

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(43) 国际公布日
2014年9月18日 (18.09.2014)

WIPO | PCT



(10) 国际公布号

WO 2014/139406 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2014/073215

(22) 国际申请日: 2014年3月11日 (11.03.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310084397.2 2013年3月15日 (15.03.2013) CN
201310084671.6 2013年3月15日 (15.03.2013) CN
201310084673.5 2013年3月15日 (15.03.2013) CN
201310084653.8 2013年3月15日 (15.03.2013) CN
201310740642.0 2013年12月27日 (27.12.2013) CN

(71) 申请人: 福建联迪商用设备有限公司 (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD) [CN/CN]; 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼, Fujian 350000 (CN)。

(72) 发明人: 苏文龙 (SU, Wenlong); 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼,

Fujian 350000 (CN)。 孟陆强 (MENG, Luqiang); 中国福建省福州市鼓楼区软件大道 89 号福州软件园一区 23 号楼, Fujian 350000 (CN)。

(74) 代理人: 福州市鼓楼区博深专利代理事务所 (普通合伙) (BORSAM INTELLECTUAL PROPERTY(FUZHOU)); 中国福建省福州市鼓楼区湖滨路 66 号中福西湖花园 3#楼 3A 单元, Fujian 350003 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA,

[见续页]

(54) Title: METHOD AND SYSTEM FOR SAFELY DOWNLOADING TERMINAL MASTER KEY (TMR)

(54) 发明名称: 一种终端主密钥 TMK 安全下载方法及系统

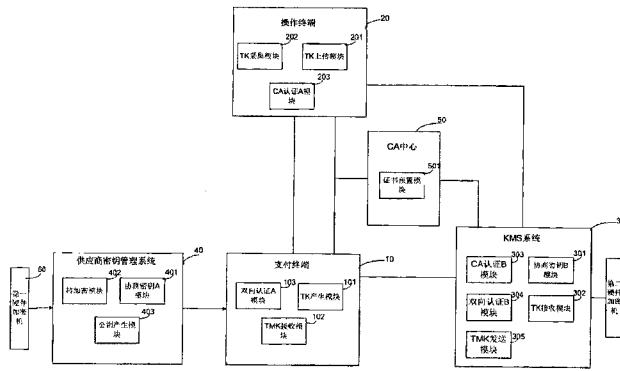


图 1 / FIG. 1

10 PAYMENT TERMINAL
20 OPERATING TERMINAL
30 KMS SYSTEM
40 SUPPLIER KEY MANAGEMENT SYSTEM
50 CA CENTER
60 FIRST HARDWARE AND SECURITY MODULE
70 SECOND HARDWARE AND SECURITY MODULE
101 TK GENERATING MODULE
102 TMK RECEIVING MODULE
103 BIDIRECTIONAL AUTHENTICATION A MODULE
201 TK UPLOADING MODULE
202 TK COLLECTING MODULE
203 CA AUTHENTICATION A MODULE
301 NEGOTIATION KEY B MODULE
302 TK RECEIVING MODULE
303 CA AUTHENTICATION B MODULE
304 BIDIRECTIONAL AUTHENTICATION B MODULE
305 TMK SENDING MODULE
401 NEGOTIATION KEY A MODULE
402 TRANSCRIPTION MODULE
403 PUBLIC KEY GENERATING MODULE
501 CREDENTIAL PRESETTING MODULE

(57) Abstract: Disclosed is a method for safely downloading a terminal master key (TMK), comprising steps of a payment terminal generating a transmission key (TK); a supplier key management system performing transcription on the TK and then sending the TK to the payment terminal; an operating terminal collecting the transcribed TK and transferring the TK to a KMS system; the KMS system performing identity authentication with a payment system; and after the authentication succeeds, the KMS system sending the TMK to the payment terminal by using the operating terminal. The beneficial effects of the present invention are as follows: According to the present invention, both TK uploading and TMK downloading are performed by using the operating terminal, and the TMK downloading is directly subsequent to the step of the TK uploading, and the TMK downloading time efficiency is greatly improved.

(57) 摘要: 本发明公开一种终端主密钥 TMK 安全下载方法, 包括步骤: 支付终端产生传输密钥 TK; 供应商密钥管理系统对 TK 进行转加密后发送给支付终端; 操作终端采集转加密后的 TK, 并将其传送给 KMS 系统; KMS 系统与支付系统进行身份认证; 认证通过后 KMS 系统通过操作终端将终端主密钥 TMK 发送给支付终端。本发明的有益效果为: 本发明 TK 上传和 TMK 下载都通过操作终端进行, 并且 TMK 下载是直接接续 TK 上传步骤之后, 大大提高了 TMK 下载时间效率。

本国际公布:

RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,
BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD,
TG)。

— 包括国际检索报告(条约第 21 条(3))。

— 包括经修改的权利要求(条约第 19 条(1))。

一种终端主密钥**TMK**安全下载方法及系统

[1] 技术领域

[2] 本发明涉及电子支付领域，尤其涉及一种终端主密钥**TMK**安全下载方法及系统。
。

[3] 背景技术

[4] 银行卡（BANK Card）作为支付工具越来越普及，通常的银行卡支付系统包括销售点终端（Point Of Sale, POS）、POS收单系统（POSP）、密码键盘（PIN PAD）和硬件加密机（Hardware and Security Module, HSM）。其中POS终端能够接受银行卡信息，具有通讯功能，并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；POS收单系统对POS终端进行集中管理，包括参数下载，密钥下载，接受、处理或转发POS终端的交易请求，并向POS终端回送交易结果信息，是集中管理和交易处理的系统；密码键盘（PIN PAD）是对各种金融交易相关的密钥进行安全存储保护，以及对PIN进行加密保护的安全设备；硬件加密机（HSM）是对传输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。个人标识码（Personal Identification Number, PIN），即个人密码，是在联机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以明文的方式出现；终端主密钥（Terminal Master Key, TMK），POS终端工作时，对工作密钥进行加密的主密钥，加密保存在系统数据库中；POS终端广泛应用于银行卡支付场合，比如厂商购物、酒店住宿等，是一种不可或缺的现代化支付手段，已经融入人们生活的各种场合。银行卡，特别是借记卡，一般都由持卡人设置了PIN，在进行支付过程中，POS终端除了上送银行卡的磁道信息等资料外，还要持卡人输入PIN供发卡银行验证持卡人的身份合法性，确保银行卡支付安全，保护持卡人的财产安全。为了防止PIN泄露或被破解，要求从终端到发卡银行整个信息交互过程中，全程对PIN进行安全加密保护，不允许在计算机网络系统的任何环节，PIN以明文的方式出现，因此目前接受输入PIN的POS终端都要求配备密钥管理体系。

[5] POS终端的密钥体系分成二级：终端主密钥（TMK）和工作密钥（WK）。其中TMK对WK进行加密保护。每台POS终端拥有唯一的TMK，必须要有安全保护，保证只能写入设备并参与计算，不能读取；TMK是一个很关键的根密钥，如果TMK被截取，工作密钥就比较容易被破解，将严重威胁银行卡支付安全。所以能否安全下载TMK到POS终端，成为整个POS终端安全性的关键。

[6] 为了保证终端主密钥TMK安全的下载到POS终端中，终端主密钥TMK的下载必须控制在收单机构的管理中心的安全机房进行，因此必需要通过人工集中POS终端，并下载终端主密钥TMK。从而带来维护中心机房工作量大；设备出厂后需要运输到管理中心安全机房下载密钥才能部署到商户，运输成本上升；为了集中下装密钥，需要大量的人手和工作时间，维护成本大、维护周期长等问题。

[7] **发明内容**

[8] 为解决上述技术问题，本发明采用的一个技术方案是：一种终端主密钥TMK安全下载方法，包括步骤：S1、支付终端产生传输密钥TK以及生成传输密钥密文；S2、支付终端上传传输密钥密文以及下载主密钥TMK；其中步骤S1包括：S11、供应商密钥管理系统调用第一硬件加密机、KMS系统调用第二硬件加密机，分别在第一硬件加密机和第二硬件加密机中将供应商权限分量及KMS系统权限分量合成保护密钥PK和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并分别存储在第一硬件加密机和第二硬件加密机中；S12、供应商密钥管理系统调用第一硬件加密机产生公私钥对Pu_hsm、Pr_hsm，并将公钥Pu_hsm发送给支付终端；S13、支付终端调用密码键盘生成传输密钥TK，所述TK包括传输加密密钥TEK和传输认证密钥AUK；S14、支付终端调用密码键盘使用公钥Pu_hsm加密TK，生成第一传输密钥密文Ctk_Pu，并将第一传输密钥密文Ctk_Pu发送给供应商密钥管理系统；S15、供应商密钥管理系统调用第一硬件加密机使用私钥Pr_hsm解密第一传输密钥密文Ctk_Pu获得传输密钥TK；S16、供应商密钥管理系统调用第一硬件加密机使用保护密钥PK 加密传输密钥TK 并使用MAC密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，并将第二传输密钥密文Ctk_pk发送给支付终端；其中步骤S2包括：S21、操作终端采集支付终端的第

二传输密钥密文Ctk_pk； S22、操作终端与KMS系统之间通过CA中心进行身份认证，认证通过后，将第二传输密钥密文Ctk_pk发送给KMS系统； S23、KMS系统调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk校验MAC合法性，如果校验通过，使用保护密钥PK

解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中； S24、KMS

系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK 与支付终端进行双向认证； S25、如果认证通过， KMS系统调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至支付终端； S26、支付终端调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[9] 本发明提供的另一技术方案是：

[10] 一种终端主密钥TMK安全下载系统，包括第一硬件加密机、第二硬件加密机、供应商密钥管理系统、支付终端、CA中心、操作终端以及KMS系统；所述供应商密钥管理系统包括协商密钥A模块、公钥产生模块、转加密模块，支付终端包括TK产生模块、双向认证A模块、TMK接收模块，操作终端包括TK采集模块、TK上传模块、CA认证A模块，KMS系统包括协商密钥B模块、TK接收模块、CA认证B模块、双向认证B模块、TMK发送模块； 协商密钥A模块与协商密钥B模块用于调用第一硬件加密机和第二硬件加密机，分别在第一硬件加密机和第二硬件加密机中将供应商权限分量及KMS 系统权限分量合成保护密钥PK和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并分别存储在第一硬件加密机和第二硬件加密机中； 公钥产生模块用于调用第一硬件加密机产生公私钥对Pu_hsm、Pr_hsm，并将公钥Pu_hsm发送给支付终端； TK产生模块用于调用密码键盘生成传输密钥TK，所述TK包括传输加密密钥TEK和传认证密钥AUK； TK产生模块还用于调用密码键盘使用公钥Pu_hsm加密TK，生成第一传输密钥密文Ctk_Pu，并将第一传输密钥密文Ctk_Pu发送给供应商密钥管理系统； 转加密模块用于调用第一硬件加密机使用私钥Pr_hsm解密第一传输密钥密文Ctk_Pu获得传输密钥TK； 转加密模块还用于调用第一硬件加密机使用保护密钥PK 加密

传输密钥TK 并使用MAC 密钥MAK 计算MAC

值，生成第二传输密钥密文Ctk_pk，并将第二传输密钥密文Ctk_pk发送给支付终端；TK采集模块用于采集支付终端的第二传输密钥密文Ctk_pk；CA认证A模块与CA认证B模块用于操作终端与KMS系统之间通过CA中心进行身份认证；TK上传模块用于当认证通过后，将第二传输密钥密文Ctk_pk发送给KMS系统；TK接收模块用于调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，还用于当校验通过时，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；双向认证A模块与双向认证B模块用于当KMS 系统获得传输密钥TK后，调用第二硬件加密机使用认证密钥AUK

与支付终端进行双向认证；TMK发送模块用于当KMS系统与支付终端认证通过后，调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至支付终端；TMK接收模块用于调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[11] 本发明的有益效果为：本发明通过支付终端上传传输密钥TK，由传输密钥对TMK进行加密传输，实现支付终端远程下载终端主密钥TMK，其中，TK包括传输加密密钥TEK和传输认证密钥AUK，支付终端与KMS系统先经过认证密钥AUK进行双向身份认证，认证通过后用非对称传输加密密钥TEK加密终端主密钥TMK进行传输，提高了TMK的传输下载安全。进一步地，所述主密钥TMK下载和传输密钥TK上传是一并进行的，且都是通过操作终端进行的，因此大大提高了TMK下载的时间效率。同时在支付终端出厂投放给商户之前就可以统一通过操作终端进行主密钥TMK下载，由于操作终端与KMS系统之间通过CA中心进行过身份认证，且TMK是集中进行下载的，因此大大减小了主密钥TMK下载风险，并且商户拿到支付终端就可直接使用，大大方便了商户的使用。更进一步地，所述供应商密钥管理系统与KMS系统分别存储有保护密钥PK和MAC密钥MAK，支付终端产生的传输密钥TK由供应商密钥管理系统的保护密钥PK和MAC密钥MAK加密后进行上传，因此操作终端无需对TK进行进一步地转加密，大大简

化了TK上传过程中的加密处理，在保证TK安全传输的前提下提高了TK上传的时间效率。

- [12] 附图说明
- [13] 图1为本发明一实施方式中一种终端主密钥TMK安全下载系统的结构框图；
- [14] 图2为图1中双向认证A模块的结构框图；
- [15] 图3为图1中双向认证B模块的结构框图；
- [16] 图4为本发明一实施方式一种终端主密钥TMK安全下载方法的方法流程图；
- [17] 图5为图4中的步骤S1的具体步骤流程图；
- [18] 图6为图4中的步骤S2的具体步骤流程图。
- [19] 主要元件符号说明：
 - [20] 10：支付终端； 20：操作终端； 30：KMS系统； 40：供应商密钥管理系统；
50：CA中心； 60：第一硬件加密机； 70：第二硬件加密机； 101：TK产生模块；
102：TMK接收模块； 103：双向认证A模块； 201：TK上传模块；
202：TK采集模块； 203：CA认证A模块； 301：协商密钥B模块； 302：TK接收模块；
303：CA认证B模块； 304：双向认证B模块； 305：TMK发送模块；
401：协商密钥A模块； 402：转加密模块； 403：公钥产生模块； 501：证书预置模块；
- [21] 具体实施方式
- [22] 为详细说明本发明的技术内容、构造特征、所实现目的及效果，以下结合实施方式并配合附图详予说明。
- [23] 首先，对本发明涉及的缩略语和关键术语进行定义和说明：
- [24] HSM_VENDOR：供应商硬件加密机；
- [25] AUK：Authentication Key
的简称，即认证密钥，用于PINPAD与密钥管理系统KMS之间的双向认证；
- [26] CA中心：所谓CA（Certificate Authority）中心，它是采用PKI（Public Key Infrastructure）公开密钥基础架构技术，专门提供网络身份认证服务，负责签发和管理数字证书，且具有权威性和公正性的第三方信任机构，它的作用就像我们现实生活中颁发证件的公司，如护照办理机构；

- [27] HSM: High Security Machine的简称，高安全设备，在该系统中为硬件加密机；
- [28] KMS系统: Key Management System, 密钥管理系统，用于管理终端主密钥TMK;
- [29] MAK: Mac Key的简称，即MAC计算密钥，与客户协商确定24字节对称密钥，用于MTMS系统与KMS系统之间TK的MAC值计算；
- [30] MTMS: 全称Material Tracking Management System, 物料追溯管理系统，主要在工厂生产时使用；
- [31] PIK: Pin Key的简称，即Pin加密密钥，是工作密钥的一种；
- [32] PINPAD: 密码键盘；
- [33] PK: Protect Key 的简称，即保护密钥，与客户协商确定，24字节对称密钥。用于MTMS/TCS 与KMS之间TK的加密传输；
- [34] POS: Point Of Sale 的简称，即销售终端
- [35] SNpinpad: 密码键盘的序列号，PINPAD是内置时，和POS终端序列号SNpos一致；
- [36] SN: POS终端的序列号；
- [37] TEK: Transmission Encrypt Key的简称，即传输加密密钥，24字节对称密钥，用于PINPAD与密钥管理系统KMS之间TMK的加密传输；
- [38] TK: Transmission Key的简称，即传输密钥。传输密钥是由传输加密密钥TEK和双向认证密钥AUK组成的；
- [39] TMS: Terminal Management System 的简称，即终端管理系统，用于完成POS终端信息管理、软件与参数配置、远程下载、终端运行状态信息收集管理、远程诊断等功能；
- [40] TMK: Terminal Master Key的简称，即终端主密钥，用于POS终端和支付收单系统之间工作密钥的加密传输；
- [41] 安全房：具有较高安全级别，用于存放服务器的房间，该房间需要身份认证后才能进去。
- [42] 智能IC卡：为CPU卡，卡内的集成电路包括中央处理器CPU、可编程只读存储

器EEPROM、随机存储器RAM和固化在只读存储器ROM中的卡内操作系统COS(Chip Operating System)，卡中数据分为外部读取和内部处理部分。

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

[44] 非对称密钥：非对称加密算法需要两个密钥：公开密钥（私钥Public key）和私有密钥（公钥Private key）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。甲方可以使用乙方的公钥对机密信息进行加密后再发送给乙方；乙方再用自己的私匙对加密后的信息进行解密。主要算法有RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）。

[45] RSA：一种非对称密钥算法。RSA公钥加密算法是1977年由Ron Rivest、Adi Shamir 和Len Adleman 在（美国麻省理工学院）开发的。RSA 取名来自开发他们三者的名字。RSA 是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的所有密码攻击，已被 ISO 推荐为公钥数据加密标准。RSA 算法基于一个十分简单的数论事实：将两个大素数相乘十分容易。RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA 是被研究得最广泛的公钥算法，从提出到现在的三十多年里，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

[46] TDES Triple-DES：DES是一种对称加密算法，密钥是8字节。TDES是基于DES的加密算法，其密钥是16 字节或者24 字节。TDES/3DES 是英文TripleDES的缩语（即三重数据加密标准），DES 则是英文Data Encryption Standard（数加密标准）的缩语。DES 是一种对称密钥加密算法，即数据加密密钥与解密密钥相同

的加密算法。DES 由 IBM 公司在 20 世纪 70 年代开发并公开，随后为美国政府采用，并被美国国家标准局和美国国家标准协会 (ANSI) 承认。TDES/3DES 是 DES 加密算法的一种模式，它使用 3 条 64 位的密钥对数据进行三次加密。是 DES 的一个更安全的变形。

- [47] 为解决背景技术中存在的技术问题，本发明采用一种新的主密钥下载方案，通过 POS 终端随机产生 TK (Transmission Key，传输密钥)，将产生后的 TK 保存于 POS 终端的密码键盘中，并将 TK 通过各种应用场景下所需的传输方式传送至 KMS (Key Management System, 密钥管理系统，用于管理终端主密钥 TMK) 中。
- [48] 当 POS 终端申请下载终端主密钥 TMK 时，KMS 系统使用 TK 加密终端主密钥 TMK，并将加密后的终端主密钥密文发送给 POS 终端，POS 终端接收后用 TK 对主密钥密文进行解密，得到终端主密钥 TMK，并将终端主密钥 TMK 保存在密码键盘里。
- [49] 如此，通过 TK 加密终端主密钥 TMK，使 TMK 能够进行远程传输，方便 TMK 的安全下载。
- [50] 上述通过 POS 终端采集传输密钥 TK 后发送至银行端对 TMK 进行加密，再通过 POS 终端远程下载经 TK 加密后的 TMK 的方法可以实现 TMK 的远程下载。但是，上述 TMK 下载方法 TMK 下载与 TK 上传是分开进行的，一般情况下是 POS 终端在生产厂家时产生并上传 TK，等 POS 终端发放到各商户后再进行 TMK 下载，因此 TMK 的下载是零散进行的，时间效率低、KMS 系统的工作量大，并且 POS 终端投放到各商户后再进行 TMK 下载不确定因素较多，TMK 的下载风险更高。因此需要一种时间效率更高、下载更为安全的终端主密钥 TMK 安全下载方法。
- [51] 下面就对本发明克服上述问题的技术方案进行详细说明。
- [52] 请参阅图 1，为本发明一实施方式一种终端主密钥 TMK 安全下载系统的结构框图，该系统包括第一硬件加密机 60、第二硬件加密机 70、供应商密钥管理系统 40、支付终端 10、CA 中心 50、操作终端 20 以及 KMS 系统 30；所述供应商密钥管理系统 40 包括协商密钥 A 模块 401、公钥产生模块 403、转加密模块 402，支付终端 10 包括 TK 产生模块 101、双向认证 A 模块 103、TMK 接收模块 102，操作终端 20

包括TK采集模块202、TK上传模块201、CA认证A模块203，KMS系统30包括协商密钥B模块301、TK接收模块302、CA认证B模块303、双向认证B模块304、TMK发送模块305。

- [53] 协商密钥A模块401与协商密钥B模块301用于调用第一硬件加密机60和第二硬件加密机70，分别在第一硬件加密机60和第二硬件加密机70中将供应商权限分量及KMS系统权限分量合成保护密钥PK和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并分别存储在第一硬件加密机60和第二硬件加密机70中；
- [54] 公钥产生模块403用于调用第一硬件加密机60产生公私钥对Pu_hsm、Pr_hsm，并将公钥Pu_hsm发送给支付终端10；
- [55] TK产生模块101用于调用密码键盘生成传输密钥TK，所述TK包括传输加密密钥TEK和传输认证密钥AUK；
- [56] TK产生模块101还用于调用密码键盘使用公钥Pu_hsm加密TK，生成第一传输密钥密文Ctk_Pu，并将第一传输密钥密文Ctk_Pu发送给供应商密钥管理系统40；
- [57] 转加密模块402用于调用第一硬件加密机60使用私钥Pr_hsm解密第一传输密钥密文Ctk_Pu获得传输密钥TK；
- [58] 转加密模块402还用于调用第一硬件加密机60使用保护密钥PK加密传输密钥TK 并使用MAC密钥MAK计算MAC值，生成第二传输密钥密文Ctk_pk，并将第二传输密钥密文Ctk_pk发送给支付终端10；
- [59] TK采集模块202用于采集支付终端的第二传输密钥密文Ctk_pk；
- [60] CA认证A模块203与CA认证B模块304用于操作终端20与KMS系统30之间通过CA中心50进行身份认证；TK上传模块201用于当认证通过后，将第二传输密钥密文Ctk_pk发送给KMS系统30；
- [61] TK接收模块302用于调用第二硬件加密机70使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk校验MAC合法性，还用于当校验通过时，使用保护密钥PK解密第二传输密钥密文Ctk_pk

- 获得传输密钥TK并将其存储在所述第二硬件加密机70中；
- [62] 双向认证A模块103与双向认证B模块304用于当KMS系统30获得传输密钥TK后，调用第二硬件加密机70使用认证密钥AUK与支付终端进行双向认证；
- [63] TMK发送模块305用于当KMS系统30与支付终端10认证通过后，调用第二硬件加密机70使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至支付终端10；
- [64] TMK接收模块102用于调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。
- [65] 其中，所述CA认证A模块包括第一随机数产生单元、第一数据收发单元、第一加解密单元、第一判断单元，CA认证B模块包括第二随机数产生单元、第二数据收发单元、第二加解密单元、第二判断单元，CA中心包括证书预置模块。
- [66] 证书预置模块用于调用操作终端生成公私钥对Pu_optm和Pr_optm，并将公钥Pu_optm和操作终端标识信息向发给CA中心，CA中心生成根证书AuthRCRT_optm和对应私钥OptmWCRT_Prk，以及用于将接收到的公钥Pu_optm和操作终端标识信息使用私钥OptmWCRT_Prk签名生成数字证书OptmWCRT，以及用于数字证书OptmWCRT以及私钥OptmWCRT_Prk存储在操作终端中，将根证书AuthRCRT_optm存储在KMS系统；
- [67] 证书预置模块用于调用第二硬件加密机产生公私钥对Pr_kms和Pu_kms，并将公钥Pu_kms和KMS标识信息发给CA中心，CA中心生成根证书AuthRCRT_kms和对应私钥ServerWCRT_Prk，以及用于将接收到的公钥Pu_kms和KMS系统标识信息使用私钥ServerWCRT_Prk签名生成数字证书ServerWCRT，以及用于将数字证书ServerWCRT以及对应私钥ServerWCRT_Prk存储在KMS系统，将根证书AuthRCRT_kms存储在操作终端；
- [68] 第二数据收发单元用于将数字证书ServerWCRT发送给操作终端；
- [69] 第一判断单元用于使用根证书AuthRCRT_kms验证数字证书ServerWCRT的合法性；第一随机数产生单元用于当所述数字证书ServerWCRT验证通过后，生成第一随机数AT1，并用于将第一随机数AT1发送给KMS系统；
- [70] 第二加解密单元用于使用私钥ServerWCRT_Prk签名第一随机数AT1生成第一随

- 机数密文Sign1，并将第一随机数密文Sign1发送给操作终端；
- [71] 第一判断单元用于使用数字证书ServerWCRT验证第一随机数密文Sign1的合法性，第一数据收发单元用于当第一随机数密文Sign1验证通过后，将数字证书OptmWCRT发送给KMS系统；
- [72] 第二判断单元用于使用根证书AuthRCRT_optm验证数字证书OptmWCRT的合法性，第二随机数产生单元用于当数字证书OptmWCRT验证通过后，生成第二随机数AT2，并将第二随机数发送给操作终端；
- [73] 第一加解密单元用于使用私钥OptmWCRT_Prk加密第二随机数AT2生成第二随机密文Sign2，并将第二随机密文Sign2发送给KMS系统；
- [74] 第二判断单元用于使用数字证书OptmWCRT验证第二随机密文Sign2的合法性，验证通过后，KMS系统与操作终端认证通过。
- [75] 请参阅图2和图3，其中，图2为所述双向认证A模块103的结构框图，图3为所述双向认证B模块304的结构框图，所述双向认证A模块103包括第三随机数产生单元、第三数据收发单元、第三加解密单元以及第三判断单元，所述双向认证B模块包括第四随机数产生单元、第四数据收发单元、第四加解密单元以及第四判断单元；
- [76] 第三随机数产生单元用于产生第三随机数AT3；第三数据收发单元用于将产生的第三随机数AT3发送至KMS系统；第四数据收发单元用于接收第三随机数AT3；第四随机数产生单元用于在接收到第三随机数AT3时，产生第四随机数AT4；第四加解密单元用于在接收到第三随机数AT3时，调用第四硬件加密机使用传输认证密钥AUK加密第三随机数AT3获得第三随机数密文Sign3；第四数据收发单元用于将第三随机数密文Sign3和第四随机数AT4发送给支付终端；
- [77] 第三加解密单元用于在接收到第三随机数密文Sign3和第四随机数AT4时，使用传输认证密钥AUK解密接收到的第三随机数密文Sign3获得第五随机数AT3'；第三判断单元用于判断第五随机数AT3'与第三随机数AT3是否一致；
- [78] 第三加解密单元用于当第五随机数AT3'与第三随机数AT3一致时，使用传输认证密钥AUK加密第四随机数AT4生成第四随机数密文Sign4；第三数据收发单元用于将第四随机数密文Sign4发送给KMS系统；

- [79] 第四加解密单元用于在接收到第四随机数密文Sign4时，调用第二硬件加密机使用传输认证密钥AUK解密接收到的第四随机数密文Sign4获得第六随机数AT4'，第四判断单元用于判断第六随机数AT4'与第四随机数AT4是否一致，并当判定第六随机数AT4'与第四随机数AT4一致时，确认KMS系统与支付终端之间的双向认证通过。
- [80] 其中，所述操作终端还包括有操作员卡和管理员卡；
- [81] 所述CA中心的证书预置模块还用于产生操作员卡证书和管理员卡证书，并用于将操作员卡证书存储在操作员卡里以及将管理员卡证书存储在管理卡里；
- [82] 所述操作员卡和管理员卡用于当操作终端读取插在操作终端上的操作员卡和管理员卡，通过CA中心对操作员证书和管理员证书进行合法性认证通过时，授权对操作终端进行操作。
- [83] 其中，所述支付终端为POS终端、手机终端、智能IC卡、或ATM机终端。
- [84] 请参阅图4，为本发明一实施方式中一种终端主密钥TMK安全下载方法，该方法包括步骤：
- [85] S1、支付终端产生传输密钥TK以及生成传输密钥密文；
- [86] S2、支付终端上传传输密钥密文以及下载主密钥TMK；
- [87] 请参阅图5，为图4中步骤S1的具体步骤流程图，其中，步骤S1包括：
- [88] S11、供应商密钥管理系统调用第一硬件加密机、KMS系统调用第二硬件加密机，分别在第一硬件加密机和第二硬件加密机中将供应商权限分量及KMS系统权限分量合成保护密钥PK和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并分别存储在第一硬件加密机和第二硬件加密机中；
- [89] S12、供应商密钥管理系统调用第一硬件加密机产生公私钥对Pu_hsm、Pr_hsm，并将公钥Pu_hsm发送给支付终端；
- [90] S13、支付终端调用密码键盘生成传输密钥TK，所述TK包括传输加密密钥TEK和传输认证密钥AUK；
- [91] S14、支付终端调用密码键盘使用公钥Pu_hsm加密TK，生成第一传输密钥密文Ctk_Pu，并将第一传输密钥密文Ctk_Pu发送给供应商密钥管理系统；
- [92] S15、供应商密钥管理系统调用第一硬件加密机使用私钥Pr_hsm解密第一传输

密钥密文Ctk_Pu获得传输密钥TK;

- [93] S16、供应商密钥管理系统调用第一硬件加密机使用保护密钥PK
加密传输密钥TK 并使用MAC 密钥MAK 计算MAC
值，生成第二传输密钥密文Ctk_pk， 并将第二传输密钥密文Ctk_pk发送给支付终
端；
- [94] 请参阅图6，为图4中步骤S2的具体步骤流程图，其中，步骤S2包括：
- [95] S21、操作终端采集支付终端的第二传输密钥密文Ctk_pk；
- [96] S22、操作终端与KMS系统之间通过CA中心进行身份认证，认证通过后，将第
二传输密钥密文Ctk_pk发送给KMS系统；
- [97] S23、KMS系统调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输
密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二
传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；
- [98] S24、KMS 系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK 与
支付终端进行双向认证；
- [99] S25、如果认证通过，KMS系统调用第二硬件加密机使用传输加密密钥TEK加
密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至支付终端；
- [100] S26、支付终端调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得
终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。
- [101] 其中，所述步骤S22具体为：
- [102] 操作终端生成公私钥对Pu_optm和Pr_optm， 将公钥Pu_optm和操作终端标识信
息发给CA中心， CA中心生成根证书AuthRCRT_optm和对应私钥OptmWCRT_Pr
k，并将接收到的公钥Pu_optm和操作终端标识信息使用私钥OptmWCRT_Prk签
名生成数字证书OptmWCRT， 将数字证书OptmWCRT以及私钥OptmWCRT_Prk
存储在操作终端中， 将根证书AuthRCRT_optm存储在KMS系统；
- [103] KMS系统调用第二硬件加密机产生公私钥对Pr_kms和Pu_kms， 将公钥Pu_kms
和KMS系统标识信息发给CA中心， CA中心生成根证书AuthRCRT_kms和对应私
钥ServerWCRT_Prk，并将接收到的公钥Pu_kms和KMS系统标识信息使用私钥Se
rverWCRT_Prk签名生成数字证书ServerWCRT， 将数字证书ServerWCRT以及对

应私钥ServerWCRT_Prk存储在KMS系统，将根证书AuthRCRT_kms存储在操作终端；

- [104] KMS系统将数字证书ServerWCRT发送给操作终端；
- [105] 操作终端使用根证书AuthRCRT_kms验证数字证书ServerWCRT的合法性，如果验证通过，操作终端生成第一随机数AT1，并将第一随机数AT1发送给KMS系统；
- [106] KMS系统使用私钥ServerWCRT_Prk签名第一随机数AT1生成第一随机数密文Sign1，并将第一随机数密文Sign1发送给操作终端；
- [107] 操作终端使用数字证书ServerWCRT验证第一随机数密文Sign1的合法性，验证通过后，将数字证书OptmWCRT发送给KMS系统；
- [108] KMS系统使用根证书AuthRCRT_optm验证数字证书OptmWCRT的合法性，验证通过后，生成第二随机数AT2，并将第二随机数AT2发送给操作终端；
- [109] 操作终端使用私钥OptmWCRT_Prk加密第二随机数AT2生成第二随机密文Sign2，并将第二随机密文Sign2发送给KMS系统；
- [110] KMS系统使用数字证书OptmWCRT验证第二随机密文Sign2的合法性，验证通过后，KMS系统与操作终端认证通过。
- [111] 其中，所述步骤S24具体包括：
- [112] 支付终端产生第三随机数AT3并将第三随机数AT3发送至KMS系统；
- [113] KMS系统接收第三随机数AT3后产生第四随机数AT4，调用第二硬件加密机使用认证密钥AUK加密第三随机数AT3获得第三随机数密文Sign3，将第三随机数密文Sign3和第四随机数AT4发送给支付终端；
- [114] 支付终端使用认证密钥AUK解密接收到的第三随机数密文Sign3获得第五随机数AT3'，判断第五随机数AT3'与第三随机数AT3是否一致；
- [115] 如果第五随机数AT3'与第三随机数AT3一致，支付终端使用认证密钥AUK加密第四随机数AT4生成第四随机数密文Sign4，并将第四随机数密文Sign4发送给KMS系统；
- [116] KMS系统调用第二硬件加密机使用认证密钥AUK解密接收到的第四随机数密文Sign4获得第六随机数AT4'，判断第六随机数AT4'与第四随机数AT4是否一致

- ；
- [117] 如果第六随机数AT4'与第四随机数AT4一致，KMS系统与支付终端认证通过。
- [118] 其中，对所述操作终端的操作必需经过操作员卡和管理员卡授权，具体包括：
- [119] 操作员卡和管理员卡分别产生公私钥对，并分别将公钥发给CA中心，生成操作员卡证书和管理员卡证书，并分别将操作员卡证书存储在操作员卡里将管理员卡证书存储在管理卡里；
- [120] 将操作员卡和管理员卡插在操作终端上，通过CA认证后，允许对操作终端的操作。
- [121] 其中，所述支付终端为POS终端、手机终端、智能IC卡或ATM机终端。
- [122] 在本发明中，传输密钥TK产生时计算TK的原始哈希值，当每次存储、传输或使用TK时先校验TK的哈希值，当检验通过后才可以使用TK。通过校验TK的哈希值可以防止存储设备异常导致存储的数据错误，确定密钥是否正确。
- [123] 本发明的有益效果为：本发明通过支付终端上传传输密钥TK，由传输密钥对TMK进行加密传输，实现支付终端远程下载终端主密钥TMK，其中，TK包括传输加密密钥TEK和传输认证密钥AUK，支付终端与KMS系统先经过认证密钥AU K进行双向身份认证，认证通过后用非对称传输加密密钥TEK加密终端主密钥T MK进行传输，提高了TMK的传输下载安全。进一步地，本发明主密钥TMK是由KMS系统生成的，因此方便KMS系统对主密钥TMK的后续维护和管理。进一步地，所述主密钥TMK下载和传输密钥TK上传是一并进行的，且都是通过操作终端进行的，因此大大提高了TMK下载的时间效率。同时在支付终端出厂投放给商户之前就可以统一通过操作终端进行主密钥TMK下载，由于操作终端与KMS系统之间通过CA中心进行过身份认证，且TMK是集中进行下载的，因此大大减小了主密钥TMK下载风险，并且商户拿到支付终端就可直接使用，大大方便了商户的使用。更进一步地，所述供应商密钥管理系统与KMS系统分别存储有保护密钥PK和MAC密钥MAK，支付终端产生的传输密钥TK由供应商密钥管理系统的保护密钥PK和MAC密钥MAK加密后进行上传，因此操作终端无需对TK进行进一步地转加密，大大简化了TK上传过程中的加密处理，在保证TK安全传输的前提下提高了TK上传的时间效率。

- [124] 在本发明中，操作终端上传TK前与KMS系统通过CA中心进行双方的身体认证，从而确保TK传送给正确的收单KMS系统，防止伪KMS系统窃取TK信息。
- [125] 在本发明中，KMS系统在下发主密钥TMK前，通过认证密钥AUK进行双方的身份认证，有效防止伪支付终端窃取TMK，以及确保支付终端是从正确的KMS系统下载TMK。
- [126] 在本发明中，所述操作终端还设置有操作员卡和管理员卡，只有在操作员卡和管理员卡均授权的情况下才能对操作终端进行操作，有效保证了上传的每一个TK的真实性和有效性。
- [127] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

[权利要求 1]

1、一种终端主密钥TMK安全下载方法，其特征在于，包括步骤：

S1、支付终端产生传输密钥TK以及生成传输密钥密文；

S2、支付终端上传传输密钥密文以及下载主密钥TMK；

其中步骤S1包括：

S11、供应商密钥管理系统调用第一硬件加密机、KMS 系统调用第二硬件加密机，分别在第一硬件加密机和第二硬件加密机中将供应商权限分量及KMS 系统权限分量合成保护密钥PK和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并分别存储在第一硬件加密机和第二硬件加密机中；

S12、供应商密钥管理系统调用第一硬件加密机产生公私钥对Pu_hsm、Pr_hsm，并将公钥Pu_hsm发送给支付终端；

S13、支付终端调用密码键盘生成传输密钥TK，所述TK包括传输加密密钥TEK和传输认证密钥AUK；

S14、支付终端调用密码键盘使用公钥Pu_hsm加密TK，生成第一传输密钥密文Ctk_Pu，并将第一传输密钥密文Ctk_Pu发送给供应商密钥管理系统；

S15、供应商密钥管理系统调用第一硬件加密机使用私钥Pr_hsm解密第一传输密钥密文Ctk_Pu获得传输密钥TK；

S16、供应商密钥管理系统调用第一硬件加密机使用保护密钥PK 加密传输密钥TK 并使用MAC 密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，并将第二传输密钥密文Ctk_pk发送给支付终端；

其中步骤S2包括：

S21、操作终端采集支付终端的第二传输密钥密文Ctk_pk；

S22、操作终端与KMS系统之间通过CA中心进行身份认证，认证通过后，将第二传输密钥密文Ctk_pk发送给KMS系统；

S23、KMS系统调用第二硬件加密机使用MAC密钥MAK对查询到

的第二传输密钥密文Ctk_pk 校验MAC 合法性，如果校验通过，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；

S24、KMS 系统获得传输密钥TK后调用第二硬件加密机使用认证密钥AUK 与支付终端进行双向认证；

S25、如果认证通过，KMS 系统调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至支付终端；

S26、支付终端调用密码键盘使用传输加密密钥TEK解密主密钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

2、根据权利要求1所述的安全下载终端主密钥TMK方法，其特征在于，所述步骤S22具体为：

操作终端生成公私钥对Pu_optm和Pr_optm，将公钥Pu_optm和操作终端标识信息发给CA中心，CA中心生成根证书AuthRCRT_optm 和对应私钥OptmWCRT_Prk，并将接收到的公钥Pu_optm和操作终端标识信息使用私钥OptmWCRT_Prk签名生成数字证书OptmWCRT，将数字证书OptmWCRT以及私钥OptmWCRT_Prk存储在操作终端中，将根证书AuthRCRT_optm存储在KMS系统；

KMS系统调用第二硬件加密机产生公私钥对Pr_kms和Pu_kms，将公钥Pu_kms和KMS系统标识信息发给CA中心，CA中心生成根证书AuthRCRT_kms和对应私钥ServerWCRT_Prk，并将接收到的公钥Pu_kms和KMS系统标识信息使用私钥ServerWCRT_Prk签名生成数字证书ServerWCRT，将数字证书ServerWCRT以及对应私钥ServerWCRT_Prk存储在KMS系统，将根证书AuthRCRT_kms存储在操作终端；

KMS系统将数字证书ServerWCRT发送给操作终端；

操作终端使用根证书AuthRCRT_kms验证数字证书ServerWCRT的

合法性，如果验证通过，操作终端生成第一随机数AT1，并将第一随机数AT1发送给KMS系统；

KMS系统使用私钥ServerWCRT_Prk签名第一随机数AT1生成第一随机数密文Sign1，并将第一随机数密文Sign1发送给操作终端；

操作终端使用数字证书ServerWCRT验证第一随机数密文Sign1的合法性，验证通过后，将数字证书OptmWCRT发送给KMS系统；

KMS系统使用根证书AuthRCRT_optm验证数字证书OptmWCRT的合法性，验证通过后，生成第二随机数AT2，并将第二随机数AT2发送给操作终端；

操作终端使用私钥OptmWCRT_Prk加密第二随机数AT2生成第二随机密文Sign2，并将第二随机密文Sign2发送给KMS系统；

KMS系统使用数字证书OptmWCRT验证第二随机密文Sign2的合法性，验证通过后，KMS系统与操作终端认证通过。

3、根据权利要求1所述的终端主密钥TMK安全下载方法，其特征在于，所述步骤S24具体包括：

支付终端产生第三随机数AT3并将第三随机数AT3发送至KMS系统；

KMS系统接收第三随机数AT3后产生第四随机数AT4，调用第二硬件加密机使用认证密钥AUK加密第三随机数AT3获得第三随机数密文Sign3，将第三随机数密文Sign3和第四随机数AT4发送给支付终端；

支付终端使用认证密钥AUK解密接收到的第三随机数密文Sign3获得第五随机数AT3'，判断第五随机数AT3'与第三随机数AT3是否一致：

如果第五随机数AT3'与第三随机数AT3一致，支付终端使用认证密钥AUK加密第四随机数AT4生成第四随机数密文Sign4，并将第四随机数密文Sign4发送给KMS系统；

KMS系统调用第二硬件加密机使用认证密钥AUK解密接收到的第

四随机数密文Sign4获得第六随机数AT4'，判断第六随机数AT4'与第四随机数AT4是否一致；

如果第六随机数AT4'与第四随机数AT4一致，KMS系统与支付终端认证通过。

4、根据权利要求1所述的终端主密钥TMK安全下载方法，其特征在于，对所述操作终端的操作必需经过操作员卡和管理员卡授权，具体包括：

操作员卡和管理员卡分别产生公私钥对，并分别将公钥发给CA中心，生成操作员卡证书和管理员卡证书，并分别将操作员卡证书存储在操作员卡里将管理员卡证书存储在管理卡里；

将操作员卡和管理员卡插在操作终端上，通过CA认证后，允许对操作终端的操作。

5、根据权利要求4所述的终端主密钥TMK安全下载方法，其特征在于，所述支付终端为POS终端、手机终端、智能IC卡或ATM机终端。

6、一种终端主密钥TMK安全下载系统，其特征在于，包括第一硬件加密机、第二硬件加密机、供应商密钥管理系统、支付终端、CA中心、操作终端以及KMS系统；所述供应商密钥管理系统包括协商密钥A模块、公钥产生模块、转加密模块，

支付终端包括TK产生模块、双向认证A模块、TMK接收模块，

操作终端包括TK采集模块、TK上传模块、CA认证A模块，

KMS系统包括协商密钥B模块、TK接收模块、CA认证B模块、双向认证B模块、TMK发送模块；

协商密钥A模块与协商密钥B模块用于调用第一硬件加密机和第二硬件加密机，分别在第一硬件加密机和第二硬件加密机中将供应商权限分量及KMS

系统权限分量合成保护密钥PK和MAC密钥MAK，并且将所述保护密钥PK和MAC密钥MAK一并分别存储在第一硬件加密机和第

二硬件加密机中；

公钥产生模块用于调用第一硬件加密机产生公私钥对Pu_hsm、Pr_hsm，并将公钥Pu_hsm发送给支付终端；

TK产生模块用于调用密码键盘生成传输密钥TK，所述TK包括传输加密密钥TEK和传输认证密钥AUK；

TK产生模块还用于调用密码键盘使用公钥Pu_hsm加密TK，生成第一传输密钥密文Ctk_Pu，并将第一传输密钥密文Ctk_Pu发送给供应商密钥管理系统；

转加密模块用于调用第一硬件加密机使用私钥Pr_hsm解密第一传输密钥密文Ctk_Pu获得传输密钥TK；

转加密模块还用于调用第一硬件加密机使用保护密钥PK 加密传输密钥TK 并使用MAC 密钥MAK 计算MAC 值，生成第二传输密钥密文Ctk_pk，并将第二传输密钥密文Ctk_pk发送给支付终端；

TK采集模块用于采集支付终端的第二传输密钥密文Ctk_pk；

CA认证A模块与CA认证B模块用于操作终端与KMS系统之间通过CA中心进行身份认证； TK上传模块用于当认证通过后，将第二传输密钥密文Ctk_pk发送给KMS系统；

TK接收模块用于调用第二硬件加密机使用MAC密钥MAK对查询到的第二传输密钥密文Ctk_pk 校验MAC 合法性，还用于当校验通过时，使用保护密钥PK 解密第二传输密钥密文Ctk_pk 获得传输密钥TK并将其存储在所述第二硬件加密机中；

双向认证A模块与双向认证B模块用于当KMS 系统获得传输密钥TK后，调用第二硬件加密机使用认证密钥AUK 与支付终端进行双向认证；

TMK发送模块用于当KMS系统与支付终端认证通过后，调用第二硬件加密机使用传输加密密钥TEK加密终端主密钥TMK生成主密钥密文Ctmk并将主密钥密文Ctmk发送至支付终端；

TMK接收模块用于调用密码键盘使用传输加密密钥TEK解密主密

钥密文Ctmk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

7、根据权利要求6所述的终端主密钥TMK安全下载系统，其特征在于，所述CA认证A模块包括第一随机数产生单元、第一数据收发单元、第一加解密单元、第一判断单元，

CA认证B模块包括第二随机数产生单元、第二数据收发单元、第二加解密单元、第二判断单元，

CA中心包括证书预置模块；

证书预置模块用于调用操作终端生成公私钥对Pu_optm和Pr_optm，并将公钥Pu_optm和操作终端标识信息向发给CA中心，CA中心生成根证书AuthRCRT_optm和对应私钥OptmWCRT_Prk，以及用于将接收到的公钥Pu_optm和操作终端标识信息使用私钥OptmWCRT_Prk签名生成数字证书OptmWCRT，以及用于数字证书OptmWCRT以及私钥OptmWCRT_Prk存储在操作终端中，将根证书AuthRCRT_optm存储在KMS系统；

证书预置模块用于调用第二硬件加密机产生公私钥对Pr_kms和Pu_kms，并将公钥Pu_kms和KMS标识信息发给CA中心，CA中心生成根证书AuthRCRT_kms和对应私钥ServerWCRT_Prk，以及用于将接收到的公钥Pu_kms和KMS系统标识信息使用私钥ServerWCRT_Prk签名生成数字证书ServerWCRT，以及用于将数字证书ServerWCRT以及对应私钥ServerWCRT_Prk存储在KMS系统，将根证书AuthRCRT_kms存储在操作终端；

第二数据收发单元用于将数字证书ServerWCRT发送给操作终端；

第一判断单元用于使用根证书AuthRCRT_kms验证数字证书ServerWCRT的合法性；第一随机数产生单元用于当所述数字证书ServerWCRT验证通过后，生成第一随机数AT1，并用于将第一随机数AT1发送给KMS系统；

第二加解密单元用于使用私钥ServerWCRT_Prk签名第一随机数AT

1生成第一随机数密文Sign1，并将第一随机数密文Sign1发送给操作终端；

第一判断单元用于使用数字证书ServerWCRT验证第一随机数密文Sign1的合法性，第一数据收发单元用于当第一随机数密文Sign1验证通过后，将数字证书OptmWCRT发送给KMS系统；

第二判断单元用于使用根证书AuthRCRT_optm验证数字证书OptmWCRT的合法性，第二随机数产生单元用于当数字证书OptmWCRT验证通过后，生成第二随机数AT2，并将第二随机数发送给操作终端；

第一加解密单元用于使用私钥OptmWCRT_Prk加密第二随机数AT2生成第二随机密文Sign2，并将第二随机密文Sign2发送给KMS系统；

第二判断单元用于使用数字证书OptmWCRT验证第二随机密文Sign2的合法性，验证通过后，KMS系统与操作终端认证通过。

8、根据权利要求6所述的终端主密钥TMK安全下载系统，其特征在于，所述双向认证A模块包括第三随机数产生单元、第三数据收发单元、第三加解密单元以及第三判断单元，所述双向认证B模块包括第四随机数产生单元、第四数据收发单元、第四加解密单元以及第四判断单元；

第三随机数产生单元用于产生第三随机数AT3；第三数据收发单元用于将产生的第三随机数AT3发送至KMS系统；第四数据收发单元用于接收第三随机数AT3；第四随机数产生单元用于在接收到第三随机数AT3时，产生第四随机数AT4；第四加解密单元用于在接收到第三随机数AT3时，调用第四硬件加密机使用传输认证密钥AUK加密第三随机数AT3获得第三随机数密文Sign3；第四数据收发单元用于将第三随机数密文Sign3和第四随机数AT4发送给支付终端；

第三加解密单元用于在接收到第三随机数密文Sign3和第四随机数

AT4时，使用传输认证密钥AUK解密接收到的第三随机数密文Sign3获得第五随机数AT3'；第三判断单元用于判断第五随机数AT3'与第三随机数AT3是否一致；

第三加解密单元用于当第五随机数AT3'与第三随机数AT3一致时，使用传输认证密钥AUK加密第四随机数AT4生成第四随机数密文Sign4；第三数据收发单元用于将第四随机数密文Sign4发送给KMS系统；

第四加解密单元用于在接收到第四随机数密文Sign4时，调用第二硬件加密机使用传输认证密钥AUK解密接收到的第四随机数密文Sign4获得第六随机数AT4'，第四判断单元用于判断第六随机数AT4'与第四随机数AT4是否一致，并当判定第六随机数AT4'与第四随机数AT4一致时，确认KMS系统与支付终端之间的双向认证通过。

9、根据权利要求6所述的终端主密钥TMK安全下载系统，其特征在于，所述操作终端还包括有操作员卡和管理员卡；

所述CA中心的证书预置模块还用于产生操作员卡证书和管理员卡证书，并用于将操作员卡证书存储在操作员卡里以及将管理员卡证书存储在管理卡里；

所述操作员卡和管理员卡用于当操作终端读取插在操作终端上的操作员卡和管理员卡，通过CA中心对操作员证书和管理员证书进行合法性认证通过时，授权对操作终端进行操作。

10、根据权利要求6至9所述的终端主密钥TMK安全下载系统，其特征在于，所述支付终端为POS终端、手机终端、智能IC卡、或ATM机终端。

经修改的权利要求**国际局收到日：2014年8月21日（21.08.2014）**

1、一种终端主密钥 TMK 安全下载方法，其特征在于，包括步骤：

S1、支付终端产生传输密钥 TK 以及生成传输密钥密文；

S2、支付终端上传传输密钥密文以及下载主密钥 TMK；

其中步骤 S1 包括：

S11、供应商密钥管理系统调用第一硬件加密机、KMS 系统调用第二硬件加密机，分别在第一硬件加密机和第二硬件加密机中将供应商权限分量及 KMS 系统权限分量合成保护密钥 PK 和 MAC 密钥 MAK，并且将所述保护密钥 PK 和 MAC 密钥 MAK 一并分别存储在第一硬件加密机和第二硬件加密机中；

S12、供应商密钥管理系统调用第一硬件加密机产生公私钥对 Pu_hsm、Pr_hsm，并将公钥 Pu_hsm 发送给支付终端；

S13、支付终端调用密码键盘生成传输密钥 TK，所述 TK 包括传输加密密钥 TEK 和传输认证密钥 AUK；

S14、支付终端调用密码键盘使用公钥 Pu_hsm 加密 TK，生成第一传输密钥密文 Ctk_Pu，并将第一传输密钥密文 Ctk_Pu 发送给供应商密钥管理系统；

S15、供应商密钥管理系统调用第一硬件加密机使用私钥 Pr_hsm 解密第一传输密钥密文 Ctk_Pu 获得传输密钥 TK；

S16、供应商密钥管理系统调用第一硬件加密机使用保护密钥 PK 加密传输密钥 TK 并使用 MAC 密钥 MAK 计算 MAC 值，生成第二传输密钥密文 Ctk_pk，并将第二传输密钥密文 Ctk_pk 发送给支付终端；

其中步骤 S2 包括：

S21、操作终端采集支付终端的第二传输密钥密文 Ctk_pk；

S22、操作终端与 KMS 系统之间通过 CA 中心进行身份认证，认证通过后，将第二传输密钥密文 Ctk_pk 发送给 KMS 系统；

S23、KMS 系统调用第二硬件加密机使用 MAC 密钥 MAK 对查询到的第二传输密钥密文 Ctk_pk 校验 MAC 合法性，如果校验通过，使用保护密钥 PK 解密第二传输密钥密文 Ctk_pk 获得传输密钥 TK 并将其存储在所述第二硬件加密机中；

S24、KMS 系统获得传输密钥 TK 后调用第二硬件加密机使用认证密钥

AUK 与支付终端进行双向认证；

S25、如果认证通过，KMS 系统调用第二硬件加密机使用传输加密密钥 TEK 加密终端主密钥 TMK 生成主密钥密文 Ctmk 并将主密钥密文 Ctmk 发送至支付终端；

S26、支付终端调用密码键盘使用传输加密密钥 TEK 解密主密钥密文 Ctmk 获得终端主密钥 TMK 并将终端主密钥 TMK 存储在密码键盘中。

2、根据权利要求 1 所述的安全下载终端主密钥 TMK 方法，其特征在于，所述步骤 S22 具体为：

操作终端生成公私钥对 Pu_optm 和 Pr_optm，将公钥 Pu_optm 和操作终端标识信息发给 CA 中心，CA 中心生成根证书 AuthRCRT_optm 和对应私钥 OptmWCRT_Prk，并将接收到的公钥 Pu_optm 和操作终端标识信息使用私钥 OptmWCRT_Prk 签名生成数字证书 OptmWCRT，将数字证书 OptmWCRT 以及私钥 OptmWCRT_Prk 存储在操作终端中，将根证书 AuthRCRT_optm 存储在 KMS 系统；

KMS 系统调用第二硬件加密机产生公私钥对 Pr_kms 和 Pu_kms，将公钥 Pu_kms 和 KMS 系统标识信息发给 CA 中心，CA 中心生成根证书 AuthRCRT_kms 和对应私钥 ServerWCRT_Prk，并将接收到的公钥 Pu_kms 和 KMS 系统标识信息使用私钥 ServerWCRT_Prk 签名生成数字证书 ServerWCRT，将数字证书 ServerWCRT 以及对应私钥 ServerWCRT_Prk 存储在 KMS 系统，将根证书 AuthRCRT_kms 存储在操作终端；

KMS 系统将数字证书 ServerWCRT 发送给操作终端；

操作终端使用根证书 AuthRCRT_kms 验证数字证书 ServerWCRT 的合法性，如果验证通过，操作终端生成第一随机数 AT1，并将第一随机数 AT1 发送给 KMS 系统；

KMS 系统使用私钥 ServerWCRT_Prk 签名第一随机数 AT1 生成第一随机数密文 Sign1，并将第一随机数密文 Sign1 发送给操作终端；

操作终端使用数字证书 ServerWCRT 验证第一随机数密文 Sign1 的合法性，验证通过后，将数字证书 OptmWCRT 发送给 KMS 系统；

KMS 系统使用根证书 AuthRCRT_optm 验证数字证书 OptmWCRT 的合法性，验证通过后，生成第二随机数 AT2，并将第二随机数 AT2 发送给操作终端；

操作终端使用私钥 OptmWCRT_Prk 加密第二随机数 AT2 生成第二随机密文 Sign2，并将第二随机密文 Sign2 发送给 KMS 系统；

KMS 系统使用数字证书 OptmWCRT 验证第二随机密文 Sign2 的合法性，验证通过后，KMS 系统与操作终端认证通过。

3、根据权利要求 1 所述的终端主密钥 TMK 安全下载方法，其特征在于，所述步骤 S24 具体包括：

支付终端产生第三随机数 AT3 并将第三随机数 AT3 发送至 KMS 系统；

KMS 系统接收第三随机数 AT3 后产生第四随机数 AT4，调用第二硬件加密机使用认证密钥 AUK 加密第三随机数 AT3 获得第三随机数密文 Sign3，将第三随机数密文 Sign3 和第四随机数 AT4 发送给支付终端；

支付终端使用认证密钥 AUK 解密接收到的第三随机数密文 Sign3 获得第五随机数 AT3'，判断第五随机数 AT3' 与第三随机数 AT3 是否一致；

如果第五随机数 AT3' 与第三随机数 AT3 一致，支付终端使用认证密钥 AUK 加密第四随机数 AT4 生成第四随机数密文 Sign4，并将第四随机数密文 Sign4 发送给 KMS 系统；

KMS 系统调用第二硬件加密机使用认证密钥 AUK 解密接收到的第四随机数密文 Sign4 获得第六随机数 AT4'，判断第六随机数 AT4' 与第四随机数 AT4 是否一致；

如果第六随机数 AT4' 与第四随机数 AT4 一致，KMS 系统与支付终端认证通过。

4、根据权利要求 1 所述的终端主密钥 TMK 安全下载方法，其特征在于，对所述操作终端的操作必需经过操作员卡和管理员卡授权，具体包括：

操作员卡和管理员卡分别产生公私钥对，并分别将公钥发给 CA 中心，生成操作员卡证书和管理员卡证书，并分别将操作员卡证书存储在操作员卡里将管理员卡证书存储在管理卡里；

将操作员卡和管理员卡插在操作终端上，通过 CA 认证后，允许对操作终端

的操作。

5、根据权利要求 4 所述的终端主密钥 TMK 安全下载方法，其特征在于，所述支付终端为 POS 终端、手机终端、智能 IC 卡或 ATM 机终端。

6、一种终端主密钥 TMK 安全下载系统，其特征在于，包括第一硬件加密机、第二硬件加密机、供应商密钥管理系统、支付终端、CA 中心、操作终端以及 KMS 系统；所述供应商密钥管理系统包括协商密钥 A 模块、公钥产生模块、转加密模块，

支付终端包括 TK 产生模块、双向认证 A 模块、TMK 接收模块，

操作终端包括 TK 采集模块、TK 上传模块、CA 认证 A 模块，

KMS 系统包括协商密钥 B 模块、TK 接收模块、CA 认证 B 模块、双向认证 B 模块、TMK 发送模块；

协商密钥 A 模块与协商密钥 B 模块用于调用第一硬件加密机和第二硬件加密机，分别在第一硬件加密机和第二硬件加密机中将供应商权限分量及 KMS 系统权限分量合成保护密钥 PK 和 MAC 密钥 MAK，并且将所述保护密钥 PK 和 MAC 密钥 MAK 一并分别存储在第一硬件加密机和第二硬件加密机中；

公钥产生模块用于调用第一硬件加密机产生公私钥对 Pu_hsm、Pr_hsm，并将公钥 Pu_hsm 发送给支付终端；

TK 产生模块用于调用密码键盘生成传输密钥 TK，所述 TK 包括传输加密密钥 TEK 和传输认证密钥 AUK；

TK 产生模块还用于调用密码键盘使用公钥 Pu_hsm 加密 TK，生成第一传输密钥密文 Ctk_Pu，并将第一传输密钥密文 Ctk_Pu 发送给供应商密钥管理系统；

转加密模块用于调用第一硬件加密机使用私钥 Pr_hsm 解密第一传输密钥密文 Ctk_Pu 获得传输密钥 TK；

转加密模块还用于调用第一硬件加密机使用保护密钥 PK 加密传输密钥 TK 并使用 MAC 密钥 MAK 计算 MAC 值，生成第二传输密钥密文 Ctk_pk，并将第二传输密钥密文 Ctk_pk 发送给支付终端；

TK 采集模块用于采集支付终端的第二传输密钥密文 Ctk_pk；

CA 认证 A 模块与 CA 认证 B 模块用于操作终端与 KMS 系统之间通过 CA

中心进行身份认证；TK 上传模块用于当认证通过后，将第二传输密钥密文 Ctk_pk 发送给 KMS 系统；

TK 接收模块用于调用第二硬件加密机使用 MAC 密钥 MAK 对查询到的第二传输密钥密文 Ctk_pk 校验 MAC 合法性，还用于当校验通过时，使用保护密钥 PK 解密第二传输密钥密文 Ctk_pk 获得传输密钥 TK 并将其存储在所述第二硬件加密机中；

双向认证 A 模块与双向认证 B 模块用于当 KMS 系统获得传输密钥 TK 后，调用第二硬件加密机使用认证密钥 AUK 与支付终端进行双向认证；

TMK 发送模块用于当 KMS 系统与支付终端认证通过后，调用第二硬件加密机使用传输加密密钥 TEK 加密终端主密钥 TMK 生成主密钥密文 Ctmk 并将主密钥密文 Ctmk 发送至支付终端；

TMK 接收模块用于调用密码键盘使用传输加密密钥 TEK 解密主密钥密文 Ctmk 获得终端主密钥 TMK 并将终端主密钥 TMK 存储在密码键盘中。

7、根据权利要求 6 所述的终端主密钥 TMK 安全下载系统，其特征在于，所述 CA 认证 A 模块包括第一随机数产生单元、第一数据收发单元、第一加解密单元、第一判断单元，

CA 认证 B 模块包括第二随机数产生单元、第二数据收发单元、第二加解密单元、第二判断单元，

CA 中心包括证书预置模块；

证书预置模块用于调用操作终端生成公私钥对 Pu_optm 和 Pr_optm，并将公钥 Pu_optm 和操作终端标识信息向发给 CA 中心，CA 中心生成根证书 AuthRCRT_optm 和对应私钥 OptmWCRT_Prk，以及用于将接收到的公钥 Pu_optm 和操作终端标识信息使用私钥 OptmWCRT_Prk 签名生成数字证书 OptmWCRT，以及用于数字证书 OptmWCRT 以及私钥 OptmWCRT_Prk 存储在操作终端中，将根证书 AuthRCRT_optm 存储在 KMS 系统；

证书预置模块用于调用第二硬件加密机产生公私钥对 Pr_kms 和 Pu_kms，并将公钥 Pu_kms 和 KMS 标识信息发给 CA 中心，CA 中心生成根证书 AuthRCRT_kms 和对应私钥 ServerWCRT_Prk，以及用于将接收到的公钥 Pu_kms

和 KMS 系统标识信息使用私钥 ServerWCRT_Prk 签名生成数字证书 ServerWCRT，以及用于将数字证书 ServerWCRT 以及对应私钥 ServerWCRT_Prk 存储在 KMS 系统，将根证书 AuthRCRT_kms 存储在操作终端；

第二数据收发单元用于将数字证书 ServerWCRT 发送给操作终端；

第一判断单元用于使用根证书 AuthRCRT_kms 验证数字证书 ServerWCRT 的合法性；第一随机数产生单元用于当所述数字证书 ServerWCRT 验证通过后，生成第一随机数 AT1，并用于将第一随机数 AT1 发送给 KMS 系统；

第二加解密单元用于使用私钥 ServerWCRT_Prk 签名第一随机数 AT1 生成第一随机数密文 Sign1，并将第一随机数密文 Sign1 发送给操作终端；

第一判断单元用于使用数字证书 ServerWCRT 验证第一随机数密文 Sign1 的合法性，第一数据收发单元用于当第一随机数密文 Sign1 验证通过后，将数字证书 OptmWCRT 发送给 KMS 系统；

第二判断单元用于使用根证书 AuthRCRT_optm 验证数字证书 OptmWCRT 的合法性，第二随机数产生单元用于当数字证书 OptmWCRT 验证通过后，生成第二随机数 AT2，并将第二随机数发送给操作终端；

第一加解密单元用于使用私钥 OptmWCRT_Prk 加密第二随机数 AT2 生成第二随机密文 Sign2，并将第二随机密文 Sign2 发送给 KMS 系统；

第二判断单元用于使用数字证书 OptmWCRT 验证第二随机密文 Sign2 的合法性，验证通过后，KMS 系统与操作终端认证通过。

8、根据权利要求 6 所述的终端主密钥 TMK 安全下载系统，其特征在于，所述双向认证 A 模块包括第三随机数产生单元、第三数据收发单元、第三加解密单元以及第三判断单元，所述双向认证 B 模块包括第四随机数产生单元、第四数据收发单元、第四加解密单元以及第四判断单元；

第三随机数产生单元用于产生第三随机数 AT3；第三数据收发单元用于将产生的第三随机数 AT3 发送至 KMS 系统；第四数据收发单元用于接收第三随机数 AT3；第四随机数产生单元用于在接收到第三随机数 AT3 时，产生第四随机数 AT4；第四加解密单元用于在接收到第三随机数 AT3 时，调用第四硬件加密机使用传输认证密钥 AUK 加密第三随机数 AT3 获得第三随机数密文 Sign3；第

四数据收发单元用于将第三随机数密文 Sign3 和第四随机数 AT4 发送给支付终端；

第三加解密单元用于在接收到第三随机数密文 Sign3 和第四随机数 AT4 时，使用传输认证密钥 AUK 解密接收到的第三随机数密文 Sign3 获得第五随机数 AT3'；第三判断单元用于判断第五随机数 AT3' 与第三随机数 AT3 是否一致；

第三加解密单元用于当第五随机数 AT3' 与第三随机数 AT3 一致时，使用传输认证密钥 AUK 加密第四随机数 AT4 生成第四随机数密文 Sign4；第三数据收发单元用于将第四随机数密文 Sign4 发送给 KMS 系统；

第四加解密单元用于在接收到第四随机数密文 Sign4 时，调用第二硬件加密机使用传输认证密钥 AUK 解密接收到的第四随机数密文 Sign4 获得第六随机数 AT4'，第四判断单元用于判断第六随机数 AT4' 与第四随机数 AT4 是否一致，并当判定第六随机数 AT4' 与第四随机数 AT4 一致时，确认 KMS 系统与支付终端之间的双向认证通过。

9、根据权利要求 6 所述的终端主密钥 TMK 安全下载系统，其特征在于，所述操作终端还包括有操作员卡和管理员卡；

所述 CA 中心的证书预置模块还用于产生操作员卡证书和管理员卡证书，并用于将操作员卡证书存储在操作员卡里以及将管理员卡证书存储在管理卡里；

所述操作员卡和管理员卡用于当操作终端读取插在操作终端上的操作员卡和管理员卡，通过 CA 中心对操作员证书和管理员证书进行合法性认证通过时，授权对操作终端进行操作。

10、根据权利要求 6 至 9 任一项所述的终端主密钥 TMK 安全下载系统，其特征在于，所述支付终端为 POS 终端、手机终端、智能 IC 卡、或 ATM 机终端。

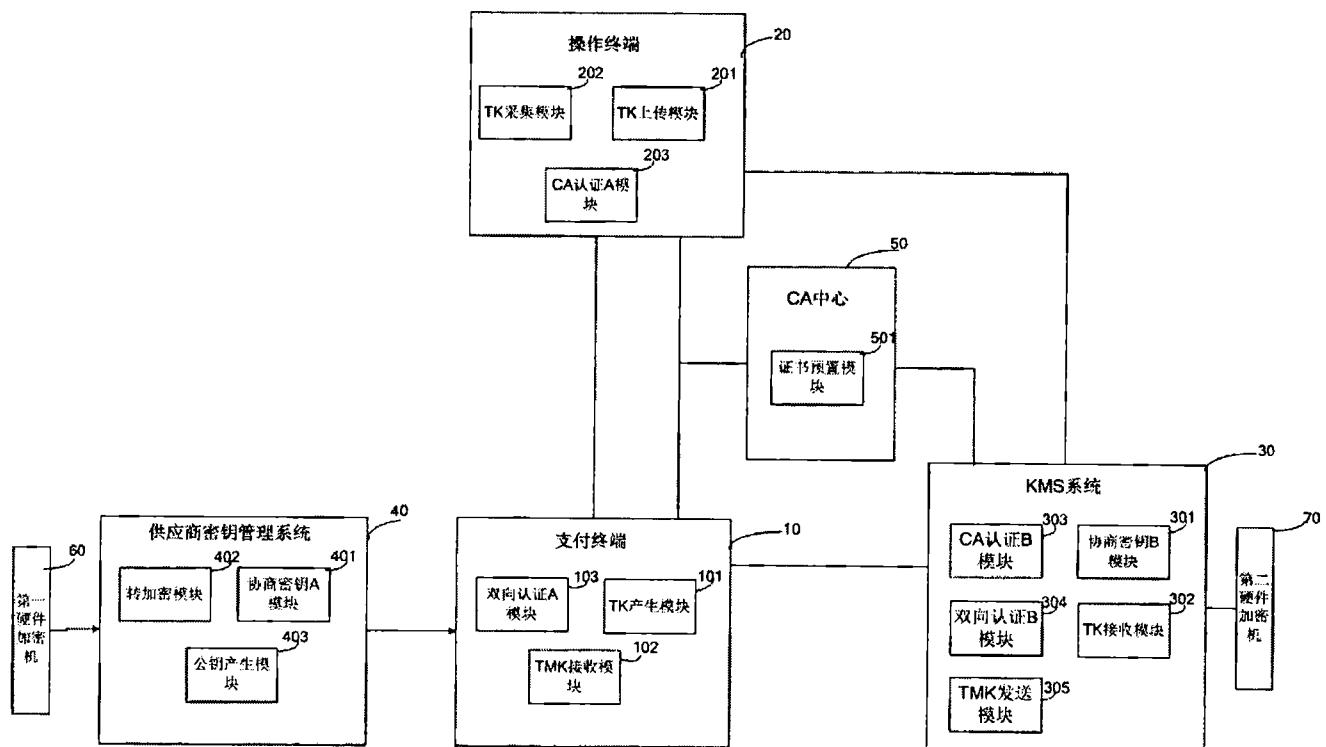


图 1

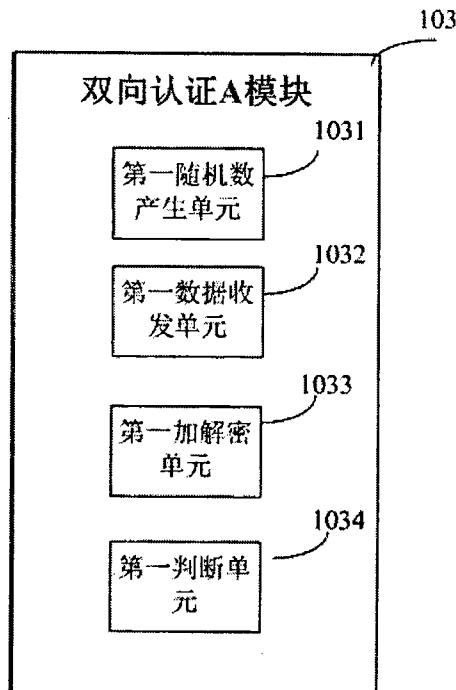


图 2

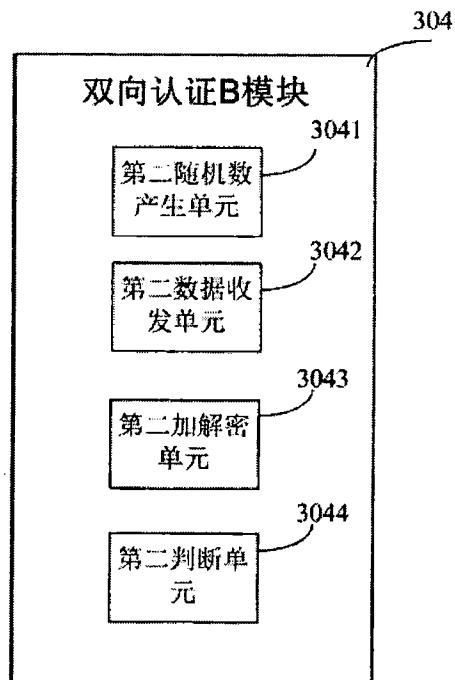


图 3

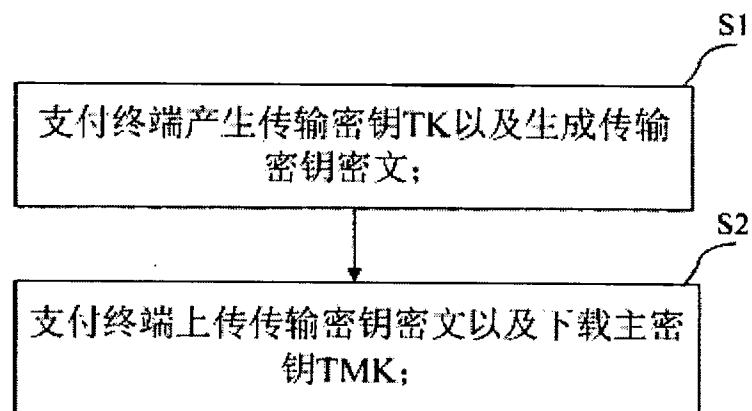


图 4

替换页 (细则第26条)

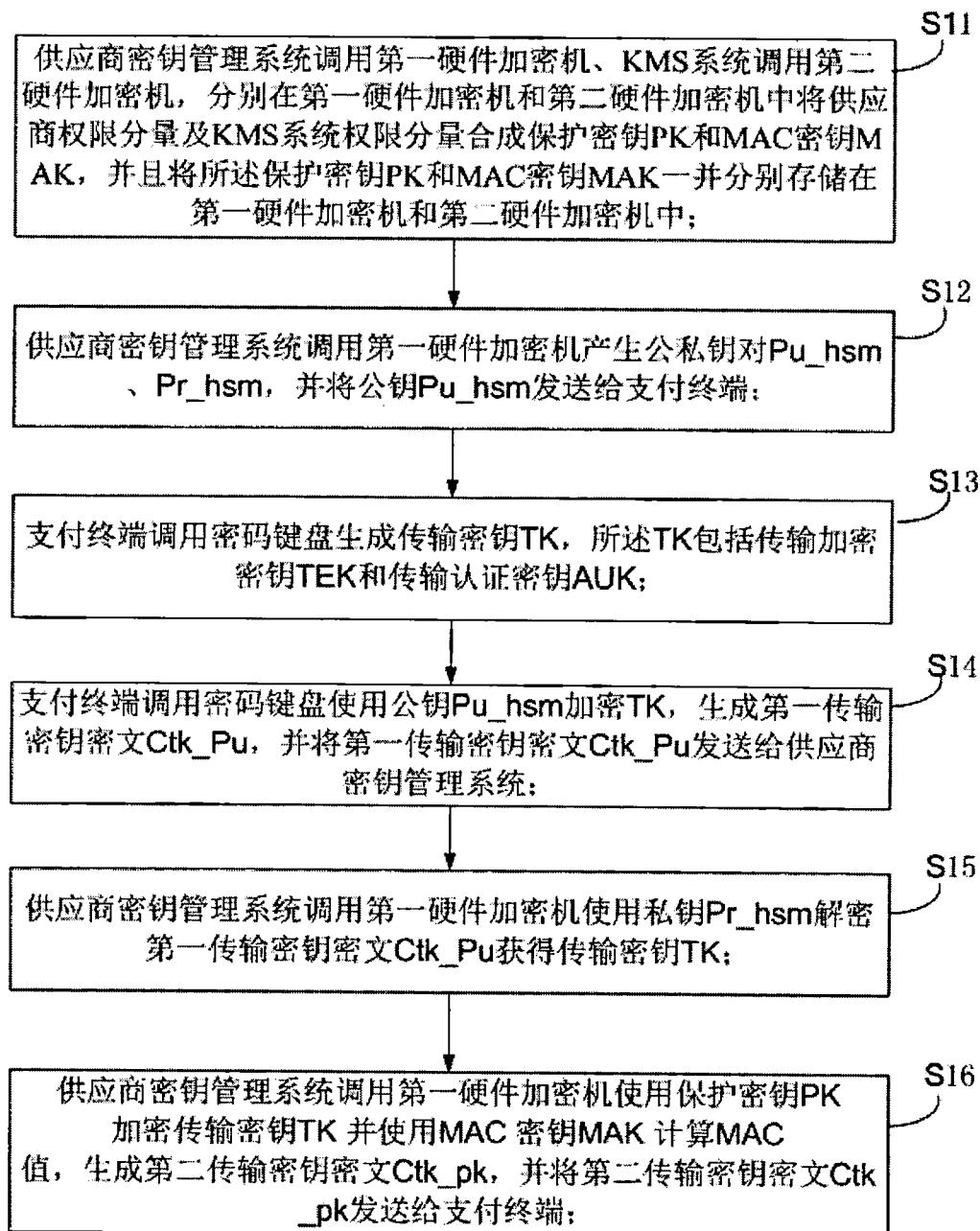


图 5

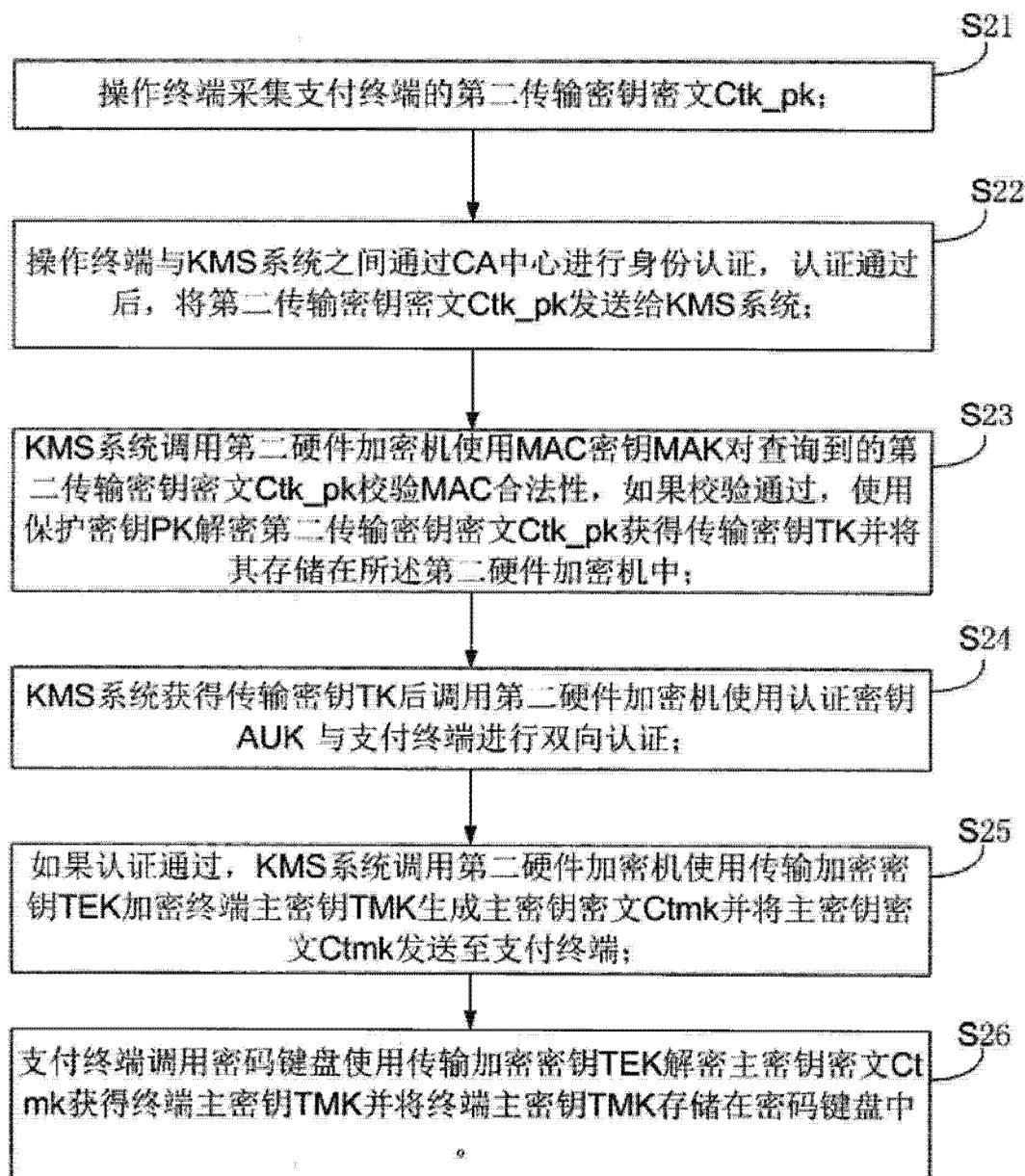


图 6

替换页(细则第26条)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/073215

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT, VEN, CPRSABS, SIPOABS: payment terminal, transmission key, hardware encryption, pos, TMK, key, CA, pay, terminal, transmi+, master key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103237004 A1 (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD.), 07 August 2013 (07.08.2013), the whole document	1-10
PX	CN 103220270 A1 (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD.), 24 July 2013 (24.07.2013), the whole document	1-10
PX	CN 103220271 A1 (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD.), 24 July 2013 (24.07.2013), the whole document	1-10
PX	CN 103237005 A1 (FUJIAN LANDI COMMERCIAL EQUIPMENT CO., LTD.), 07 August 2013 (07.08.2013), the whole document	1-10
A	CN 101930644 A (CHINA UNIONPAY CO., LTD.), 29 December 2010 (29.12.2010), the whole document	1-10
A	CN 101656007 A (ALLINPAY NETWORK SERVICE CO., LTD.), 24 February 2010 (24.02.2010), the whole document	1-10
A	CN 102148799 A (CHINA UNIONPAY CO., LTD.), 10 August 2011 (10.08.2011), the whole document	1-10

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

- “A” document defining the general state of the art which is not considered to be of particular relevance
- “E” earlier application or patent but published on or after the international filing date
- “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- “O” document referring to an oral disclosure, use, exhibition or other means
- “P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
16 May 2014 (16.05.2014)

Date of mailing of the international search report
26 June 2014 (26.06.2014)

Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer
YANG, Hongli
Telephone No.: (86-10) **62411277**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/073215**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7837098 B2 (NAUTILUS HYOSUNG INC.), 23 November 2010 (23.11.2010), the whole document	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2014/073215

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103237004 A1	07.08.2013	None	
CN 103220270 A1	24.07.2013	None	
CN 103220271 A1	24.07.2013	None	
CN 103237005 A1	07.08.2013	None	
CN 101930644 A	29.12.2010	SG 177349 A1 WO 2010148646 A1 CN 101930644 B CA 2766491 A1 SG 177349 B	28.02.2012 29.12.2010 16.04.2014 29.12.2010 15.11.2012
CN 101656007 A	24.02.2010	CN 101656007 B	16.02.2011
CN 102148799 A	10.08.2011	None	
US 7837098 B2	23.11.2010	US 2010116878 A1 KR 20100052668 A	13.05.2010 20.05.2010

国际检索报告

国际申请号

PCT/CN2014/073215

A. 主题的分类

H04L 9/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNTXT, VEN, CPRSABS, SIPOABS: 支付终端, 传输密钥, 硬件加密, pos, 主密钥, TMK, key, CA, pay, terminal, transmi+, master key

C. 相关文件

类型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 103237004A1 (福建联迪商用设备有限公司) 2013年 8月 07日 (2013 - 08 - 07) 全文	1-10
PX	CN 103220270A1 (福建联迪商用设备有限公司) 2013年 7月 24日 (2013 - 07 - 24) 全文	1-10
PX	CN 103220271A1 (福建联迪商用设备有限公司) 2013年 7月 24日 (2013 - 07 - 24) 全文	1-10
PX	CN 103237005A1 (福建联迪商用设备有限公司) 2013年 8月 07日 (2013 - 08 - 07) 全文	1-10
A	CN 101930644A (中国银联股份有限公司) 2010年 12月 29日 (2010 - 12 - 29) 全文	1-10
A	CN 101656007A (通联支付网络服务股份有限公司) 2010年 2月 24日 (2010 - 02 - 24) 全文	1-10
A	CN 102148799A (中国银联股份有限公司) 2011年 8月 10日 (2011 - 08 - 10) 全文	1-10

 其余文件在C栏的续页中列出。 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“&” 同族专利的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

国际检索实际完成的日期 2014年 5月 16日	国际检索报告邮寄日期 2014年 6月 26日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	受权官员 杨红丽 电话号码 (86-10)62411277

国际检索报告

国际申请号

PCT/CN2014/073215

C. 相关文件

类型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A 全文	US 7837098B2 (NAUTILUS HYOSUNG INC.) 2010年 11月 23日 (2010 - 11 - 23)	1-10

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/073215

检索报告引用的专利文件	公布日 (年/月/日)	同族专利		公布日 (年/月/日)
CN 103237004A1	2013年 8月 07日	无		
CN 103220270A1	2013年 7月 24日	无		
CN 103220271A1	2013年 7月 24日	无		
CN 103237005A1	2013年 8月 07日	无		
CN 101930644A	2010年 12月 29日	SG	177349A1	2012年 2月 28日
		WO	2010148646A1	2010年 12月 29日
		CN	101930644B	2014年 4月 16日
		CA	2766491A1	2010年 12月 29日
		SG	177349B	2012年 11月 15日
CN 101656007A	2010年 2月 24日	CN	101656007B	2011年 2月 16日
CN 102148799A	2011年 8月 10日	无		
US 7837098B2	2010年 11月 23日	US	2010116878A1	2010年 5月 13日
		KR	20100052668A	2010年 5月 20日

表 PCT/ISA/210 (同族专利附件) (2009年7月)