，标准化成为一国提升企业核心竞争力，争取发展话语权的重要途径。世界主要发达国家已逐渐将标准化提高到了国家发展战略的高度，成立专门从事标准化工作的组织，开展标准化工作，将发展中的成功经验，通过标准的形式固化下来。

党中央、国务院历来高度重视标准化工作，并将标准化提高到了国家发展战略的高度，多次就标准化工作作出重要指示。金融作为现代服务业的重要组成部分、现代经济的血液，已成为衡量某个国家或地区综合竞争力和现代化水平的重要标志，对于标准化的要求显得更为迫切、更为重要。改革开放以来，我国金融标准化经过近二十年的发展，已逐步成为保证金融业规范化经营，提高整体核心竞争力的重要基础性条件。作为国家的中央银行，中国人民银行承担着制定和执行货币政策、维护金融稳定、提供金融服务的重要职责。随着金融改革的逐步深入，金融经济市场化程度的不断加深，金融标准化的地位和作用日益提高。在各相关单位的大力支持、积极参与下，人民银行和全国金融标准化技术委员会以立足现状、适度前瞻、突出重点、务实可行原则，在金融领域内稳步推进标准化工作，陆续制定和发布了多项涉及银行、保险、证券、银行卡、征信业务等内容的国家标准和行业标准。同时，根据信息系统建设、标准先行的指导原则，研制推出了一系列标准规范。

为使广大业内工作者和社会各界多渠道、多层次地了解中国金融标准化成果、标准化政策法规、国际标准化发展趋势等方面的内容，中国人民

银行决定出版金融标准化系列丛书。经过精心的准备和各方面的共同努力，这套丛书现在可以陆续和大家见面，丛书的出版必将有力地推动我国金融标准化的发展，为大家提供有益的参考。希望可以借此推动社会各界更好地了解金融标准化，并希望金融标准化在全社会的关心支持下，在全行业人员的共同努力下，得以更好、更快地发展，为金融业持续、健康、创新发展奠定基础。

李東榮

中国人民银行行长助理
全国金融标准化技术委员会主任委员
二〇一〇年九月

前 言

标准化是国民经济和社会发展的重要基础性技术工作，金融标准化作为同世界接轨的重要手段，对于全面提高金融行业服务质量、规范市场秩序、提高产业和产品竞争力、促进业务创新、提高金融技术水平具有重要意义。全国金融标准化技术委员会成立的近二十年间，在金融标准制修订、金融标准应用、金融标准国际采标以及标准化服务领域取得了丰硕的成果，共发布金融国家标准 41 项，金融行业标准 80 项。

为适应银行卡产业的迅猛发展，银行卡标准的制定工作也不断加快，工作力度不断加大。特别是 2007 年以来，人民银行结合银行卡产业的发展和应用情况启动了一系列银行卡标准的制定、修订工作并取得了较大进展。截至目前，中国人民银行已发布银行卡国家标准 18 项、行业标准 26 项。这些标准的制定与发布有力地推动了银行卡产业的健康发展，为我国银行卡受理网络的互联互通奠定了坚实的基础。

人民银行于 2009 年开始启动《银行卡名词术语》的制定工作，力图通过该项工作，建立银行卡标准用语的术语集，解决因缺乏术语标准引起的歧义和误解问题，推进银行卡名词术语的规范化。同时，为普及银行卡相关标准，我们将几项最新的银行卡标准一起收录在本书中，供广大读者参阅。

希望本书能在方便业界理解银行卡名词术语，方便银行卡产业的各参与方在业务和产品方面的创新，向社会大众普及银行卡知识等方面起到积极作用。同时，本书也存在诸多不足，需要在今后的使用过程中不断改进和完善，我们也将及时地对其进行修订。我们恳切希望金融行业，以及参阅本书的广大读者能够提出宝贵的意见。

2010 年 10 月

目 录

银行卡名词术语	1
银行卡名词术语中文索引	50
银行卡名词术语英文索引	72
参考文献	94
银行卡销售点 (POS) 终端规范 JR/T 0001—2009	98
银行卡自动柜员机 (ATM) 终端规范 JR/T 0002—2009	161
银行卡卡片规范 JR/T 0052—2009	191
银行卡联网联合技术规范 第 1 部分: 交易处理 JR/T 0055.1—2009	200
银行卡联网联合技术规范 第 2 部分: 报文交换 JR/T 0055.2—2009	218
银行卡联网联合技术规范 第 3 部分: 文件数据格式 JR/T 0055.3—2009	313
银行卡联网联合技术规范 第 4 部分: 数据安全传输控制 JR/T 0055.4—2009	324
银行卡联网联合技术规范 第 5 部分: 通信接口 JR/T 0055.5—2009	337

1 卡片术语

1.1 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。

1.2 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。

1.3 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。

1.4 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和准贷记卡两类。

1.5 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。

1.6 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。

1.7 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。

1.8 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。

1.9 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。

1.10 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。

1.11 错误制卡 **misembossed card**

压卡时包含错误信息的有效卡片。

1.12 编码错卡 **misencoded card**

在编码时包含错误信息的有效卡片。

1.13 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。

1.14 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。

1.15 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。

1.16 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。

1.17 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。

1.18 磁条 **magnetic stripe**

包括磁编码信息的条状物。

1.19 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。

1.20 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。

1.21 一磁 **track 1**

银行卡的第一条磁道，为只读属性，其定义见 GB/T 19584。

1.22 二磁 **track 2**

银行卡的第二条磁道，为只读属性，其定义见 GB/T 19584。

1.23 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。

1.24 三磁 track 3

银行卡的第三条磁道，为读写属性，其定义见 GB/T 19584。

1.25 集成电路 (IC) integrated circuit (IC)

具有处理和/或存储功能的电子器件。

1.26 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。

1.27 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。

1.28 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。

1.29 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。

1.30 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。

1.31 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。

1.32 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。

1.33 TIM 卡 TIM card

用户初始化终端参数的接触式 IC 卡。

1.34 TKEY 卡 TKEY card

用于下载终端认证密钥的接触式 IC 卡。

1.35 TSAM 卡 TSAM card

用于终端安全控制的接触式 IC 卡。

1.36 无触点的 contactless

无须使用通电元件完成与卡交换信号和给卡供应能量（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)。

1.37 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。

1.38 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。

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

一种 ID-1 型卡,其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的。

1.40 发卡行标识域 **issuer identification area**

在卡面上不同于银行卡组织标识的地方,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。

1.41 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,应遵照 JR/T 0008 的规定。

1.42 卡段 **card range**

卡号的一段范围。

1.43 签名条 **signature panel**

卡上用于签名的特定区域。

1.44 凸印 **embossing**

一种使字符从卡的正面显著地凸起的印刷方式。

1.45 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。

1.46 (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。

1.47 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。

1.48 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。

1.49 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。

1.50 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。

1.51 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。

1.52 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。

1.53 磁通翻转 flux transition

垂直于磁条表面最大磁通分量的位置。

1.54 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。

1.55 平均信号幅度 average signal amplitude

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

1.56 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）。

1.57 剥离强度 peel strength

在构造方面，卡抵御相邻层材料分离的能力。

1.58 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。

1.59 黏连或并块 adhesion or blocking

将新卡堆积时的黏接性。

1.60 翘曲 warpage

相对平面的偏离。

1.61 弯曲韧性 bending stiffness

卡抗弯曲的能力。

1.62 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。

1.63 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。

1.64 可燃性 flammability

一旦点燃，卡维持和扩散火焰的能力。

1.65 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。

2 机构及人员术语

2.1 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。

2.2 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。

2.3 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。

2.4 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。

2.5 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。

2.6 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。

2.7 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。

2.8 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。

2.9 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。

2.10 发起方 initiator

开始某一过程的节点或实体。

2.11 响应方 respondent

对一过程的发起者作出响应的节点或实体。

2.12 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。

2.13 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。

2.14 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。

2.15 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。

2.16 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。

2.17 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）。

2.18 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。与收单行签有合同的，为商户提供支付服务的在线实体。

2.19 应用提供商 application provider

将各种所需组件装载至卡片以提供完整应用的实体。应用提供商与持卡人具有直接的商业关系并向持卡人提供各种基于卡片的服务。

2.20 封装机构 embedder

进行 IC 封装工作的实体。

2.21 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。

2.22 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。

2.23 持卡人 cardholder

卡的合法持有者。

2.24 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。

2.25 持卡者标识 cardholder identification

标识持卡者的代码。

2.26 合法用户 authorized customer

可以合法进行交易的持卡人。

2.27 授权者 grantor

具有授予访问权利的实体。

2.28 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。

3 终端及设备术语

3.1 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。

3.2 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(如与主机的通信)。

3.3 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。

3.4 读磁条终端 magnetic stripe terminal

能够读取卡片磁条信息的终端。

3.5 IC 卡终端 integrated circuit card terminal

能够处理集成电路卡的读取、通信及进行交易的交易点终端。

3.6 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信的终端。

3.7 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。

3.8 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。

3.9 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。

3.10 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。

3.11 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。

3.12 银行自助设备 **bank self – service equipment**

由银行提供，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。

3.13 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。

3.14 在行式 **in – bank mode**

自助设备设置在银行营业场所的应用模式。

3.15 穿墙式 **through – the – 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。

3.16 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。

3.17 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。

3.18 收银终端 **cash register terminal**

在商户内部网络内，接收银行卡信息，具有通信功能，接收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。

3.19 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。

3.20 销售点终端 **point – of – sale terminal**

能够接收银行卡信息，具有通信功能，并接收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。

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

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。

3.22 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。

3.23 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。

3.24 出钞模块 (CDM) cash dispense 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。

3.25 存款模块 deposit module

用于实现合法用户存入现金的部件单元。

3.26 终端控制模块 (TCM) terminal control module (TCM)

终端的主控处理机。

3.27 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。

3.28 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。

3.29 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。

3.30 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。

3.31 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。

3.32 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。

3.33 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。

3.34 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。

3.35 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。

3.36 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。