(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103714642 B
(45)授权公告日 2016.02.03

(21)申请号 201310743191.6

(22)申请日 2013.12.27

(73)专利权人 福建联迪商用设备有限公司
地址 350003 福建省福州市软件大道89号
福州软件园一区23号楼

(72)发明人 姚承勇 彭荣收 孟陆强 洪逸轩

(74)专利代理机构 福州市鼓楼区博深专利代理事务所(普通合伙) 35214
代理人 林志峥

(51)Int.Cl.
G07G 1/00(2006.01)

审查员 徐丽莉

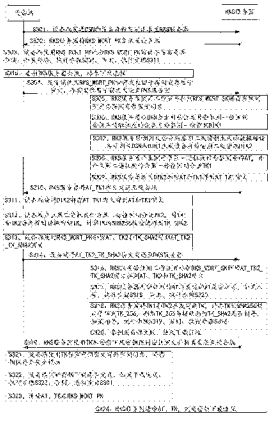
权利要求书4页 说明书10页 附图5页

(54)发明名称

密钥下载方法、管理方法、下载管理方法及装置和系统

(57)摘要

本发明公开一种密钥下载管理方法，设备端通过校验RKS服务器的工作证书公钥的数字签名来认证RKS服务器的合法性，RKS服务器生成一个鉴别令牌AT，用设备端的二级身份鉴别密钥DK2加密，将密文发送给设备端，设备端用其保存的二级身份鉴别密钥DK2解密，再用工作证书公钥加密后返回给RKS服务器，RKS服务器用其工作证书私钥解密后再对比鉴别令牌AT与生成的鉴别令牌AT是否一样，一样则表示设备端合法，从而实现双向身份认证。



CN 103714642 B

1.一种密钥下载方法,其特征在于,包括 :

设备端发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器 ;

设备端接收 RKS 服务器发送的工作证书公钥 RKS_WCRT_PK ;

设备端使用根公钥证书 RKS_RCRT 校验 RKS_WCRT_PK 的数字签名是否合法,如果合法,设备端使用 RKS_WCRT_PK 加密发散因子得到发散因子密文,并将发散因子密文发送至 RKS 服务器 ;

设备端接收 RKS 服务器发送的 AT_TK1 密文,所述 AT_TK1 密文由设备身份鉴别二级密钥 DIK2 加密鉴别令牌 AT 和第一传输密钥分量 TK1 得到,DIK2 通过调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和设备身份鉴别一级密钥 DIK1 生成 ;

设备端使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文 ;

设备端产生第三随机数作为第二传输密钥分量 TK2,将 TK1 和 TK2 异或得到传输密钥 TK,计算 TK 的 SHA256 校验值得到 TK_SHA2 ;

设备端使用 RKS_WCRT_PK 加密 AT、TK2 和 TK_SHA2 得到 AT_TK2_TK_SHA2 密文并将 AT_TK2_TK_SHA2 密文发送至 RKS 服务器 ;

设备端接收 RKS 服务器发送的密钥密文,所述密钥密文由 TK 加密需要下载的密钥得到 ;

设备端使用 TK 解密密钥密文得到密钥明文,将密钥保存至安全模块 ;

设备端判断密钥下载是否完成,如果下载完成,清除 AT、TK 及 RKS_WCRT_PK。

2.一种密钥管理方法,其特征在于,包括 :

RKS 服务器接收至少一个设备端发送的设备序列号 DSN 和设备身份鉴别请求 ;

RKS 服务器将工作证书公钥 RKS_WCRT_PK 发送至设备端 ;

RKS 服务器接收设备端发送的发散因子密文 ;

RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文 ;

RKS 服务器以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1 ;

调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2 ;

RKS 服务器产生 24 字节第一随机数作为鉴别令牌 AT,并产生第二随机数作为第一传输密钥分量 TK1 ;

RKS 服务器使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文,将 AT_TK1 密文发送至设备端 ;

RKS 服务器接收设备端发送的 AT_TK2_TK_SHA2 密文,所述 AT_TK2_TK_SHA2 密文由 RKS_WCRT_PK 加密 AT、第二传输密钥分量 TK2 和 TK_SHA2 得到,所述 TK_SHA2 是传输密钥 TK 的 SHA256 校验值,所述 TK 由 TK1 和 TK2 异或得到 ;

RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文,所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对 ;

RKS 服务器判断收到的 AT 与发送的 AT 是否相等,如果相等,将 TK1 和 TK2 异或得到 TK,计算 TK 的 SHA256 校验值得到 TK_256 ;

RKS 服务器判断 TK_256 与接收到的 TK_SHA2 是否相等,如果相等,使用 TK 加密需要下载的密钥得到密钥密文 ;

RKS 服务器将密钥密文发送至设备端；

RKS 服务器清除 AT、TK，完成密钥下载流程。

3. 一种密钥下载管理方法，其特征在于，包括：

设备端发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器；

RKS 服务器将工作证书公钥 RKS_WCRT_PK 发送至设备端；

设备端使用根公钥证书 RKS_RCRT 校验 RKS_WCRT_PK 的数字签名是否合法，如果合法，设备端使用 RKS_WCRT_PK 加密发散因子得到发散因子密文；

设备端将发散因子密文发送至 RKS 服务器；

RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文；

RKS 服务器以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1；

RKS 服务器调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2；

RKS 服务器产生 24 字节第一随机数作为鉴别令牌 AT，并产生第二随机数作为第一传输密钥分量 TK1；

RKS 服务器使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文，将 AT_TK1 密文发送至设备端；

设备端使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文；

设备端产生第三随机数作为第二传输密钥分量 TK2，将 TK1 和 TK2 异或得到传输密钥 TK，计算 TK 的 SHA256 校验值得到 TK_SHA2；

设备端使用 RKS_WCRT_PK 加密 AT、TK2 和 TK_SHA2 得到 AT_TK2_TK_SHA2 密文并将 AT_TK2_TK_SHA2 密文发送至 RKS 服务器；

RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文，所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对；

RKS 服务器判断收到的 AT 与发送的 AT 是否相等，如果相等，将 TK1 和 TK2 异或得到 TK，计算 TK 的 SHA256 校验值得到 TK_256，判断 TK_256 与接收到的 TK_SHA2 是否相等，如果相等，使用 TK 加密需要下载的密钥得到密钥密文并将密钥密文发送至设备端；

设备端使用 TK 解密密钥密文得到密钥明文，将密钥保存至安全模块；

设备端判断密钥下载是否完成，如果下载完成，清除 AT、TK 及 RKS_WCRT_PK；

RKS 服务器清除 AT、TK，完成密钥下载流程。

4. 一种密钥下载装置，其特征在于，包括：

鉴别请求发送单元，用于发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器；

第一接收单元，用于接收 RKS 服务器发送的工作证书公钥 RKS_WCRT_PK；

服务器身份校验单元，用于使用根公钥证书 RKS_RCRT 校验 RKS_WCRT_PK 的数字签名是否合法；

第一加密单元，用于当服务器校验单元校验合法时，使用 RKS_WCRT_PK 加密发散因子得到发散因子密文；

第一发送单元，用于将发散因子密文发送至 RKS 服务器；

第二接收单元，接收 RKS 服务器发送的 AT_TK1 密文，所述 AT_TK1 密文由设备身份鉴别二级密钥 DIK2 加密鉴别令牌 AT 和第一传输密钥分量 TK1 得到，DIK2 通过调用设备身份鉴

别二级密钥生成函数根据设备序列号 DSN 和设备身份鉴别一级密钥 DIK1 生成；

第一解密单元，使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文；

第二传输密钥分量生成单元，用于产生第三随机数作为第二传输密钥分量 TK2；

第一传输密钥运算单元，用于将 TK1 和 TK2 异或得到传输密钥 TK，计算 TK 的 SHA256 校验值得到 TK_SHA2；

第三接收单元，用于接收 RKS 服务器发送的密钥密文，所述密钥密文由 TK 加密需要下载的密钥得到；

第二解密单元，用于使用 TK 解密密钥密文得到密钥明文；

密钥下载单元，用于将密钥保存至安全模块；

第一清除单元，用于判断密钥下载是否完成，并当下载完成时清除 AT、TK 及 RKS_WCRT_PK。

5. 一种密钥管理装置，其特征在于，包括：

鉴别请求接收单元，用于接收至少一个设备端发送的设备序列号 DSN 和设备身份鉴别请求；

第二发送单元，用于将工作证书公钥 RKS_WCRT_PK 发送至设备端；

第四接收单元，用于接收设备端发送的发散因子密文，发散因子密文由 RKS_WCRT_PK 加密发散因子得到；

第三解密单元，用于使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文；

设备身份鉴别单元，用于以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1；

设备身份鉴别二级密钥生成单元，用于调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2；

鉴别令牌生成单元，用于产生 24 字节第一随机数作为鉴别令牌 AT；

第一传输密钥生成单元，用于产生第二随机数作为第一传输密钥分量 TK1；

第二加密单元，用于使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文；

第三发送单元，用于将 AT_TK1 密文发送至设备端；

第四接收单元，用于接收设备端发送的 AT_TK2_TK_SHA2 密文，所述 AT_TK2_TK_SHA2 密文由 RKS_WCRT_PK 加密 AT、第二传输密钥分量 TK2 和 TK_SHA2 得到，所述 TK_SHA2 是传输密钥 TK 的 SHA256 校验值，所述 TK 由 TK1 和 TK2 异或得到；

第四解密单元，用于使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文，所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对；

鉴别令牌校验单元，用于判断收到的 AT 与发送的 AT 是否相等；

第二传输密钥运算单元，用于当所述鉴别令牌校验单元判定相等时，将 TK1 和 TK2 异或得到 TK，计算 TK 的 SHA256 校验值得到 TK_256；

传输密钥校验单元，用于判断第二传输密钥运算单元生成的 TK_256 与接收到的 TK_SHA2 是否相等；

第三加密单元，用于当所述传输密钥校验单元判定相等时，使用 TK 加密需要下载的密钥得到密钥密文；

第三发送单元，用于将密钥密文发送至设备端；

第二清除单元，用于清除 AT、TK，完成密钥下载流程。

6. 一种密钥下载管理系统，包括 RKS 服务器和与所述 RKS 服务器通信连接的至少一个设备端，其特征在于，所述 RKS 服务器包括密钥管理装置，所述密钥管理装置如权利 5 所述；所述设备端包括密钥下载装置，所述密钥下载装置如权利要求 4 所述。

密钥下载方法、管理方法、下载管理方法及装置和系统

技术领域

[0001] 本发明涉及电子支付领域，尤其涉及一种设备端的密钥下载方法、管理方法、下载管理方法及装置和系统。

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)、终端管理系统(Terminal ManageSystem，TMS)、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；TMS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，保存在系统硬件中，只能使用，不能读取；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，全称对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以密文的方式出现，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在WK更新过程中，对WK进行加密保护。每台POS终端与TMS之间共享唯一的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都会被破解，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。下面归纳现有的TMK下载方案如下：

[0004] 1、明文手工输入方案：由TMS生成TMK明文，由手工方式直接输入到POS终端的密码键盘。这种方式存在很大的安全漏洞，操作人员容易截取TMK明文，而且存在手工输入错误的可能性，而且大量的设备需要逐一输入对应的TMK，通常为了提高安全性，每台POS的TMK都不一样，管理成本和工作量都相当复杂和巨大。

[0005] 2、IC卡密文导入方案：IC卡密文导入。TMK由TMS生成后，存在IC卡中，并由IC卡持有人设置IC卡密码保护IC卡中的TMK，导入POS终端时，通过POS终端密码键盘输入IC卡密码后，从IC卡导入到密码键盘中。该方案需要在TMS生成POS终端时由管理人员

一一插入 IC 卡并设置 IC 卡片密码。并在 POS 终端导入时，依然需要手工输入 IC 卡密码，IC 卡片密码泄露依然会导致 TMK 泄露也存在风险，而且大量的 POS 采用此方式，其管理成本及工作量也相当巨大。

[0006] 3、本地密钥母 POS 方案：当前支付行业的密钥下载多采用本地下载的方式，下载到金融 POS 终端的主密钥需要本地才能进行安全的下载，即金融 POS 终端需要携带到管理中心的安全机房，和位于安全机房的密钥母 POS 进行物理连接，并在管理员的操作下，从密钥母 POS 下载主密钥，然后将金融 POS 布放到部署地点，再通过主密钥进行远程下载工作密钥。

[0007] 上述三种方案都有以下缺点：设备需要到管理中心的安全机房，通过人工集中下载密钥。维护中心机房，工作量大；设备出厂后需要运算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。

[0008] 目前也有一种远程密钥下载方案：该方案 TMS 调用加密机产生一对公私钥，POS 终端调用密码键盘随机生成主密钥 TMK，并用 TMS 的公钥进行加密后上传给 TMS，TMS 调用加密机并用私钥解密 TMK 后存储，用 TMK 加密工作密钥下载给 POS 终端。该方案有以下缺点：TMS 对 POS 终端缺少身份鉴别，无法防止伪终端连接 TMS 下载工作密钥；POS 终端缺少对 TMS 的身份鉴别，无法防止伪 TMS 后台下载伪工作密钥。

发明内容

[0009] 为解决上述技术问题，本发明采用的一个技术方案是：

[0010] 提供一种密钥下载方法，包括：设备端发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器；设备端接收 RKS 服务器发送的工作证书公钥 RKS_WCRT_PK；设备端使用根公钥证书 RKS_RCRT 校验 RKS_WCRT_PK 的数字签名是否合法，如果合法，设备端使用 RKS_WCRT_PK 加密发散因子得到发散因子密文，并将发散因子密文发送至 RKS 服务器；设备端接收 RKS 服务器发送的 AT_TK1 密文，所述 AT_TK1 密文由设备身份鉴别二级密钥 DIK2 加密鉴别令牌 AT 和第一传输密钥分量 TK1 得到，DIK2 通过调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和设备身份鉴别一级密钥 DIK1 生成；设备端使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文；设备端产生第三随机数作为第二传输密钥分量 TK2，将 TK1 和 TK2 异或得到传输密钥 TK，计算 TK 的 SHA256 校验值得到 TK_SHA2；设备端使用 RKS_WCRT_PK 加密 AT、TK2 和 TK_SHA2 得到 AT_TK2_TK_SHA2 密文并将 AT_TK2_TK_SHA2 密文发送至 RKS 服务器；设备端接收 RKS 服务器发送的密钥密文，所述密钥密文由 TK 加密需要下载的密钥得到；设备端使用 TK 解密密钥密文得到密钥明文，将密钥保存至安全模块；设备端判断密钥下载是否完成，如果下载完成，清除 AT、TK 及 RKS_WCRT_PK。

[0011] 本发明采用的另一个技术方案是：

[0012] 提供一种密钥管理方法，包括：RKS 服务器接收至少一个设备端发送的设备序列号 DSN 和设备身份鉴别请求；RKS 服务器将工作证书公钥 RKS_WCRT_PK 发送至设备端；RKS 服务器接收设备端发送的发散因子密文；RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文；RKS 服务器以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1；调用设备身份鉴别二级密钥生成函数根据设

备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2 ;RKS 服务器产生 24 字节第一随机数作为鉴别令牌 AT,并产生第二随机数作为第一传输密钥分量 TK1 ;RKS 服务器使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文,将 AT_TK1 密文发送至设备端 ;RKS 服务器接收设备端发送的 AT_TK2_TK_SHA2 密文,所述 AT_TK2_TK_SHA2 密文由 RKS_WCRT_PK 加密 AT、第二传输密钥分量 TK2 和 TK_SHA2 得到,所述 TK_SHA2 是传输密钥 TK 的 SHA256 校验值,所述 TK 由 TK1 和 TK2 异或得到 ;RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文,所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对 ;RKS 服务器判断收到的 AT 与发送的 AT 是否相等,如果相等,将 TK1 和 TK2 异或得到 TK,计算 TK 的 SHA256 校验值得到 TK_256 ;RKS 服务器判断 TK_256 与接收到的 TK_SHA2 是否相等,如果相等,使用 TK 加密需要下载的密钥得到密钥密文 ;RKS 服务器将密钥密文发送至设备端 ;RKS 服务器清除 AT、TK,完成密钥下载流程。

[0013] 本发明采用的另一个技术方案是 :

[0014] 提供一种密钥下载管理方法,包括 :设备端发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器 ;RKS 服务器将工作证书公钥 RKS_WCRT_PK 发送至设备端 ;设备端使用根公钥证书 RKS_RCRT 校验 RKS_WCRT_PK 的数字签名是否合法,如果合法,设备端使用 RKS_WCRT_PK 加密发散因子得到发散因子密文 ;设备端将发散因子密文发送至 RKS 服务器 ;RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文 ;RKS 服务器以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1;RKS 服务器调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2 ;RKS 服务器产生 24 字节第一随机数作为鉴别令牌 AT,并产生第二随机数作为第一传输密钥分量 TK1 ;RKS 服务器使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文,将 AT_TK1 密文发送至设备端 ;设备端使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文 ;设备端产生第三随机数作为第二传输密钥分量 TK2,将 TK1 和 TK2 异或得到传输密钥 TK,计算 TK 的 SHA256 校验值得到 TK_SHA2; 设备端使用 RKS_WCRT_PK 加密 AT、TK2 和 TK_SHA2 得到 AT_TK2_TK_SHA2 密文并将 AT_TK2_TK_SHA2 密文发送至 RKS 服务器 ;RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文,所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对 ;RKS 服务器判断收到的 AT 与发送的 AT 是否相等,如果相等,将 TK1 和 TK2 异或得到 TK,计算 TK 的 SHA256 校验值得到 TK_256,判断 TK_256 与接收到的 TK_SHA2 是否相等,如果相等,使用 TK 加密需要下载的密钥得到密钥密文并将密钥密文发送至设备端 ;设备端使用 TK 解密密钥密文得到密钥明文,将密钥保存至安全模块 ;设备端判断密钥下载是否完成,如果下载完成,清除 AT、TK 及 RKS_WCRT_PK ;RKS 服务器清除 AT、TK,完成密钥下载流程。

[0015] 本发明采用的另一个技术方案是 :

[0016] 提供一种密钥下载装置,包括 :鉴别请求发送单元,用于发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器 ;第一接收单元,用于接收 RKS 服务器发送的工作证书公钥 RKS_WCRT_PK ;服务器身份校验单元,用于使用根公钥证书 RKS_RCRT 校验 RKS_WCRT_PK 的数字签名是否合法 ;第一加密单元,用于当服务器校验单元校验合法时,使用 RKS_WCRT_PK 加密发散因子得到发散因子密文 ;第一发送单元,用于将发散因子密文发送至 RKS 服务器 ;第二接收单元,接收 RKS 服务器发送的 AT_TK1 密文,所述 AT_TK1 密文由设备身份鉴别二级密

钥 DIK2 加密鉴别令牌 AT 和第一传输密钥分量 TK1 得到，DIK2 通过调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和设备身份鉴别一级密钥 DIK1 生成；第一解密单元，使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文；第二传输密钥分量生成单元，用于产生第三随机数作为第二传输密钥分量 TK2；第一传输密钥运算单元，用于将 TK1 和 TK2 异或得到传输密钥 TK，计算 TK 的 SHA256 校验值得到 TK_SHA2；第三接收单元，用于接收 RKS 服务器发送的密钥密文，所述密钥密文由 TK 加密需要下载的密钥得到；第二解密单元，用于使用 TK 解密密钥密文得到密钥明文；密钥下载单元，用于将密钥保存至安全模块；第一清除单元，用于判断密钥下载是否完成，并当下载完成时清除 AT、TK 及 RKS_WCRT_PK。

[0017] 本发明采用的另一个技术方案是：

[0018] 提供一种密钥管理装置包括：鉴别请求接收单元，用于接收至少一个设备端发送的设备序列号 DSN 和设备身份鉴别请求；第二发送单元，用于将工作证书公钥 RKS_WCRT_PK 发送至设备端；第四接收单元，用于接收设备端发送的发散因子密文，发散因子密文由 RKS_WCRT_PK 加密发散因子得到；第三解密单元，用于使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文；设备身份鉴别单元，用于以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1；设备身份鉴别二级密钥生成单元，用于调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2；鉴别令牌生成单元，用于产生 24 字节第一随机数作为鉴别令牌 AT；第一传输密钥生成单元，用于产生第二随机数作为第一传输密钥分量 TK1；第二加密单元，用于使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文；第三发送单元，用于将 AT_TK1 密文发送至设备端；第四接收单元，用于接收设备端发送的 AT_TK2_TK_SHA2 密文，所述 AT_TK2_TK_SHA2 密文由 RKS_WCRT_PK 加密 AT、第二传输密钥分量 TK2 和 TK_SHA2 得到，所述 TK_SHA2 是传输密钥 TK 的 SHA256 校验值，所述 TK 由 TK1 和 TK2 异或得到；第四解密单元，用于使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文，所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对；鉴别令牌校验单元，用于判断收到的 AT 与发送的 AT 是否相等；第二传输密钥运算单元，用于当所述鉴别令牌校验单元判定相等时，将 TK1 和 TK2 异或得到 TK，计算 TK 的 SHA256 校验值得到 TK_256；传输密钥校验单元，用于判断第二传输密钥运算单元生成的 TK_256 与接收到的 TK_SHA2 是否相等；第三加密单元，用于当所述传输密钥校验单元判定相等时，使用 TK 加密需要下载的密钥得到密钥密文；第三发送单元，用于将密钥密文发送至设备端；第二清除单元，用于清除 AT、TK，完成密钥下载流程。装置如上所述；所述设备端包括密钥下载装置，所述密钥下载装置如上所述。

[0019] 本发明的密钥下载方法、管理方法、下载管理方法及装置和系统，实现设备端从 RKS 服务器远程下载主密钥，避免设备端需要集中下载主密钥后才能布放到商户，设备端出厂后，可以直接布放到部署地点，避免需要将设备端集中到某固定机房下载密钥后再布放到部署地点。

附图说明

[0020] 图 1 是本发明一实施方式中一种密钥下载管理系统的结构框图；

[0021] 图 2 是本发明一实施方式中一种密钥下载装置的结构框图；

[0022] 图 3 是本发明一实施方式中一种密钥管理装置的结构框图；

[0023] 图 4 是本发明一实施方式中一种密钥下载方法的流程图；

[0024] 图 5 是本发明一实施方式中一种密钥管理方法的流程图；

[0025] 图 6 是本发明一实施方式中一种密钥下载管理方法的流程图。

[0026] 主要元件符号说明

[0027] 设备端 1；密钥下载装置 10；RKS 服务器 3；密钥管理装置 30；

[0028] 鉴别请求发送单元 11；第一接收单元 12；服务器身份校验单元 13；

[0029] 第一解密单元 14；第二传输密钥分量生成单元 15；

[0030] 第一传输密钥运算单元 16；第一加密单元 17；第一发送单元 18；

[0031] 第二接收单元 19；第二解密单元 20；密钥下载单元 21；第一清除单元 22；

[0032] 第三接收单元 23；鉴别请求接收单元 31；设备身份鉴别单元 32；

[0033] 鉴别令牌生成单元 33；第一传输密钥生成单元 34；

[0034] 第二加密单元 35；第三发送单元 36；第四接收单元 37；

[0035] 第三解密单元 38；鉴别令牌校验单元 39；第二传输密钥运算单元 40；

[0036] 传输密钥校验单元 41；第三加密单元 42；第三发送单元 43；

[0037] 第二清除单元 44；设备身份鉴别二级密钥生成单元 45；第四解密单元 46。

具体实施方式

[0038] 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。

[0039] 首先，对本发明涉及的缩略语和关键术语进行定义和说明：

[0040] 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。

[0041] 非对称密钥：非对称加密算法需要两个密钥：公开密钥(public key)和私有密钥(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）。

[0042] 数字签名：是非对称密钥加密技术与数字摘要技术的应用。数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送的公钥才能解密被加密的摘要信息，然后用对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性和合法性。数字签名是个加密的过程，数字签名验证是个解密的过程。

[0043] RSA：一种非对称密钥算法。RSA 公钥加密算法是 1977 年由 Ron Rivest、Adi Shamirh 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。

[0044] 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 Triple DES 的缩语(即三重数据加密标准)，DES 则是英文 Data Encryption Standard(数据加密标准)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。

[0045] 请参阅图 1，是本发明一实施方式中一种密钥下载管理系统的结构框图，该密钥下载管理系统包括 RKS 服务器 3 和与所述 RKS 服务器 3 通信连接的至少一个设备端 1，所述 RKS 服务器 3 包括密钥管理装置 30，所述设备端 1 包括密钥下载装置 10，该设备端 1 为 POS 终端，该 RKS 服务器 3 为远程密钥服务器，位于管理中心机房，负责 POS 终端主密钥、工作密钥等密钥的生成和维护等，该 RKS 服务器 3 包括密钥数据库，即 POS 终端的主密钥数据库或工作密钥数据库，此处代表需要通过远程下载的 TMK 密钥数据库，该 TMK 密钥数据库通常由一台专门的加密机进行产生并存储密钥。

[0046] 请参阅图 2，是本发明一实施方式中一种密钥下载装置的结构框图。一种密钥下载装置 10 包括鉴别请求发送单元 11、第一接收单元 12、服务器身份校验单元 13、第一解密单元 14、第二传输密钥分量生成单元 15、第一传输密钥运算单元 16、第一加密单元 17、第一发送单元 18、第二接收单元 19、第二解密单元 20、密钥下载单元 21、第一清除单元 22、第三接收单元 23。

[0047] 所述鉴别请求发送单元 11 用于发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器，其中，DSN 与设备端 1 一一对应；第一接收单元 12 用于接收 RKS 服务器 3 发送的工作证书公钥 RKS_WCRT_PK，其中，RKS_WCRT_PK 包含根私钥证书 RKS_RCRT_SK 对其的数字签名，确保 RKS_WCRT_PK 的合法，没有办法进行伪造。工作证书 RKS_WCRT 是一对非对称密钥对，如果是 RSA 密钥，位数最低 2048 位，工作证书 RKS_WCRT 由工作证书公钥 RKS_WCRT_PK 和工作证书私钥 RKS_WCRT_SK 组成，RKS_WCRT 需要保存在安全介质中，例如，可以静态存储于 IC 卡中作为备份，然后导入到 RKS 服务器 3 的安全存储介质中。

[0048] 服务器身份校验单元 13 用于使用根公钥证书 RKS_RCRT_PK 校验 RKS_WCRT_PK 的数字签名是否合法，其中，RKS_RCRT_PK 在设备端 1 出厂时预装在固件中，密钥服务器根证书 RKS_RCRT 是一对非对称密钥对，如果是 RSA 密钥，数最低为 2048 位，RKS_RCRT 由根公钥证书 RKS_RCRT_PK 和根私钥证书 RKS_RCRT_SK 组成，RKS_RCRT_PK 用于校验 RKS_WCRT_PK 的合法性。RKS_RCRT_SK 用于产生数字签名给 RKS_WCRT_PK 进行签名。RKS_RCRT 需要存储在安全介质中，根私钥证书 RKS_RCRT_SK 需要严格保护，可保存在 IC 卡中，只能用于对工作证书公钥 RKS_WCRT_PK 进行签名。

[0049] 第一加密单元 17 用于当服务器校验单元 13 校验合法时，使用 RKS_WCRT_PK 加密

发散因子得到发散因子密文；第一发送单元 18 用于将发散因子密文发送至 RKS 服务器 3；第二接收单元 19 用于接收 AT_TK1 密文，所述 AT_TK1 密文由设备身份鉴别二级密钥 DIK2 加密鉴别令牌 AT 和第一传输密钥分量 TK1 得到，DIK2 通过调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和设备身份鉴别一级密钥 DIK1 生成。其中，设备身份鉴别二级密钥 DIK2 和发散因子在设备端 1 生产阶段，由本地密钥母 POS 生成。发散因子用于参与设备身份鉴别二级密钥产生，是随机数或者用于辅助 RKS 服务器或本地密钥母 POS 的数据，例如，可以由本地密钥母 POS 序列号、生产日期、生产批次号等组成。设备身份鉴别一级密钥由 RKS 服务器生成，并以安全的方式导入到本地密钥母 POS 中。在生产阶段，建立一个安全环境，将设备端 1 和本地密钥母 POS 进行物理连接，本地密钥母 POS 从设备读取设备序列号 DSN，在本地密钥母 POS 内部生成设备鉴别二级密钥，以安全的方式将设备鉴别二级密钥 DIK2 和发散因子导入到设备端 1 中。设备序列号 DSN 每设备端唯一，从而保证设备鉴别二级密钥 DIK2 也能每设备端唯一。设备身份鉴别二级密钥生成函数为单向发散算法，单向发散算法由设备端 1 和 RKS 服务器 3 预先约定而成，保证以设备序列号 DSN 和发散因子作为输入参数 1，设备身份鉴别一级密钥 DIK1 作为输入参数 2，生成输出结果为设备设备鉴别二级密钥 DIK2。此过程单向，即知道设备鉴别二级密钥 DIK2 和输入参数 1，不能反推参数 2。设备身份鉴别密钥采用 24 字节 TDES 密钥，发散过程举例如下：Step1：对设备序号生成 SHA-256 校验值 32 字节，取前 24 字节作为被加密数据 DATA1。用设备身份鉴别一级密钥 DIK1 对 DATA1 做 TDES-ECB 加密，作为 KEY1。Step2：对发散因子生成 SHA-256 校验值 32 字节，取前 24 字节作为被加密数据 DATA2。KEY1 对 DATA2 做 TDES-ECB 解密，作为该设备身份鉴别二级密钥 DIK2。

[0050] 第一解密单元 14 用于使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文；第二传输密钥分量生成单元 15 用于产生第三随机数作为第二传输密钥分量 TK2；第一传输密钥运算单元 16 用于将 TK1 和 TK2 异或得到传输密钥 TK，计算 TK 的 SHA256 校验值得到 TK_SHA2；第三接收单元 23 用于接收 RKS 服务器 3 发送的密钥密文，所述密钥密文由 TK 加密需要下载的密钥得到；第二解密单元 20 用于使用 TK 解密密钥密文得到密钥明文；密钥下载单元 21 用于将密钥保存至安全模块；第一清除单元 22 用于判断密钥下载是否完成，并当下载完成时清除 AT、TK 及 RKS_WCRT_PK。

[0051] 请参阅图 3，是本发明一实施方式中一种密钥管理装置的结构框图。一种密钥管理装置 30 包括鉴别请求接收单元 31、设备身份鉴别单元 32、鉴别令牌生成单元 33、第一传输密钥生成单元 34、第二加密单元 35、第二发送单元 36、第四接收单元 37、第三解密单元 38、鉴别令牌校验单元 39、第二传输密钥运算单元 40、传输密钥校验单元 41、第三加密单元 42、第三发送单元 43、第二清除单元 44、设备身份鉴别二级密钥生成单元 45、第四解密单元 46。

[0052] 鉴别请求接收单元 31 用于接收至少一个设备端 1 发送的设备序列号 DSN 和设备身份鉴别请求；第二发送单元 36 用于将工作证书公钥 RKS_WCRT_PK 发送至设备端；第四接收单元 37 用于接收设备端发送的发散因子密文，发散因子密文由 RKS_WCRT_PK 加密发散因子得到；第三解密单元 38 用于使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文；设备身份鉴别单元 32 用于以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1；设备身份鉴别二级密钥生成单元 45 用于调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2。

[0053] 鉴别令牌生成单元33用于产生24字节第一随机数作为鉴别令牌AT；第一传输密钥生成单元34用于产生第二随机数作为第一传输密钥分量TK1；第二加密单元35用于使用DIK2加密AT和TK1得到AT_TK1密文；第三发送单元36用于将AT_TK1密文发送至设备端；第四接收单元37用于接收设备端1发送的AT_TK2_TK_SHA2密文，所述AT_TK2_TK_SHA2密文由RKS_WCRT_PK加密AT、第二传输密钥分量TK2和TK_SHA2得到，所述TK_SHA2是传输密钥TK的SHA256校验值，所述TK由TK1和TK2异或得到；第四解密单元46用于使用工作证书私钥RKS_WCRT_SK解密AT_TK2_TK_SHA2密文得到AT、TK2和TK_SHA2明文，所述RKS_WCRT_PK和RKS_WCRT_SK是非对称密钥对；鉴别令牌校验单元39用于判断收到的AT与发送的AT是否相等；第二传输密钥运算单元40用于当所述鉴别令牌校验单元39判定相等时，将TK1和TK2异或得到TK，计算TK的SHA256校验值得到TK_256；传输密钥校验单元41用于判断第二传输密钥运算单元40生成的TK_256与接收到的TK_SHA2是否相等；第三加密单元42用于当所述传输密钥校验单元41判定相等时，使用TK加密需要下载的密钥得到密钥密文；第三发送单元43用于将密钥密文发送至设备端1；第二清除单元44用于清除AT、TK，完成密钥下载流程。

[0054] 请参阅图4，是本发明一实施方式中一种密钥下载方法的流程图。该密钥下载方法运行于所述设备端1中，该方法包括：

[0055] 步骤S101、设备端发送设备序列号DSN和设备身份鉴别请求至RKS服务器；

[0056] 步骤S102、设备端接收RKS服务器发送的工作证书公钥RKS_WCRT_PK；

[0057] 步骤S103、设备端使用根公钥证书RKS_RCRT校验RKS_WCRT_PK的数字签名是否合法，如果合法，则使用RKS_WCRT_PK加密发散因子得到发散因子密文，并将发散因子密文发送至RKS服务器；

[0058] 步骤S104、设备端接收RKS服务器发送的AT_TK1密文，所述AT_TK1密文由设备身份鉴别公钥DIK_PK加密鉴别令牌AT和第一传输密钥分量TK1得到，DIK2通过调用设备身份鉴别二级密钥生成函数根据设备序列号DSN和设备身份鉴别一级密钥DIK1生成；

[0059] 步骤S105、设备端使用DIK2解密AT_TK1密文得到AT和TK1明文；

[0060] 步骤S106、设备端产生第三随机数作为第二传输密钥分量TK2，将TK1和TK2异或得到传输密钥TK，计算TK的SHA256校验值得到TK_SHA2；

[0061] 步骤S107、设备端使用RKS_WCRT_PK加密AT、TK2和TK_SHA2得到AT_TK2_TK_SHA2密文并将AT_TK2_TK_SHA2密文发送至RKS服务器；

[0062] 步骤S108、设备端接收RKS服务器发送的密钥密文，所述密钥密文由TK加密需要下载的密钥得到；

[0063] 步骤S109、设备端使用TK解密密钥密文得到密钥明文，将密钥保存至安全模块；

[0064] 步骤S110、设备端判断密钥下载是否完成，如果下载完成，清除AT、TK及RKS_WCRT_PK。

[0065] 请参阅图5，是本发明一实施方式中一种密钥管理方法的流程图。该密钥管理方法运行于所述RKS服务器3中，该方法包括：

[0066] 步骤S201、RKS服务器接收至少一个设备端发送的设备序列号DSN和设备身份鉴别请求；

[0067] 步骤S202、RKS服务器将工作证书公钥RKS_WCRT_PK发送至设备端；

[0068] 步骤 S203、RKS 服务器接收设备端发送的发散因子密文；

[0069] 步骤 S204、RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文；

[0070] 步骤 S205、RKS 服务器以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1；

[0071] 步骤 S206、RKS 服务器调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2；

[0072] 步骤 S207、RKS 服务器产生 24 字节第一随机数作为鉴别令牌 AT，并产生第二随机数作为第一传输密钥分量 TK1；

[0073] 步骤 S208、RKS 服务器使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文；

[0074] 步骤 S209、RKS 服务器将 AT_TK1 密文发送至设备端；

[0075] 步骤 S210、RKS 服务器接收设备端发送的 AT_TK2_TK_SHA2 密文，所述 AT_TK2_TK_SHA2 密文由 RKS_WCRT_PK 加密 AT、第二传输密钥分量 TK2 和 TK_SHA2 得到，所述 TK_SHA2 是传输密钥 TK 的 SHA256 校验值，所述 TK 由 TK1 和 TK2 异或得到；

[0076] 步骤 S211、RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文，所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对；

[0077] 步骤 S212、RKS 服务器判断收到的 AT 与发送的 AT 是否相等，如果相等，将 TK1 和 TK2 异或得到 TK，计算 TK 的 SHA256 校验值得到 TK_256；

[0078] 步骤 S213、RKS 服务器判断 TK_256 与接收到的 TK_SHA2 是否相等，如果相等，使用 TK 加密需要下载的密钥得到密钥密文；

[0079] 步骤 S214、RKS 服务器将密钥密文发送至设备端；

[0080] 步骤 S215、RKS 服务器清除 AT、TK，完成密钥下载流程。

[0081] 请参阅图 6，是本发明一实施方式中一种密钥下载管理方法的流程图。该密钥下载管理方法运行于所述密钥下载管理系统中，该方法包括：

[0082] 步骤 S301、设备端发送设备序列号 DSN 和设备身份鉴别请求至 RKS 服务器；

[0083] 步骤 S302、RKS 服务器将工作证书公钥 RKS_WCRT_PK 发送至设备端；

[0084] 步骤 S303、设备端使用根公钥证书 RKS_RCRT 校验 RKS_WCRT_PK 的数字签名是否合法，如果合法，执行步骤 S304，否则，执行步骤 S315；

[0085] 步骤 S304、设备端使用 RKS_WCRT_PK 加密发散因子得到发散因子密文并将发散因子密文发送至 RKS 服务器；

[0086] 步骤 S305、RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密发散因子密文得到发散因子明文；

[0087] 步骤 S306、RKS 服务器以 DSN 为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥 DIK1；

[0088] 步骤 S307、RKS 服务器调用设备身份鉴别二级密钥生成函数根据设备序列号 DSN 和 DIK1 生成设备身份鉴别二级密钥 DIK2；

[0089] 步骤 S308、RKS 服务器产生 24 字节第一随机数作为鉴别令牌 AT，并产生第二随机数作为第一传输密钥分量 TK1；

[0090] 步骤 S309、RKS 服务器使用 DIK2 加密 AT 和 TK1 得到 AT_TK1 密文；

[0091] 步骤 S310、RKS 服务器将 AT_TK1 密文发送至设备端；

[0092] 步骤 S311、设备端使用 DIK2 解密 AT_TK1 密文得到 AT 和 TK1 明文；

[0093] 步骤 S312、设备端产生第三随机数作为第二传输密钥分量 TK2，将 TK1 和 TK2 异或得到传输密钥 TK，计算 TK 的 SHA256 校验值得到 TK_SHA2；

[0094] 步骤 S313、设备端使用 RKS_WCRT_PK 加密 AT、TK2 和 TK_SHA2 得到 AT_TK2_TK_SHA2 密文；

[0095] 步骤 S314、设备端将 AT_TK2_TK_SHA2 密文发送至 RKS 服务器；

[0096] 步骤 S315、鉴别 RKS 服务器失败，结束下载流程；

[0097] 步骤 S316、RKS 服务器使用工作证书私钥 RKS_WCRT_SK 解密 AT_TK2_TK_SHA2 密文得到 AT、TK2 和 TK_SHA2 明文，所述 RKS_WCRT_PK 和 RKS_WCRT_SK 是非对称密钥对；

[0098] 步骤 S317、RKS 服务器判断收到的 AT 与发送的 AT 是否相等，如果相等，执行步骤 S318，否则，执行步骤 S320；

[0099] 步骤 S318、RKS 服务器将 TK1 和 TK2 异或得到 TK，计算 TK 的 SHA256 校验值得到 TK_256，判断 TK_256 与接收到的 TK_SHA2 是否相等，如果相等，执行步骤 S319，否则，执行步骤 S320；

[0100] 步骤 S319、使用 TK 加密需要下载的密钥得到密钥密文并将密钥密文发送至设备端；

[0101] 步骤 S320、鉴别设备端失败，结束下载流程；

[0102] 步骤 S321、设备端使用 TK 解密密钥密文得到密钥明文，将密钥保存至安全模块；

[0103] 步骤 S322、设备端判断密钥下载是否完成，如果下载完成，执行步骤 S323，否则，返回步骤 S301；

[0104] 步骤 S323、设备端清除 AT、TK 及 RKS_WCRT_PK；

[0105] 步骤 S324、RKS 服务器清除 AT、TK，完成密钥下载流程。

[0106] 本发明的密钥下载方法、管理方法、下载管理方法及装置和系统，实现设备端从 RKS 服务器远程下载主密钥，避免设备端需要集中下载主密钥后才能布放到商户，设备端出厂后，可以直接布放到部署地点，避免需要将设备端集中到某固定机房下载密钥后再布放到部署地点；

[0107] 利用对称密钥管理技术实现双向合法身份认证，确保 RKS 服务器和设备端双方身份的合法性，设备端通过校验 RKS 服务器的工作证书公钥的数字签名来认证 RKS 服务器的合法性，RKS 服务器生成一个鉴别令牌 AT，用设备端的二级身份鉴别密钥 DK2 加密，将密文发送给设备端，设备端用其保存的二级身份鉴别密钥 DK2 解密，再用工作证书公钥加密后返回给 RKS 服务器，RKS 服务器用其工作证书私钥解密后再对比鉴别令牌 AT 与生成的鉴别令牌 AT 是否一样，一样则表示设备端合法，从而实现双向身份认证；

[0108] 利用随机生成的对称密钥来保护下载的密钥，线路传输的 TMK 由一个临时传输密钥加密，传输密钥由 POS 终端和密钥服务器各自生成一个分量，并采用对方的公钥加密后传输给对方，实现临时传输密钥的同步，从而提高 TMK 传输安全性和效率。

[0109] 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。

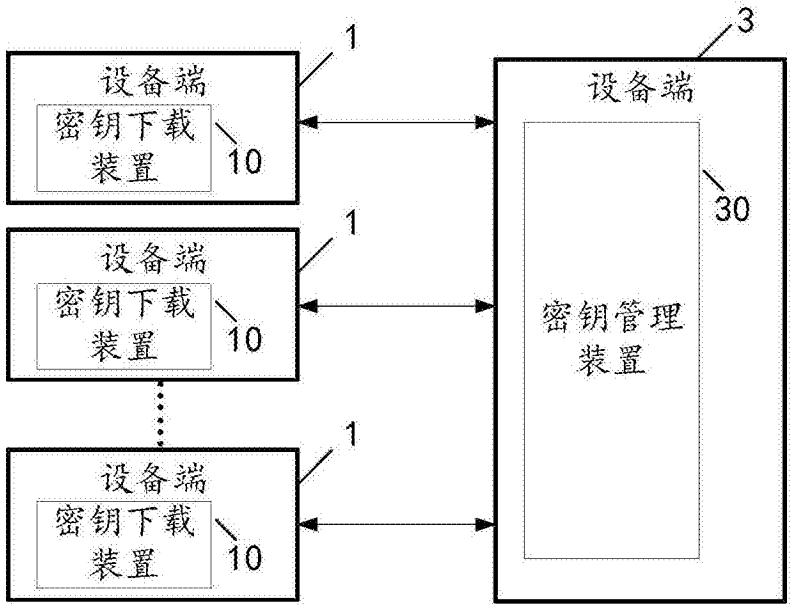

1
设备端
密钥下载装置
10
1
设备端
密钥下载装置
10
1
设备端
密钥下载装置
10
3
设备端
30
密钥管理装置

图 1

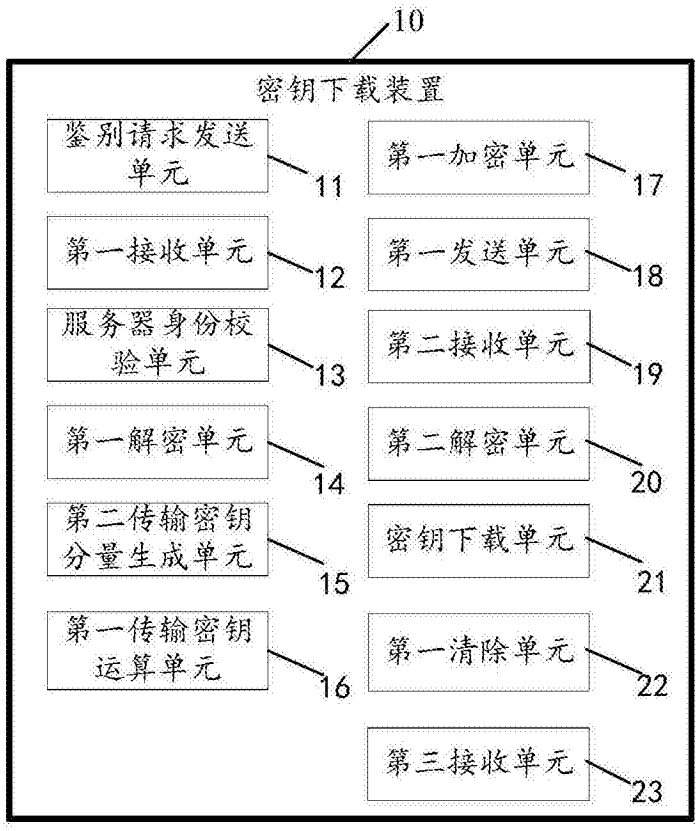

10
密钥下载装置
鉴别请求发送单元
11
第一接收单元
12
服务器身份校验单元
13
第一解密单元
14
第二传输密钥分量生成单元
15
第一传输密钥运算单元
16
第一加密单元
17
第一发送单元
18
第二接收单元
19
第二解密单元
20
密钥下载单元
21
第一清除单元
22
第三接收单元
23

图 2

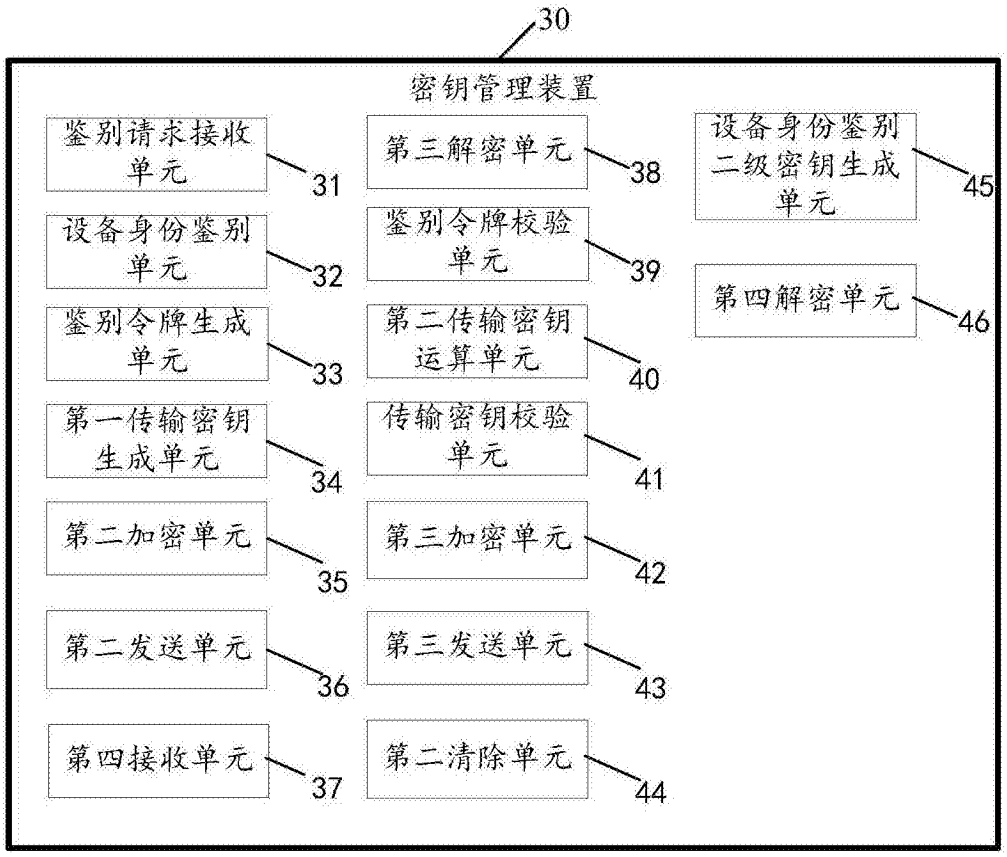

30
密钥管理装置
鉴别请求接收单元
31
设备身份鉴别单元
32
鉴别令牌生成单元
33
第一传输密钥生成单元
34
第二加密单元
35
第二发送单元
36
第四接收单元
37
第三解密单元
38
鉴别令牌校验单元
39
第二传输密钥运算单元
40
传输密钥校验单元
41
第三加密单元
42
第三发送单元
43
第二清除单元
44
设备身份鉴别二级密钥生成单元
45
第四解密单元
46

图 3

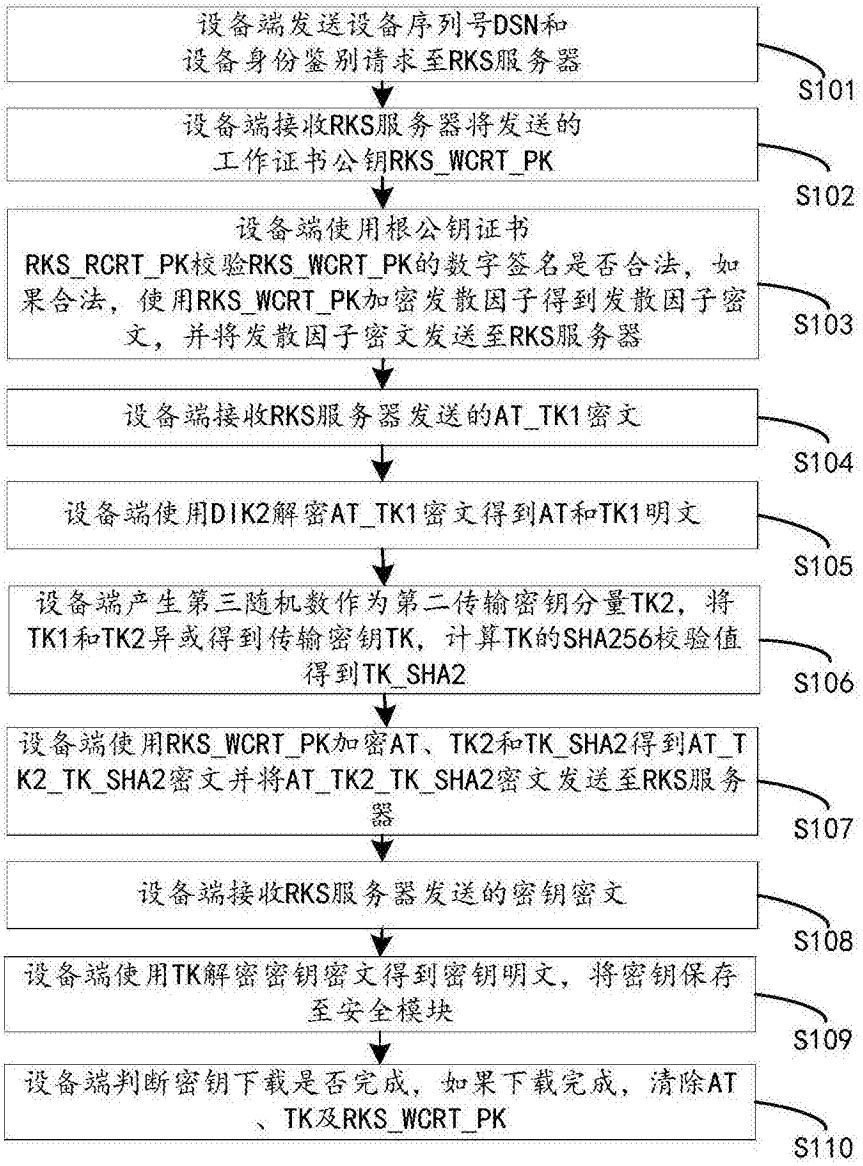

设备端发送设备序列号DSN和
设备身份鉴别请求至RKS服务器
S101
设备端接收RKS服务器将发送的
工作证书公钥RKS_WCRT_PK
S102
设备端使用根公钥证书
RKS_RCRT_PK校验RKS_WCRT_PK的数字签名是否合法，如果合法，使用RKS_WCRT_PK加密发散因子得到发散因子密文，并将发散因子密文发送至RKS服务器
S103
设备端接收RKS服务器发送的AT_TK1密文
S104
设备端使用DIK2解密AT_TK1密文得到AT和TK1明文
S105
设备端产生第三随机数作为第二传输密钥分量TK2，将TK1和TK2异或得到传输密钥TK，计算TK的SHA256校验值得到TK_SHA2
S106
设备端使用RKS_WCRT_PK加密AT、TK2和TK_SHA2得到AT_TK2_TK_SHA2密文并将AT_TK2_TK_SHA2密文发送至RKS服务器
S107
设备端接收RKS服务器发送的密钥密文
S108
设备端使用TK解密密钥密文得到密钥明文，将密钥保存至安全模块
S109
设备端判断密钥下载是否完成，如果下载完成，清除AT、TK及RKS_WCRT_PK
S110

图 4

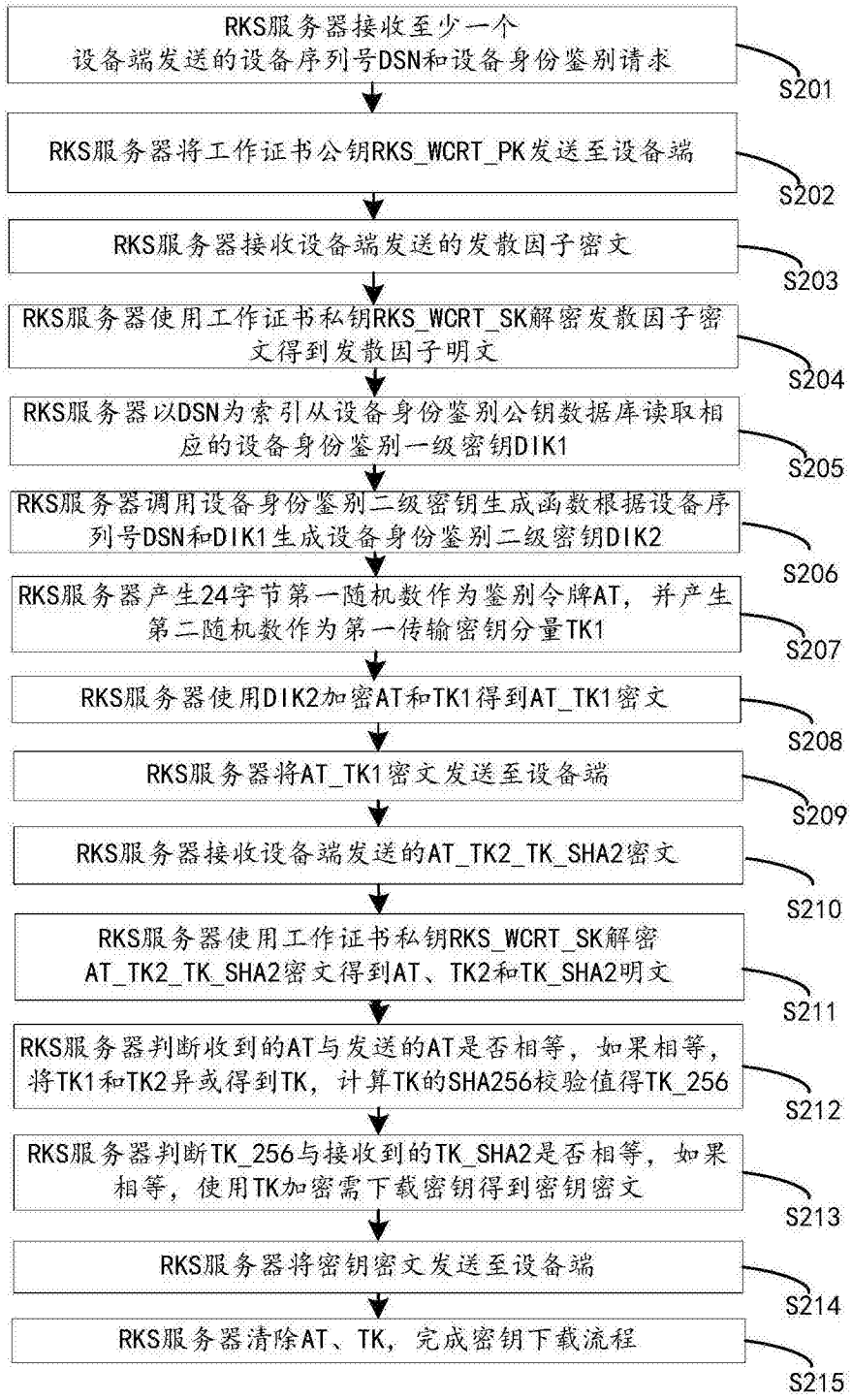

RKS服务器接收至少一个设备端发送的设备序列号DSN和设备身份鉴别请求
S201
RKS服务器将工作证书公钥RKS_WCRT_PK发送至设备端
S202
RKS服务器接收设备端发送的发散因子密文
S203
RKS服务器使用工作证书私钥RKS_WCRT_SK解密发散因子密文得到发散因子明文
S204
RKS服务器以DSN为索引从设备身份鉴别公钥数据库读取相应的设备身份鉴别一级密钥DIK1
S205
RKS服务器调用设备身份鉴别二级密钥生成函数根据设备序列号DSN和DIK1生成设备身份鉴别二级密钥DIK2
S206
RKS服务器产生24字节第一随机数作为鉴别令牌AT，并产生第二随机数作为第一传输密钥分量TK1
S207
RKS服务器使用DIK2加密AT和TK1得到AT_TK1密文
S208
RKS服务器将AT_TK1密文发送至设备端
S209
RKS服务器接收设备端发送的AT_TK2_TK_SHA2密文
S210
RKS服务器使用工作证书私钥RKS_WCRT_SK解密AT_TK2_TK_SHA2密文得到AT、TK2和TK_SHA2明文
S211
RKS服务器判断收到的AT与发送的AT是否相等，如果相等，将TK1和TK2异或得到TK，计算TK的SHA256校验值得TK_256
S212
RKS服务器判断TK_256与接收到的TK_SHA2是否相等，如果相等，使用TK加密需下载密钥得到密钥密文
S213
RKS服务器将密钥密文发送至设备端
S214
RKS服务器清除AT、TK，完成密钥下载流程
S215

图 5

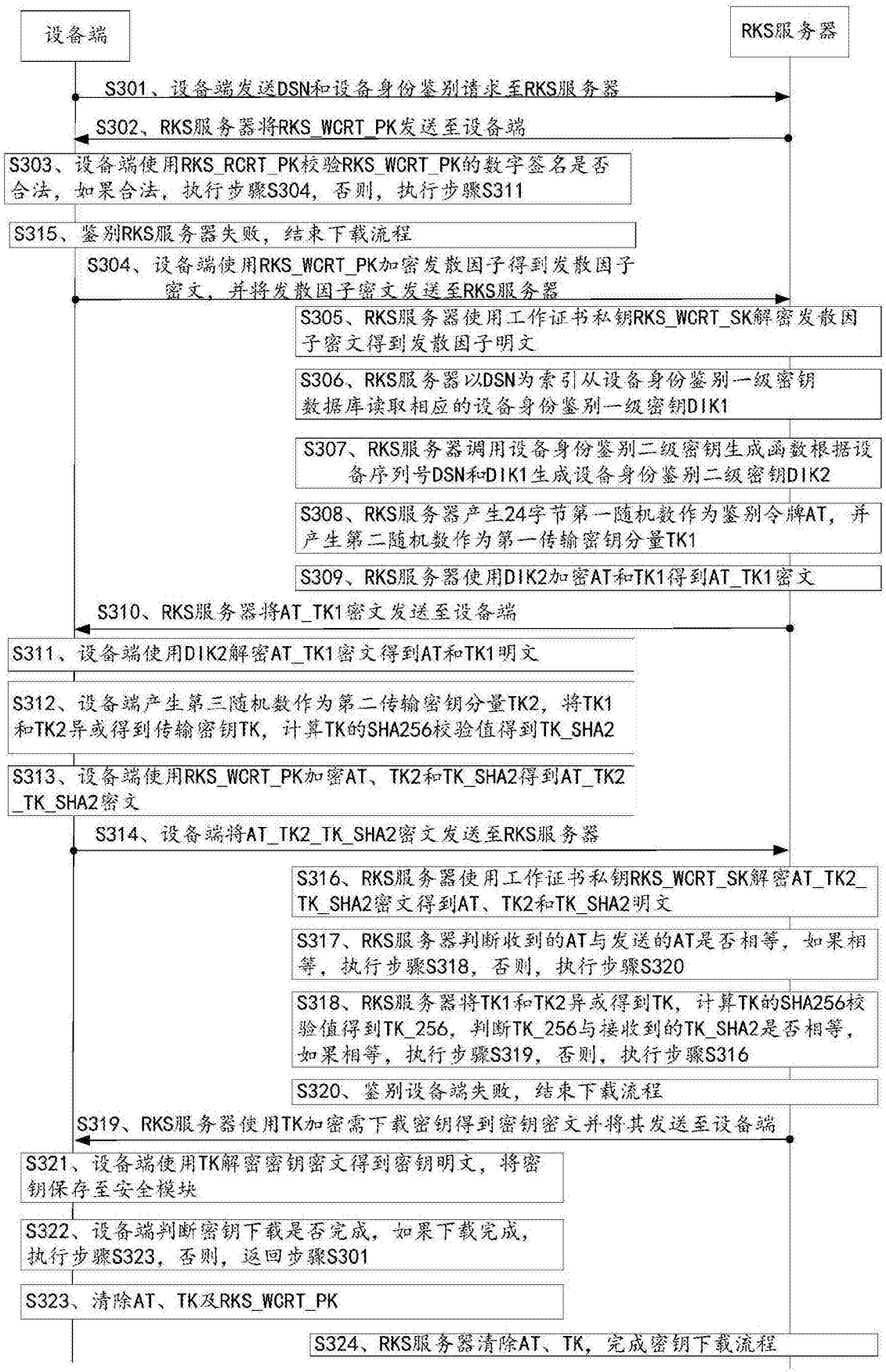

设备端
RKS服务器
S301、设备端发送DSN和设备身份鉴别请求至RKS服务器
S302、RKS服务器将RKS_WCRT_PK发送至设备端
S303、设备端使用RKS_RCRT_PK校验RKS_WCRT_PK的数字签名是否合法，如果合法，执行步骤S304，否则，执行步骤S311
S315、鉴别RKS服务器失败，结束下载流程
S304、设备端使用RKS_WCRT_PK加密发散因子得到发散因子密文，并将发散因子密文发送至RKS服务器
S305、RKS服务器使用工作证书私钥RKS_WCRT_SK解密发散因子密文得到发散因子明文
S306、RKS服务器以DSN为索引从设备身份鉴别一级密钥数据库读取相应的设备身份鉴别一级密钥DIK1
S307、RKS服务器调用设备身份鉴别二级密钥生成函数根据设备序列号DSN和DIK1生成设备身份鉴别二级密钥DIK2
S308、RKS服务器产生24字节第一随机数作为鉴别令牌AT，并产生第二随机数作为第一传输密钥分量TK1
S309、RKS服务器使用DIK2加密AT和TK1得到AT_TK1密文
S310、RKS服务器将AT_TK1密文发送至设备端
S311、设备端使用DIK2解密AT_TK1密文得到AT和TK1明文
S312、设备端产生第三随机数作为第二传输密钥分量TK2，将TK1和TK2异或得到传输密钥TK，计算TK的SHA256校验值得到TK_SHA2
S313、设备端使用RKS_WCRT_PK加密AT、TK2和TK_SHA2得到AT_TK2_TK_SHA2密文
S314、设备端将AT_TK2_TK_SHA2密文发送至RKS服务器
S316、RKS服务器使用工作证书私钥RKS_WCRT_SK解密AT_TK2_TK_SHA2密文得到AT、TK2和TK_SHA2明文
S317、RKS服务器判断收到的AT与发送的AT是否相等，如果相等，执行步骤S318，否则，执行步骤S320
S318、RKS服务器将TK1和TK2异或得到TK，计算TK的SHA256校验值得到TK_256，判断TK_256与接收到的TK_SHA2是否相等，如果相等，执行步骤S319，否则，执行步骤S316
S320、鉴别设备端失败，结束下载流程
S319、RKS服务器使用TK加密需下载密钥得到密钥密文并将其发送至设备端
S321、设备端使用TK解密密钥密文得到密钥明文，将密钥保存至安全模块
S322、设备端判断密钥下载是否完成，如果下载完成，执行步骤S323，否则，返回步骤S301
S323、清除AT、TK及RKS_WCRT_PK
S324、RKS服务器清除AT、TK，完成密钥下载流程

图 6