



(12)发明专利

(10)授权公告号 CN 103716154 B

(45)授权公告日 2017.08.01

(21)申请号 201310740540.9

(74)专利代理机构 福州市博深专利事务所(普

(22)申请日 2013.12.27

通合伙) 35214

(65)同一申请的已公布的文献号

代理人 林志峥

申请公布号 CN 103716154 A

(51)Int.Cl.

(43)申请公布日 2014.04.09

H04L 9/08(2006.01)

(66)本国优先权数据

G06Q 20/40(2012.01)

201310084397.2 2013.03.15 CN

G06Q 20/20(2012.01)

201310084671.6 2013.03.15 CN

(56)对比文件

201310084673.5 2013.03.15 CN

CN 101593389 A, 2009.12.02,

201310084653.8 2013.03.15 CN

CN 103237005 A, 2013.08.07,

(73)专利权人 福建联迪商用设备有限公司

CN 101656007 A, 2010.02.24,

地址 350003 福建省福州市软件大道89号

US 2006281442 A1, 2006.12.14,

福州软件园一区23号楼

CN 102148799 A, 2011.08.10,

(72)发明人 洪逸轩 苏文龙 孟陆强 姚承勇

审查员 徐佳

权利要求书3页 说明书7页 附图2页

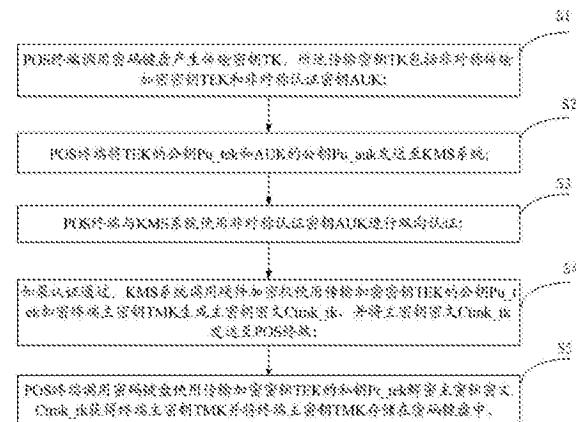
(54)发明名称

一种终端主密钥TMK安全下载方法及系统

(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：POS终端调用密码键盘产生传输密钥TK，所述传输密钥TK包括非对称传输加密密钥TEK和非对称认证密钥AUK；POS终端将TEK的公钥Pu_tek和AUK的公钥Pu_auk发送至KMS系统；POS终端与KMS系统使用非对称认证密钥AUK进行双向认证；如果认证通过，KMS系统调用硬件加密机使用传输加密密钥TEK的公钥Pu_tek加密终端主密钥TMK生成主密钥密文Ctmk_tk，并将主密钥密文Ctmk_tk发送至POS终端；POS终端调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。本发明的有益效果为采用非对称传输密钥TK加密TMK，实现POS终端远程下载TMK，非对称传输密钥TK保证TMK的安全传输。

B CN 103716154



CN

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、POS终端调用密码键盘产生传输密钥TK,所述传输密钥TK包括非对称传输加密密钥TEK和非对称认证密钥AUK;

S2、POS终端将TEK的公钥Pu_tek和AUK的公钥Pu_auk发送至KMS系统,所述KMS系统为密钥管理系统;

S3、POS终端与KMS系统使用非对称认证密钥AUK进行双向认证;

S4、如果认证通过,KMS系统调用硬件加密机使用传输加密密钥TEK的公钥Pu_tek加密终端主密钥TMK生成主密钥密文Ctmk_tk,并将主密钥密文Ctmk_tk发送至POS终端;

S5、POS终端调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk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所述的终端主密钥TMK安全下载方法,其特征在于,所述步骤S5具体包括:

POS终端调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK,并将主密钥TMK按TR-31格式进行打包,打包后以密文形式存储于密码键盘中。

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S3之前还包括:KMS系统调用硬件加密机产生公钥Pu_kms和私钥Pr_kms,将私钥Pr存储在硬件加密机中,将公钥Pu发给CA中心;CA中心使用根证书RootCrt_kms对公钥Pu_kms签名生成工作证书WorkCrt_kms;

将工作证书WorkCrt_kms预置于KMS系统,将工作证书WorkCrt_kms的上级根证书RootCrt_kms预置于POS终端。

4. 根据权利要求3所述的一种终端主密钥TMK安全下载方法,其特征在于,所述“POS终端与KMS系统使用非对称认证密钥AUK进行双向认证”具体包括:

POS终端产生第一随机数Rnd1,将硬件序列号SN和第一随机数Rnd1发送给KMS系统;

KMS系统生成第二随机数Rnd2,使用私钥Pr_kms对Rnd1加密生成第一密文C1,将Rnd2、C1以及WorkCrt_kms发送至POS终端;

POS终端使用KMS系统根证书RootCrt_kms校验KMS系统工作证书WorkCrt_kms的合法性,如果合法,从WorkCrt_kms提取公钥Pu_kms,使用Pu_kms解密第一密文C1获得第三随机数Rnd1' ;

POS终端判断第一随机数Rnd1与第三随机数Rnd1' 是否一致,如果一致,使用认证密钥AUK的私钥Pr_auk对第二随机数Rnd2加密生成第二密文C2,将C2发送给KMS系统;

KMS系统使用硬件序列号SN对应的认证密钥AUK的公钥Pu_auk解密第二密文C2生成第四随机数Rnd2' ;

KMS系统判断第二随机数Rnd2和第四随机数Rnd2' 是否一致,如果一致,判定双向认证成功。

5. 一种终端主密钥TMK安全下载系统,其特征在于,包括KMS系统、与KMS系统通信连接的POS终端、以及硬件加密机;所述POS终端包括TK产生模块、TK发送模块、解密模块、双向认证A模块,所述KMS系统包括TK接收模块、加密模块、双向认证B模块;

所述TK产生模块用于调用密码键盘产生传输密钥TK,其中,所述传输密钥TK包括非对

称传输加密密钥TEK和非对称认证密钥AUK；

所述TK发送模块用于将TEK的公钥Pu_tek和AUK的公钥Pu_auk发送至KMS系统，所述KMS系统为密钥管理系统；

所述双向认证A模块与双向认证B模块用于使用非对称认证密钥AUK进行POS终端与KMS系统之间的双向认证；

所述加密模块用于当认证通过时，调用硬件加密机使用传输加密密钥TEK的公钥Pu_tek加密终端主密钥TMK生成主密钥密文Ctmk_tk，并用于将主密钥密文Ctmk_tk发送至POS终端；

所述解密模块用于调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK，并用于将终端主密钥TMK存储在密码键盘中。

6. 根据权利要求5所述的终端主密钥TMK安全下载系统，其特征在于，所述POS终端还包括TR-31打包模块；

所述TR-31打包模块用于将TMK按TR-31格式进行打包，打包后以密文形式存储于密码键盘中。

7. 根据权利要求5所述的终端主密钥TMK安全下载系统，其特征在于，所述KMS系统还包括第一证书预置模块，所述POS终端还包括第二证书预置模块；

所述第一证书预置模块用于调用硬件加密机产生公钥Pu_kms和私钥Pr_kms，并将私钥Pr存储在硬件加密机中，将公钥Pu发给CA中心；还用于调用CA中心使用根证书RootCrt_kms对公钥Pu_kms签名生成工作证书WorkCrt_kms；以及用于将工作证书WorkCrt_kms预置于KMS系统；

所述第二证书预置模块用于将工作证书WorkCrt_kms的上级根证书RootCrt_kms预置于POS终端。

8. 根据权利要求7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模块包括第一随机数产生单元、第一数据收发单元、第一加解密单元以及第一判断单元，所述双向认证B模块包括第二随机数产生单元、第二数据收发单元、第二加解密单元以及第二判断单元；

所述第一随机数产生单元用于产生第一随机数Rnd1；

所述第一数据收发单元用于将硬件序列号SN和第一随机数Rnd1发送给KMS系统；

所述第二随机数产生单元用于生成第二随机数Rnd2；

所述第二加解密单元用于使用私钥Pr_kms对Rnd1加密生成第一密文C1，所述第二数据收发单元用于将Rnd2、C1以及WorkCrt_kms发送至POS终端；

所述第一判断单元用于使用KMS系统根证书RootCrt_kms校验KMS系统工作证书WorkCrt_kms的合法性；

所述第一加解密单元用于当所述工作证书WorkCrt_kms检验合法时，从WorkCrt_kms提取公钥Pu_kms，使用Pu_kms解密第一密文C1获得第三随机数Rnd1'；

第一判断单元还用于判断第一随机数Rnd1与第三随机数Rnd1'是否一致；

第一加解密单元用于当第一随机数Rnd1与第三随机数Rnd1'一致时，使用认证密钥AUK的私钥Pr_auk对第二随机数Rnd2加密生成第二密文C2；

第一数据收发单元用于将C2发送给KMS系统；

第二加解密单元用于使用硬件序列号SN对应的认证密钥AUK的公钥Pu_auk解密第二密文C2生成第四随机数Rnd2'；

第二判断单元用于判断第二随机数Rnd2和第四随机数Rnd2'是否一致，并当判定第四随机数Rnd2'与第二随机数Rnd2一致时，确认KMS系统与POS终端之间的双向认证通过。

一种终端主密钥TMK安全下载方法及系统

技术领域

[0001] 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。

背景技术

[0002] 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。

[0003] 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。

[0004] 为防范密钥泄露风险,POS终端主密钥的下载必须控制在管理中心的安全机房进行,通过人工集中下载终端主密钥。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。

发明内容

[0005] 为解决上述技术问题,本发明采用的一个技术方案是:

[0006] 一种终端主密钥TMK安全下载方法,包括步骤:S1、POS终端调用密码键盘产生传输

密钥TK,所述传输密钥TK包括非对称传输加密密钥TEK和非对称认证密钥AUK;S2、POS终端将TEK的公钥Pu_tek和AUK的公钥Pu_auk发送至KMS系统;S3、POS终端与KMS系统使用非对称认证密钥AUK进行双向认证;S4、如果认证通过,KMS系统调用硬件加密机使用传输加密密钥TEK的公钥Pu_tek加密终端主密钥TMK生成主密钥密文Ctmk_tk,并将主密钥密文Ctmk_tk发送至POS终端;S5、POS终端调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[0007] 本发明提供的另一种技术方案是:

[0008] 一种终端主密钥TMK安全下载系统,包括KMS系统、与KMS系统通信连接的POS终端、以及硬件加密机;所述POS终端包括TK产生模块、TK发送模块、解密模块、双向认证A模块,所述KMS系统包括TK接收模块、加密模块、双向认证B模块;所述TK产生模块用于调用密码键盘产生传输密钥TK,其中,所述传输密钥TK包括非对称传输加密密钥TEK和非对称认证密钥AUK;所述TK发送模块用于将TEK的公钥Pu_tek和AUK的公钥Pu_auk发送至KMS系统;所述双向认证A模块与双向认证B模块用于使用非对称认证密钥AUK进行POS终端与KMS系统之间的双向认证;所述加密模块用于当认证通过时,调用硬件加密机使用传输加密密钥TEK的公钥Pu_tek加密终端主密钥TMK生成主密钥密文Ctmk_tk,并用于将主密钥密文Ctmk_tk发送至POS终端;所述解密模块用于调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK,并用于将终端主密钥TMK存储在密码键盘中。

[0009] 本发明的有益效果为:本发明通过POS终端上传传输密钥TK,使用TK进行POS终端与KMS系统之间的认证和对终端主密钥TMK进行加密下载,实现POS终端远程下载终端主密钥TMK,大大方便了POS终端下载TMK。进一步地,所述TK包含的加密密钥TEK和认证密钥AUK都是非对称密钥,因此增强了POS终端与KMS系统之间双向认证的准确性以及TMK密文传输过程中的安全性。

附图说明

[0010] 图1为本发明一实施方式终端主密钥TMK安全下载系统的结构框图;

[0011] 图2为双向认证A模块的结构框图;

[0012] 图3为双向认证B模块的结构框图;

[0013] 图4为本发明一实施方式终端主密钥TMK安全下载方法的方法流程图;

[0014] 主要元件符号说明:

[0015] 10:POS终端;20:KMS系统;30:硬件加密机;101:TK产生模块;102:解密模块;103:TK发送模块;104:双向认证A模块;201:TK接收模块;202:加密模块;203:双向认证B模块;1041:第一随机数产生单元;1042:第一数据收发单元;1043:第一加解密单元;1044:第一判断单元;2031:第二随机数产生单元;2032:第二数据收发单元;2033:第二加解密单元;2034:第二判断单元

具体实施方式

[0016] 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。

[0017] 首先,对本发明涉及的缩略语和关键术语进行定义和说明:

- [0018] 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;
- [0019] 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;
- [0020] HSM: High Security Machine的简称,高安全设备,在该系统中为硬件加密机;
- [0021] KMS系统: Key Management System,密钥管理系统,用于管理终端主密钥TMK;
- [0022] 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;
- [0023] 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;
- [0024] PIK:Pin Key的简称,即Pin加密密钥,是工作密钥的一种;
- [0025] PINPAD:密码键盘;
- [0026] 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;
- [0027] POS:Point Of Sale的简称,即销售终端
- [0028] SNpinpad: 密码键盘的序列号,PINPAD是内置时,和POS终端序列号SNpos一致;
- [0029] SN: 支付终端的序列号;
- [0030] 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;
- [0031] 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;
- [0032] TMS:Terminal Management System的简称,即终端管理系统,用于完成支付终端信息管理、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;
- [0033] TMK:Terminal Master Key的简称,即终端主密钥,用于支付终端和支付收单系统之间工作密钥的加密传输;
- [0034] 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。
- [0035] 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。
- [0036] 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。
- [0037] 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)。

[0038] 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。

[0039] 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。

[0040] 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。

[0041] 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。

[0042] 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。

[0043] 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的方法可以保证TMK在传输过程中不会被破解。但是,在KMS系统下传TMK前没有认证POS终端的身份,仍然可能在在伪POS终端上传假TK窃取终端主密钥TMK的情况,因此需要一种能够在传输所述TMK前认证收送双方身份的终端主密钥TMK安全下载方案。

[0044] 下面就对本发明克服上述问题的技术方案进行详细说明。

[0045] 请参阅图1,为本发明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KMS系统20、与KMS系统20通信连接的POS终端10、以及硬件加密机30;所述POS终端10包括TK产生模块101、TK发送模块103、解密模块102、双向认证A模块104,所述KMS系统20包括TK接收模块201、加密模块202、双向认证B模块203。

[0046] 所述TK产生模块101用于调用密码键盘产生传输密钥TK,其中,所述传输密钥TK包括非对称传输加密密钥TEK和非对称认证密钥AUK;

[0047] 所述TK发送模块103用于将TEK的公钥Pu_tek和AUK的公钥Pu_auk发送至KMS系统

20。

[0048] 所述双向认证A模块104与双向认证B模块203用于使用非对称认证密钥AUK进行POS终端10与KMS系统20之间的双向认证；

[0049] 所述加密模块202用于当认证通过时，调用硬件加密机30使用传输加密密钥TEK的公钥Pu_tek加密终端主密钥TMK生成主密钥密文Ctmk_tk，并用于将主密钥密文Ctmk_tk发送至POS终端10；

[0050] 所述解密模块102用于调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK，并用于将终端主密钥TMK存储在密码键盘中。

[0051] 其中，所述POS终端10还包括TR-31打包模块；

[0052] 所述TR-31打包模块用于将TMK按TR-31格式进行打包，打包后以密文形式存储于密码键盘中。

[0053] 其中，所述KMS系统20还包括第一证书预置模块，所述POS终端还包括第二证书预置模块；

[0054] 所述第一证书预置模块用于调用硬件加密机产生公钥Pu_kms和私钥Pr_kms，并将私钥Pr_kms存储在硬件加密机中，将公钥Pu_kms发给CA中心；还用于调用CA中心使用根证书RootCrt_kms对公钥Pu_kms签名生成工作证书WorkCrt_kms；以及用于将工作证书WorkCrt_kms预置于KMS系统；

[0055] 所述第二证书预置模块用于将工作证书WorkCrt_kms的上级根证书RootCrt_kms预置于POS终端。

[0056] 请参阅图3和图4，图3为双向认证A模块104的结构框图，图4为双向认证B模块203的结构框图，其中，所述双向认证A模块104包括第一随机数产生单元1041、第一数据收发单元1042、第一加解密单元1043以及第一判断单元1044，所述双向认证B模块203包括第二随机数产生单元2031、第二数据收发单元2032、第二加解密单元2033以及第二判断单元2034；

[0057] 所述第一随机数产生单元1041用于产生第一随机数Rnd1；

[0058] 所述第一数据收发单元1042用于将硬件序列号SN和第一随机数Rnd1发送给KMS系统20；

[0059] 所述第二随机数产生单元2031用于生成第二随机数Rnd2；

[0060] 所述第二加解密单元2033用于使用私钥Pr_kms对Rnd1加密生成第一密文C1，所述第二数据收发单元2032用于将Rnd2、C1以及WorkCrt_kms发送至POS终端10；

[0061] 所述第一判断单元1044用于使用KMS系统根证书RootCrt_kms校验KMS系统工作证书WorkCrt_kms的合法性；

[0062] 所述第一加解密单元1043用于当所述工作证书WorkCrt_kms检验合法时，从WorkCrt_kms提取公钥Pu_kms，使用Pu_kms解密第一密文C1获得第三随机数Rnd1'；

[0063] 第一判断单元1044还用于判断第一随机数Rnd1与第三随机数Rnd1'是否一致；

[0064] 第一加解密单元1043用于当第一随机数Rnd1与第三随机数Rnd1'一致时，使用认证密钥AUK的私钥Pr_auk对第二随机数Rnd2加密生成第二密文C2；

[0065] 第一数据收发单元1042用于将C2发送给KMS系统20；

[0066] 第二加解密单元2033用于使用硬件序列号SN对应的认证密钥AUK的公钥Pu_auk解密第二密文C2生成第四随机数Rnd2'；

[0067] 第二判断单元2034用于判断第二随机数Rnd2和第四随机数Rnd2'是否一致，并当判定第四随机数Rnd2'与第二随机数Rnd2一致时，确认KMS系统20与POS终端10之间的双向认证通过。

[0068] 请参阅图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，该终端主密钥TMK安全下载方法包括：

[0069] S1、POS终端调用密码键盘产生传输密钥TK，所述传输密钥TK包括非对称传输加密密钥TEK和非对称认证密钥AUK；

[0070] S2、POS终端将TEK的公钥Pu_tek和AUK的公钥Pu_auk发送至KMS系统；

[0071] S3、POS终端与KMS系统使用非对称认证密钥AUK进行双向认证；

[0072] S4、如果认证通过，KMS系统调用硬件加密机使用传输加密密钥TEK的公钥Pu_tek加密终端主密钥TMK生成主密钥密文Ctmk_tk，并将主密钥密文Ctmk_tk发送至POS终端；

[0073] S5、POS终端调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK并将终端主密钥TMK存储在密码键盘中。

[0074] 其中，所述步骤S5具体包括：POS终端调用密码键盘使用传输加密密钥TEK的私钥Pr_tek解密主密钥密文Ctmk_tk获得终端主密钥TMK，并将主密钥TMK按TR-31格式进行打包，打包后以密文形式存储于密码键盘中。

[0075] 其中，所述步骤S3之前还包括：KMS系统调用硬件加密机产生公钥Pu_kms和私钥Pr_kms，将私钥Pr存储在硬件加密机中，将公钥Pu发给CA中心；CA中心使用根证书RootCrt_kms对公钥Pu_kms签名生成工作证书WorkCrt_kms；

[0076] 将工作证书WorkCrt_kms预置于KMS系统，将工作证书WorkCrt_kms的上级根证书RootCrt_kms预置于POS终端。

[0077] 其中，所述“POS终端与KMS系统使用非对称认证密钥AUK进行双向认证”具体包括：

[0078] POS终端产生第一随机数Rnd1，将硬件序列号SN和第一随机数Rnd1发送给KMS系统；

[0079] KMS系统生成第二随机数Rnd2，使用私钥Pr_kms对Rnd1加密生成第一密文C1，将Rnd2、C1以及WorkCrt_kms发送至POS终端；

[0080] POS终端使用KMS系统根证书RootCrt_kms校验KMS系统工作证书WorkCrt_kms的合法性，如果合法，从WorkCrt_kms提取公钥Pu_kms，使用Pu_kms解密第一密文C1获得第三随机数Rnd1'；

[0081] POS终端判断第一随机数Rnd1与第三随机数Rnd1'是否一致，如果一致，使用认证密钥AUK的私钥Pr_auk对第二随机数Rnd2加密生成第二密文C2，将C2发送给KMS系统；

[0082] KMS系统使用硬件序列号SN对应的认证密钥AUK的公钥Pu_auk解密第二密文C2生成第四随机数Rnd2'；

[0083] KMS系统判断第二随机数Rnd2和第四随机数Rnd2'是否一致，如果一致，判定双向认证成功。

[0084] 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。

[0085] 本发明的有益效果为：本发明通过上传传输密钥TK，其中TK包括非对称的加密密

钥AUK和非对称的认证密钥TEK,由AUK进行POS终端与KMS系统之间的双向认证,认证通过后由TEK进行加密终端主密钥TMK后进行下载,从而实现了POS终端远程下载终端主密钥TMK,通过认证密钥AUK进行双向谁保证了POS终端与KMS系统为合法身份,防止伪POS终端窃取TMK或伪KMS系统下发伪TMK,同时,AUK与TEK都是非对称密钥进一步提高了TMK的下载安全。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,下载后的主密钥TMK使用密码键盘键盘提供的加密方式加密后存储在POS终端的密码键盘内,提高了主密钥TMK在POS终端的安全。

[0086] 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。

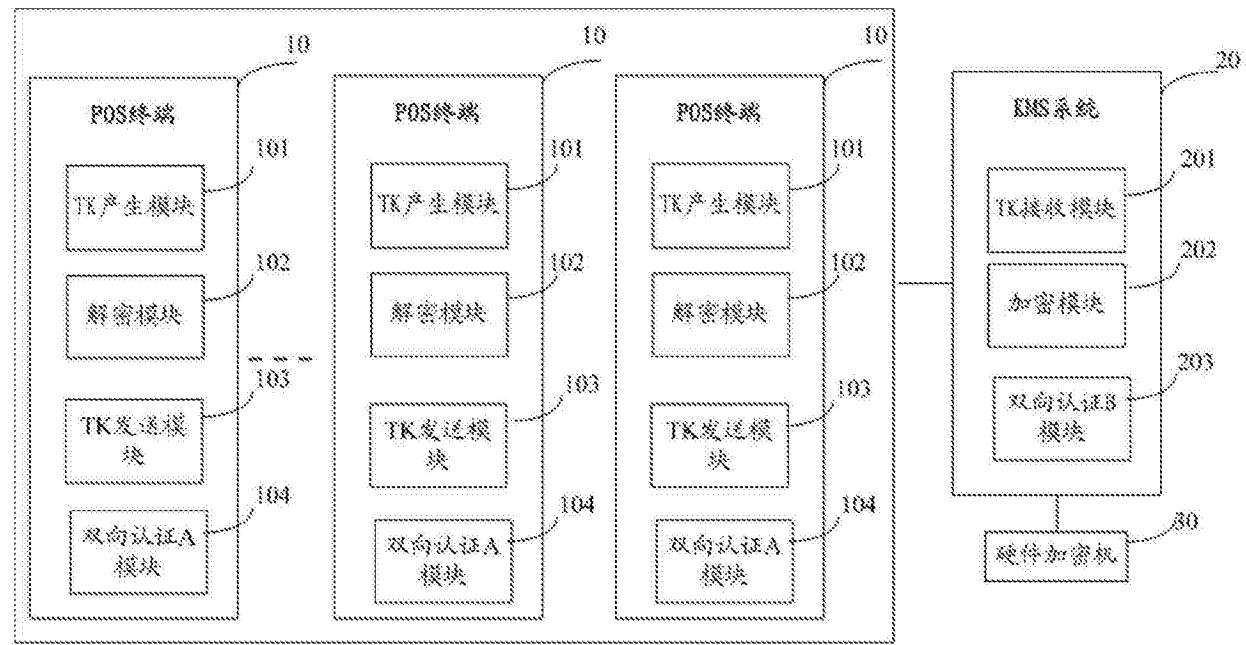


图1

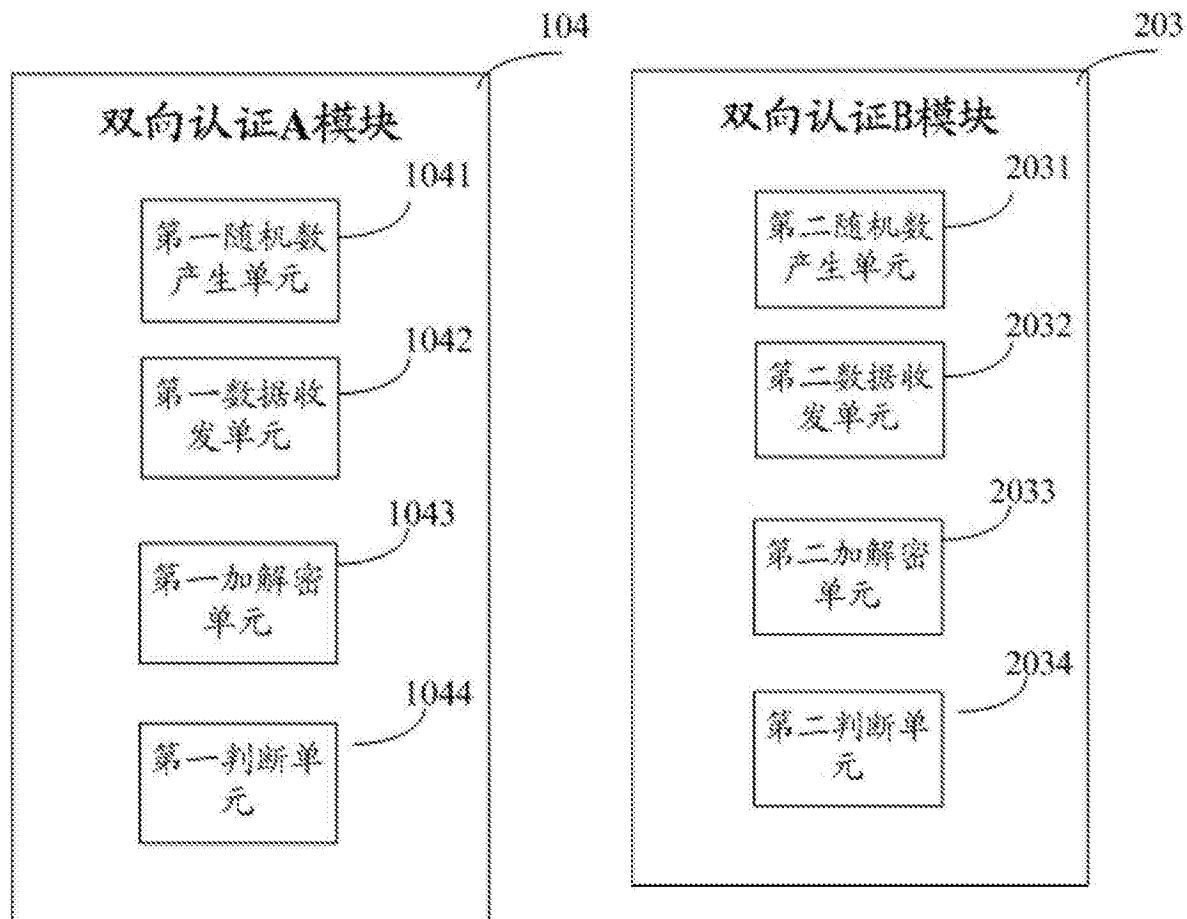


图2

图3

