(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107104795 A
(43)申请公布日 2017.08.29

(21)申请号 201710276856.5

(22)申请日 2017.04.25

(71)申请人 上海汇尔通信息技术有限公司
地址 200000 上海市青浦区华纺路99弄99号厂区内第5幢八层A区849室

(72)发明人 谢芳铭 林培春

(74)专利代理机构 福州市博深专利事务所(普通合伙) 35214
代理人 林志峥

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 29/06(2006.01)
G06Q 20/20(2012.01)
G06Q 20/38(2012.01)

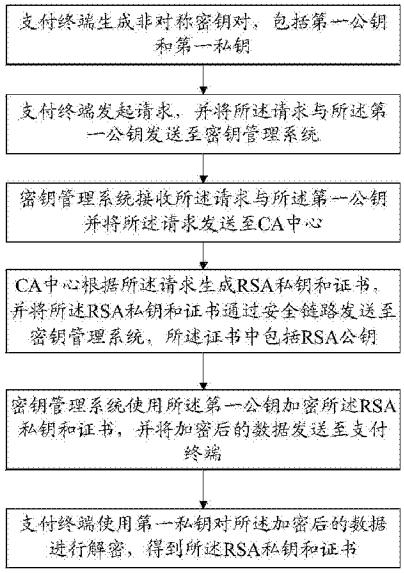
权利要求书2页 说明书8页 附图4页

(54)发明名称

RSA密钥对和证书的注入方法、架构及系统

(57)摘要

本发明公开了一种RSA密钥对和证书的注入方法、架构及系统，方法包括支付终端生成非对称密钥对，包括第一公钥和第一私钥；支付终端发起请求，并将请求与第一公钥发送至密钥管理系统；密钥管理系统将请求发送至CA中心；CA中心根据请求生成RSA私钥和证书，并通过安全链路发送至密钥管理系统，证书中包括RSA公钥；密钥管理系统使用第一公钥加密RSA私钥和证书，并将加密后的数据发送至支付终端；支付终端使用第一私钥解密加密后的数据，得到RSA私钥和证书。本发明有效解决了支付终端自己产生RSA密钥对效率低下的问题，通过借助非对称密钥技术，无需提前与CA中心共享秘密信息，减少了人工操作，节约了成本且保证安全。



CN 107104795 A

1.一种RSA密钥对和证书的注入方法，其特征在于，包括：

支付终端生成非对称密钥对，包括第一公钥和第一私钥；

支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

2.根据权利要求1所述的RSA密钥对和证书的注入方法，其特征在于，所述“支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统”具体为：

支付终端生成请求数据，并将所述请求数据与第一公钥进行打包，得到请求数据包；

使用第一私钥对所述请求数据包进行签名，并将所述请求数据包及其签名发送至密钥管理系统。

3.根据权利要求2所述的RSA密钥对和证书的注入方法，其特征在于，所述“密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心”具体为：

密钥管理系统接收所述请求数据包及其签名，并使用所述第一公钥对所述请求数据包的签名进行合法性验证；

若验证通过，则将所述请求数据发送至CA中心。

4.根据权利要求1所述的RSA密钥对和证书的注入方法，其特征在于，所述“得到所述RSA私钥和证书”之后，进一步包括：

支付终端将所述RSA私钥和证书存储至安全区域中。

5.根据权利要求1-4任一项所述的RSA密钥对和证书的注入方法，其特征在于，所述非对称密钥对为ECC密钥对、SM2密钥对或Rabin密钥对。

6.一种RSA密钥对和证书的注入架构，其特征在于，包括依次通信连接的支付终端、密钥管理系统和CA中心；

所述支付终端用于生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

所述支付终端还用于发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

所述密钥管理系统用于接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

所述CA中心用于根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

所述密钥管理系统还用于使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

所述支付终端还用于使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

7.一种RSA密钥对和证书的注入系统，其特征在于，包括：

第一生成模块，用于支付终端生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

第一发送模块，用于支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管

理系统；

第二发送模块，用于密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

第二生成模块，用于CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

加密模块，用于密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

解密模块，用于支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

RSA密钥对和证书的注入方法、架构及系统

技术领域

[0001] 本发明涉及电子支付领域，尤其涉及一种RSA密钥对和证书的注入方法、架构及系统。

背景技术

[0002] 随着电子支付产业的迅速发展，比如银行卡支付、消费卡支付、行业卡支付以及其它借由网络的电子支付技术，电子支付以其快捷方便的特点，越来越受到人们的欢迎。电子支付系统包括供消费者使用的终端设备以及支付平台和密钥管理等设备。为了确保消费的安全性，消费者通过专用的支付终端输入消费信息(比如帐号密码等)，然后由支付终端传输到支付平台。

[0003] 支付终端，以POS(Point of Sale，POS)为例，保护消费者账户安全的原理如下：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中对敏感信息处理的模块称为密码键盘(PIN PAD)，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，持卡人的个人识别码(Personal Identification Number，PIN)通过密码键盘输入。为防止PIN泄露或者被破解，以保护持卡人的财产安全，整个支付过程中对PIN必须进行加密保护，避免其以明文形式出现。为此，接受PIN输入的POS终端需配备相应的密钥管理体系。

[0004] POS终端中常用的密钥管理体系有两类，不论是分级的密钥体系，主密钥/工作密钥(Master Key/Session Key，MK/SK)还是每笔交易衍生单钥管理方法(Derived Unique Key per Transaction，DUKPT)，都需要将一个初始密钥(Initiail Key，IK)下载到终端，如何下载初始密钥到终端，目前主流的方向是采用远程密钥下载方式，要求支付终端在出厂前预置非对称RSA密钥和证书，终端出厂后使用RSA密钥和证书与KMS系统进行双向认证，通过KMS安全下载终端主密钥(TMK)。考虑到终端的运算性能差异较大，而当前标准的RSA密钥需要达到2048比特的安全强度，RSA密钥对的生成速度一直是低性能终端的瓶颈。那么如何在生产阶段安全高效地注入非对称RSA密钥和证书呢，目前通常有以下几种方式：

[0005] 方式一：将支付终端放到安全房内，物理连接硬件加密机(Hardware Security Module，HSM)注入密钥对和证书；

[0006] 方式二：由支付终端内部生成密钥对，生成证书请求文件导出，请求认证中心(Certification Authority，CA)签发证书。

[0007] 方式三：支付终端和认证中心CA共享一个秘密信息，CA中心生成密钥对和证书之后使用该秘密信息加密后传递给支付终端。

[0008] 但上述方式存在以下缺点：

[0009] 缺点1：证书的注入工作需要在一个高安全管控的安全机房内进行，通过人工方式集中注入，增加了安全房的构建及维护成本。

[0010] 缺点2：终端性能差异较大，且对大多数终端来说，RSA密钥对的生成时间随机性大，最长时间可达到十几分钟左右，极大影响生产效率。

[0011] 缺点3：为了在支付终端和认证中心预置一个共享秘密信息，通常采用人工方式，而且终端数量庞大，要保证该秘密信息每台设备唯一，需要大量的人力资源开销，且对该秘密进行的管控要达到极高的安全级别，否则一旦该秘密信息泄露，终端的私钥也泄露了。

发明内容

[0012] 本发明所要解决的技术问题是：提供一种RSA密钥对和证书的注入方法、架构及系统，可在生产阶段安全高效地注入RSA密钥对和证书。

[0013] 为了解决上述技术问题，本发明采用的技术方案为：一种RSA密钥对和证书的注入方法，包括：

[0014] 支付终端生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

[0015] 支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

[0016] 密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

[0017] CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

[0018] 密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

[0019] 支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

[0020] 本发明还涉及一种RSA密钥对和证书的注入架构，包括依次通信连接的支付终端、密钥管理系统和CA中心；

[0021] 所述支付终端用于生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

[0022] 所述支付终端还用于发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

[0023] 所述密钥管理系统用于接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

[0024] 所述CA中心用于根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

[0025] 所述密钥管理系统还用于使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

[0026] 所述支付终端还用于使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

[0027] 本发明还涉及一种RSA密钥对和证书的注入系统，包括：

[0028] 第一生成模块，用于支付终端生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

[0029] 第一发送模块，用于支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

[0030] 第二发送模块，用于密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

[0031] 第二生成模块，用于CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥

和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

[0032] 加密模块，用于密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

[0033] 解密模块，用于支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

[0034] 本发明的有益效果在于：首先支付终端生成一组非对称密钥对，该非对称密钥对的密钥尺寸和系统参数均小于RSA密钥对，因此即便是对于低性能的支付终端，生成该非对称密钥对的时间和加解密速度也很快；然后支付终端将公钥传输给密钥管理系统，密钥管理系统通过公钥加密要下载的敏感数据，包括RSA密钥对和证书等，即便其他人截获传给支付终端的数据，由于没有私钥也无法正确解密，从而保证了数据的机密性和完整性；同时，支付终端将请求通过密钥管理系统发送给CA中心，由CA中心集中生成RSA密钥对和证书，提高了RSA密钥对和证书的生成速度，从而提高了生产效率。本发明适用于所有类型的支付终端，有效解决了支付终端自己产生RSA密钥对效率低下的问题，通过借助非对称密钥技术，无需提前与CA中心共享秘密信息，减少了人工操作，节约了成本且保证安全。

附图说明

[0035] 图1为本发明一种RSA密钥对和证书的注入方法的流程图；

[0036] 图2为本发明一种RSA密钥对和证书的注入架构的结构示意图；

[0037] 图3为本发明实施例一的方法流程图；

[0038] 图4为本发明实施例二的方法流程图；

[0039] 图5为本发明一种RSA密钥对和证书的注入系统的结构示意图；

[0040] 图6为本发明实施例三的系统结构示意图。

[0041] 标号说明：

[0042] 100、支付终端；200、密钥管理系统；300、CA中心；

[0043] 1、第一生成模块；2、第一发送模块；3、第二发送模块；4、第二生成模块；5、加密模块；6、解密模块；7、存储模块；

[0044] 21、生成单元；22、签名单元；

[0045] 31、验证单元；32、发送单元。

具体实施方式

[0046] 为详细说明本发明的技术内容、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。

[0047] 本发明最关键的构思在于：基于非对称密钥技术，将RSA密钥对和证书安全注入到支付终端。

[0048] 缩略语和关键术语定义：

[0049] LKMS：Local Key Management System本地密钥管理系统；

[0050] CA：Certification Authority，认证中心；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；

[0051] 安全房：具有较高安全级别，用于存放HSM(高安全设备，硬件加密机)、服务器、数据库的房间，该房间需要访问控制，通常需要双重控制认证后才能进去；

[0052] 对称密钥：加密和解密操作必须使用相同的密钥对明文进行运算；对称密钥加密算法主要包括：DES、TDES、AES，IDEA、等；

[0053] 非对称密钥：加密密钥和解密密钥是不同的，其中一个密钥可以公开，另外一个密钥需要保密存储。公开的密钥通常称为公钥(Public Key)，需要秘密存储的密钥称为私钥(Private Key)。常用的非对称密钥算法有：RSA、ECC、国密SM2、Rabin等。

[0054] 请参阅图1，一种RSA密钥对和证书的注入方法，包括：

[0055] 支付终端生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

[0056] 支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

[0057] 密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

[0058] CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

[0059] 密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

[0060] 支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

[0061] 从上述描述可知，本发明的有益效果在于：有效解决了支付终端自己产生RSA密钥对效率低下的问题，通过借助非对称密钥技术，无需提前与CA中心共享秘密信息，减少了人工操作，节约了成本且保证安全。

[0062] 进一步地，所述“支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统”具体为：

[0063] 支付终端生成请求数据，并将所述请求数据与第一公钥进行打包，得到请求数据包；

[0064] 使用第一私钥对所述请求数据包进行签名，并将所述请求数据包及其签名发送至密钥管理系统。

[0065] 进一步地，所述“密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心”具体为：

[0066] 密钥管理系统接收所述请求数据包及其签名，并使用所述第一公钥对所述请求数据包的签名进行合法性验证；

[0067] 若验证通过，则将所述请求数据发送至CA中心。

[0068] 由上述描述可知，通过使用非对称密钥对中的私钥对请求与公钥进行数字签名，密钥管理系统使用公钥验证支付终端的合法性，保证RSA密钥和证书的下载请求是由合法的支付终端发送过来的，进一步保证了安全性。

[0069] 进一步地，所述“得到所述RSA私钥和证书”之后，进一步包括：

[0070] 支付终端将所述RSA私钥和证书存储至安全区域中。

[0071] 由上述描述可知，保证RSA私钥和证书存储的安全性。

[0072] 进一步地，所述非对称密钥对为ECC密钥对、SM2密钥对或Rabin密钥对。

[0073] 由上述描述可知，通过采用密钥尺寸和系统参数均小于RSA密钥对的非对称密钥对，因此即便是对于低性能的支付终端，生成该非对称密钥对的时间和加解密速度也很快。

[0074] 请参照图5，本发明还提出一种RSA密钥对和证书的注入系统，包括：

[0075] 第一生成模块，用于支付终端生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

[0076] 第一发送模块，用于支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

[0077] 第二发送模块，用于密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

[0078] 第二生成模块，用于CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

[0079] 加密模块，用于密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

[0080] 解密模块，用于支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

[0081] 进一步地，所述第一发送模块包括：

[0082] 生成单元，用于支付终端生成请求数据，并将所述请求数据与第一公钥进行打包，得到请求数据包；

[0083] 签名单元，用于使用第一私钥对所述请求数据包进行签名，并将所述请求数据包及其签名发送至密钥管理系统。

[0084] 进一步地，所述第二发送模块包括：

[0085] 验证单元，用于密钥管理系统接收所述请求数据包及其签名，并使用所述第一公钥对所述请求数据包的签名进行合法性验证；

[0086] 发送单元，用于若验证通过，则将所述请求数据发送至CA中心。

[0087] 进一步地，还包括：

[0088] 存储模块7，用于支付终端将所述RSA私钥和证书存储至安全区域中。

[0089] 进一步地，所述非对称密钥对为ECC密钥对、SM2密钥对或Rabin密钥对。

[0090] 实施例一

[0091] 本发明的实施例一为：一种RSA密钥对和证书的注入方法，可远程安全注入RSA密钥对和证书到支付终端；所述方法基于非对称密钥技术，并基于如图2所示的RSA密钥对和证书的注入架构，包括依次通信连接的支付终端100、密钥管理系统200和CA中心300。

[0092] 由于需要从CA中心获取RSA密钥对和证书，因此需部署CA中心，搭建自己的KPI体系，有以下两种可选的做法，一是挂靠一个“可信的第三方CA机构”，成为其附属机构，所谓“第三方CA机构”也即商用CA，比如CFCA(中国金融认证中心)，CTCA(中信安全认证中心)等；二是厂家建立自己的CA中心，涉及到本方案中，CA中心的主要任务是给设备颁发中心，可建立自有CA(in-house CA)。

[0093] 同时，还需建立密钥管理系统(LKMS)和CA中心的安全通信链路，根据建立CA属性的不同，安全通信链路采用不同的方式。以建立自有CA中心为例，CA中心和LKMS部署于同一个安全房中，CA中心位于安全房里间，安全等级最高；LKMS部署于安全房外间，二者通过专用线路和端口进行通信。

[0094] 如图3所示，所述方法包括如下步骤：

[0095] S1:支付终端生成非对称密钥对,所述非对称密钥对包括第一公钥和第一私钥;其中,采用密钥尺寸和系统参数均小于RSA密钥对的密钥对作为所述非对称密钥对,如ECC密钥对、SM2密钥对或Rabin密钥对;优选地,所述非对称密钥对为ECC密钥对。

[0096] S2:支付终端发起请求,并将所述请求与所述第一公钥发送至密钥管理系统;

[0097] S3:密钥管理系统接收所述请求与所述第一公钥,并将所述请求发送至CA中心;第一公钥不是敏感数据,传递过程中只需要保证完整性即可;

[0098] S4:CA中心根据所述请求生成RSA私钥和证书,并将所述RSA私钥和证书通过安全链路发送至密钥管理系统,所述证书中包括RSA公钥;

[0099] S5:密钥管理系统使用所述第一公钥加密所述RSA私钥和证书,并将加密后的数据发送至支付终端;

[0100] S6:支付终端使用第一私钥对所述加密后的数据进行解密,得到所述RSA私钥和证书;

[0101] S7:支付终端将所述RSA私钥和证书存储至安全区域中,即保存到支付终端的安全存储区。

[0102] 通过上述步骤安全注入RSA私钥和证书后,支付终端即可根据该RSA私钥和证书下载初始密钥。

[0103] 本实施例先由支付终端生成一对较简短的非对称密钥对,因此即便是对于低性能的支付终端,生成该非对称密钥对的时间和加解密速度也很快;然后支付终端将公钥传输给密钥管理系统,密钥管理系统通过公钥加密要下载的敏感数据,即便其他人截获传给支付终端的数据,由于没有私钥也无法正确解密,从而保证了数据的机密性和完整性;同时,支付终端将请求通过密钥管理系统发送给CA中心,由CA中心集中生成RSA密钥对和证书,提高了RSA密钥对和证书的生成速度,从而提高了生产效率。

[0104] 本发明适用于所有类型的支付终端,有效解决了支付终端自己产生RSA密钥对效率低下的问题,通过借助非对称密钥技术,无需提前与CA中心共享秘密信息,减少了人工操作,节约了成本且保证安全。

[0105] 实施例二

[0106] 请参照图4,本实施例是实施例一中步骤S2-S3的进一步拓展。

[0107] 所述步骤S2包括:

[0108] S201:支付终端生成请求数据,并将所述请求数据与第一公钥进行打包,得到请求数据包;

[0109] S202:使用第一私钥对所述请求数据包进行签名,并将所述请求数据包及其签名发送至密钥管理系统。

[0110] 所述步骤S3包括:

[0111] S301:密钥管理系统接收所述请求数据包及其签名,并使用所述第一公钥对所述请求数据包的签名进行合法性验证;

[0112] S302:若验证通过,则将所述请求数据发送至CA中心。

[0113] 本实施例通过使用非对称密钥对中的私钥对请求与公钥进行数字签名,密钥管理系统使用公钥验证支付终端的合法性,保证RSA密钥和证书的下载请求是由合法的支付终端发送过来的,进一步保证了安全性。同时,通过采用数字签名的方法,保证传输的数据不

可篡改和可认证性。

[0114] 实施例三

[0115] 请参照图6，本实施例是对应上述实施例的一种RSA密钥对和证书的注入系统，包括：

[0116] 第一生成模块1，用于支付终端生成非对称密钥对，所述非对称密钥对包括第一公钥和第一私钥；

[0117] 第一发送模块2，用于支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统；

[0118] 第二发送模块3，用于密钥管理系统接收所述请求与所述第一公钥，并将所述请求发送至CA中心；

[0119] 第二生成模块4，用于CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥；

[0120] 加密模块5，用于密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端；

[0121] 解密模块6，用于支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书。

[0122] 进一步地，所述第一发送模块2包括：

[0123] 生成单元21，用于支付终端生成请求数据，并将所述请求数据与第一公钥进行打包，得到请求数据包；

[0124] 签名单元22，用于使用第一私钥对所述请求数据包进行签名，并将所述请求数据包及其签名发送至密钥管理系统。

[0125] 进一步地，所述第二发送模块3包括：

[0126] 验证单元31，用于密钥管理系统接收所述请求数据包及其签名，并使用所述第一公钥对所述请求数据包的签名进行合法性验证；

[0127] 发送单元32，用于若验证通过，则将所述请求数据发送至CA中心。

[0128] 进一步地，还包括：

[0129] 存储模块7，用于支付终端将所述RSA私钥和证书存储至安全区域中。

[0130] 进一步地，所述非对称密钥对为ECC密钥对、SM2密钥对或Rabin密钥对。

[0131] 综上所述，本发明提供的一种RSA密钥对和证书的注入方法、架构及系统，首先支付终端生成一组非对称密钥对，该非对称密钥对的密钥尺寸和系统参数均小于RSA密钥对，因此即便是对于低性能的支付终端，生成该非对称密钥对的时间和加解密速度也很快；然后支付终端将公钥传输给密钥管理系统，密钥管理系统通过公钥加密要下载的敏感数据，包括RSA密钥对和证书等，即便其他人截获传给支付终端的数据，由于没有私钥也无法正确解密，从而保证了数据的机密性和完整性；同时，支付终端将请求通过密钥管理系统发送给CA中心，由CA中心集中生成RSA密钥对和证书，提高了RSA密钥对和证书的生成速度，从而提高了生产效率。本发明适用于所有类型的支付终端，有效解决了支付终端自己产生RSA密钥对效率低下的问题，通过借助非对称密钥技术，无需提前与CA中心共享秘密信息，减少了人工操作，节约了成本且保证安全。

[0132] 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同变换，或直接或间接运用在相关的技术领域，均同理包括在本发明的专利保护范围内。

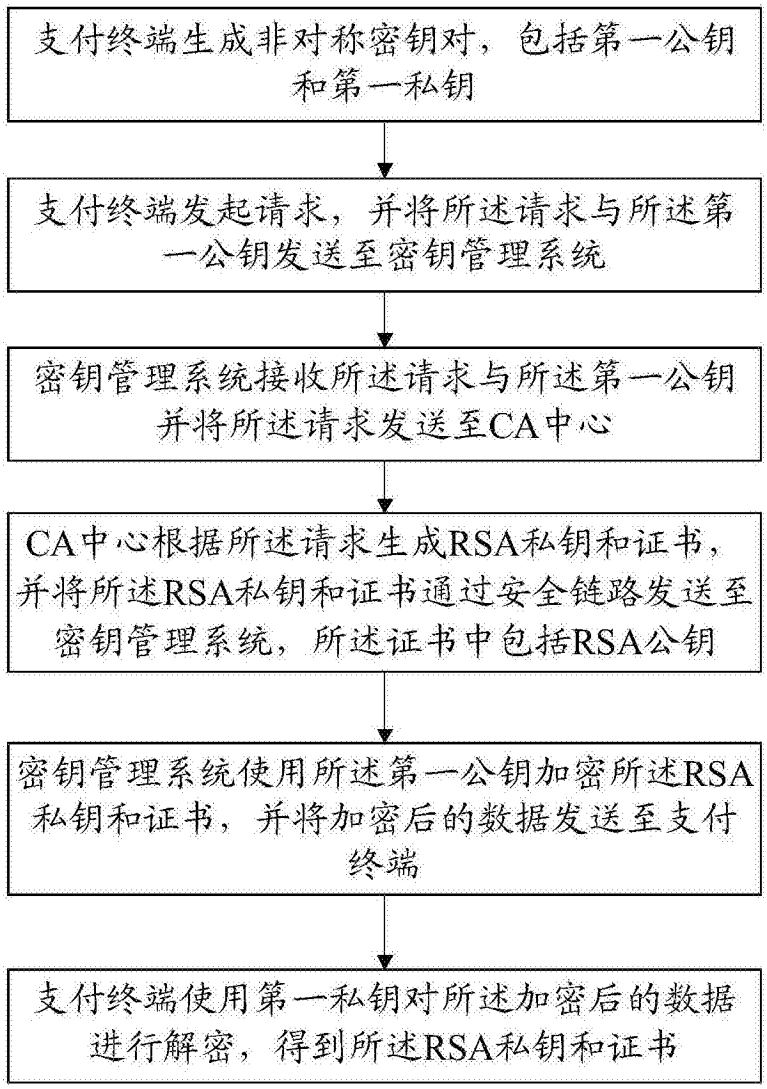

支付终端生成非对称密钥对，包括第一公钥和第一私钥
支付终端发起请求，并将所述请求与所述第一公钥发送至密钥管理系统
密钥管理系统接收所述请求与所述第一公钥并将所述请求发送至CA中心
CA中心根据所述请求生成RSA私钥和证书，并将所述RSA私钥和证书通过安全链路发送至密钥管理系统，所述证书中包括RSA公钥
密钥管理系统使用所述第一公钥加密所述RSA私钥和证书，并将加密后的数据发送至支付终端
支付终端使用第一私钥对所述加密后的数据进行解密，得到所述RSA私钥和证书

图1

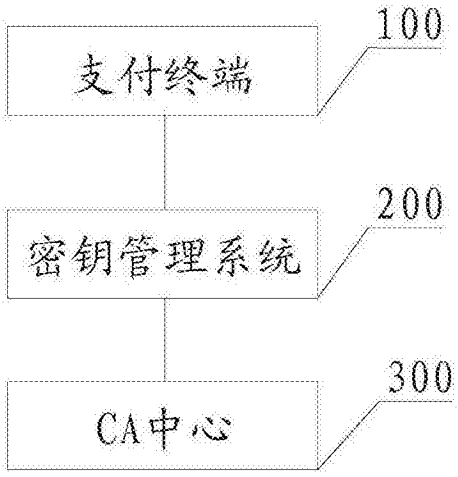

支付终端
100
密钥管理系统
200
CA中心
300

图2

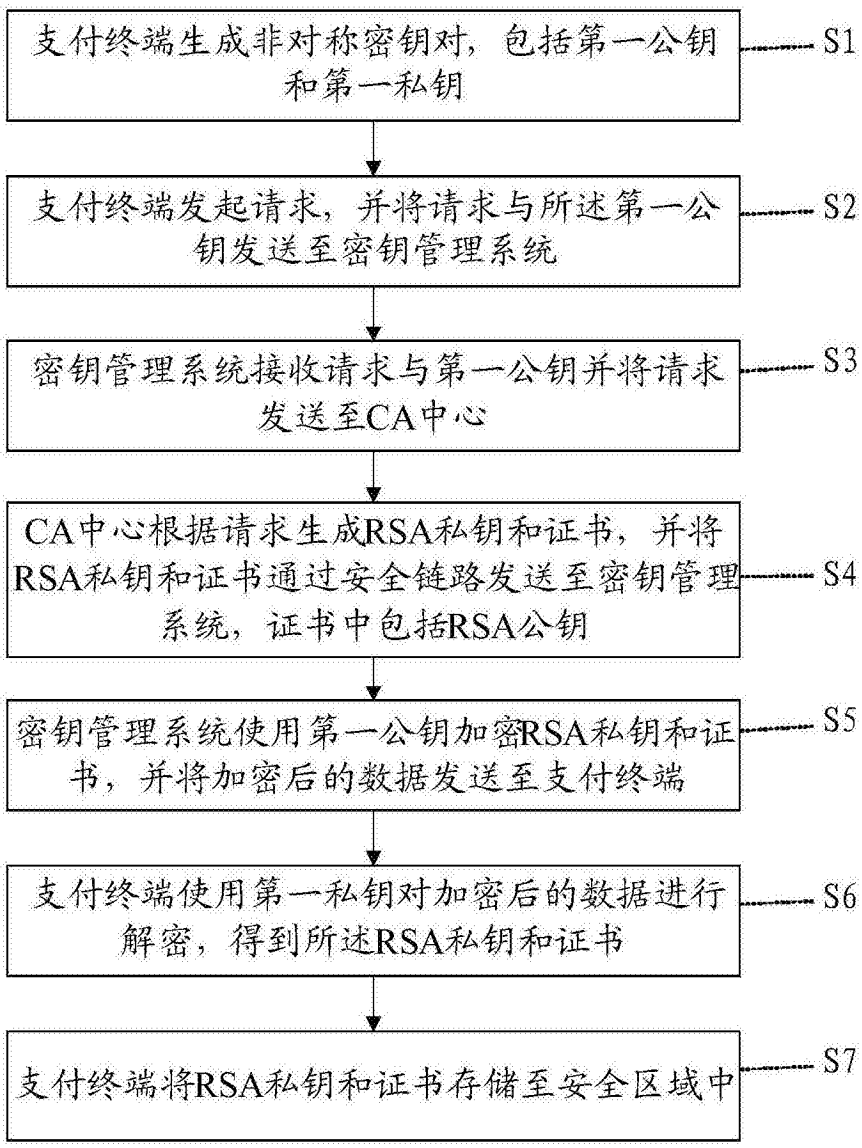

支付终端生成非对称密钥对，包括第一公钥和第一私钥
S1
支付终端发起请求，并将请求与所述第一公钥发送至密钥管理系统
S2
密钥管理系统接收请求与第一公钥并将请求发送至CA中心
S3
CA中心根据请求生成RSA私钥和证书，并将RSA私钥和证书通过安全链路发送至密钥管理系统，证书中包括RSA公钥
S4
密钥管理系统使用第一公钥加密RSA私钥和证书，并将加密后的数据发送至支付终端
S5
支付终端使用第一私钥对加密后的数据进行解密，得到所述RSA私钥和证书
S6
支付终端将RSA私钥和证书存储至安全区域中
S7

图3

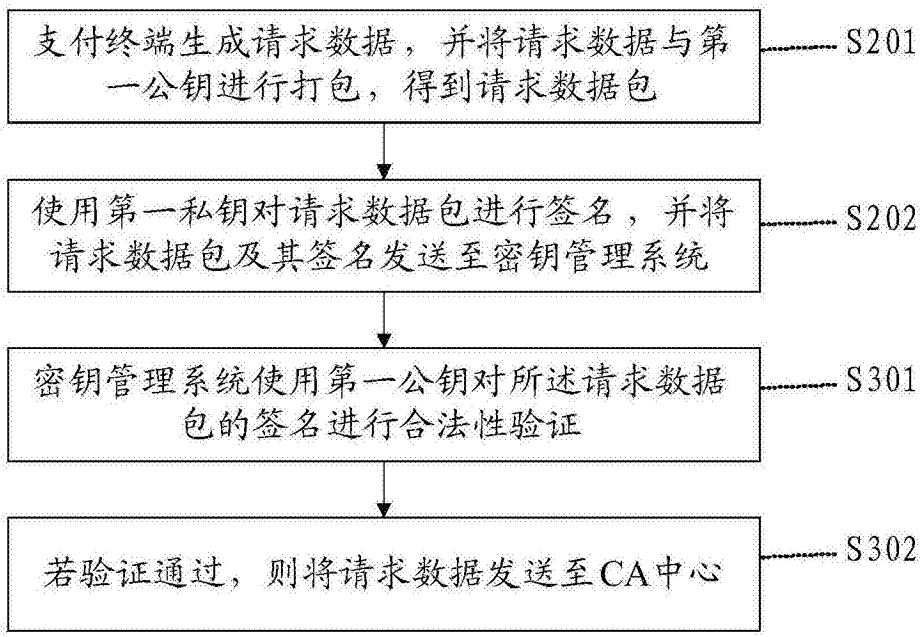

支付终端生成请求数据，并将请求数据与第一公钥进行打包，得到请求数据包
S201
使用第一私钥对请求数据包进行签名，并将请求数据包及其签名发送至密钥管理系统
S202
密钥管理系统使用第一公钥对所述请求数据包的签名进行合法性验证
S301
若验证通过，则将请求数据发送至CA中心
S302

图4


RSA密钥对和证书的注入系统
第一生成模块
1
第一发送模块
2
第二发送模块
3
第二生成模块
4
加密模块
5
解密模块
6

图5

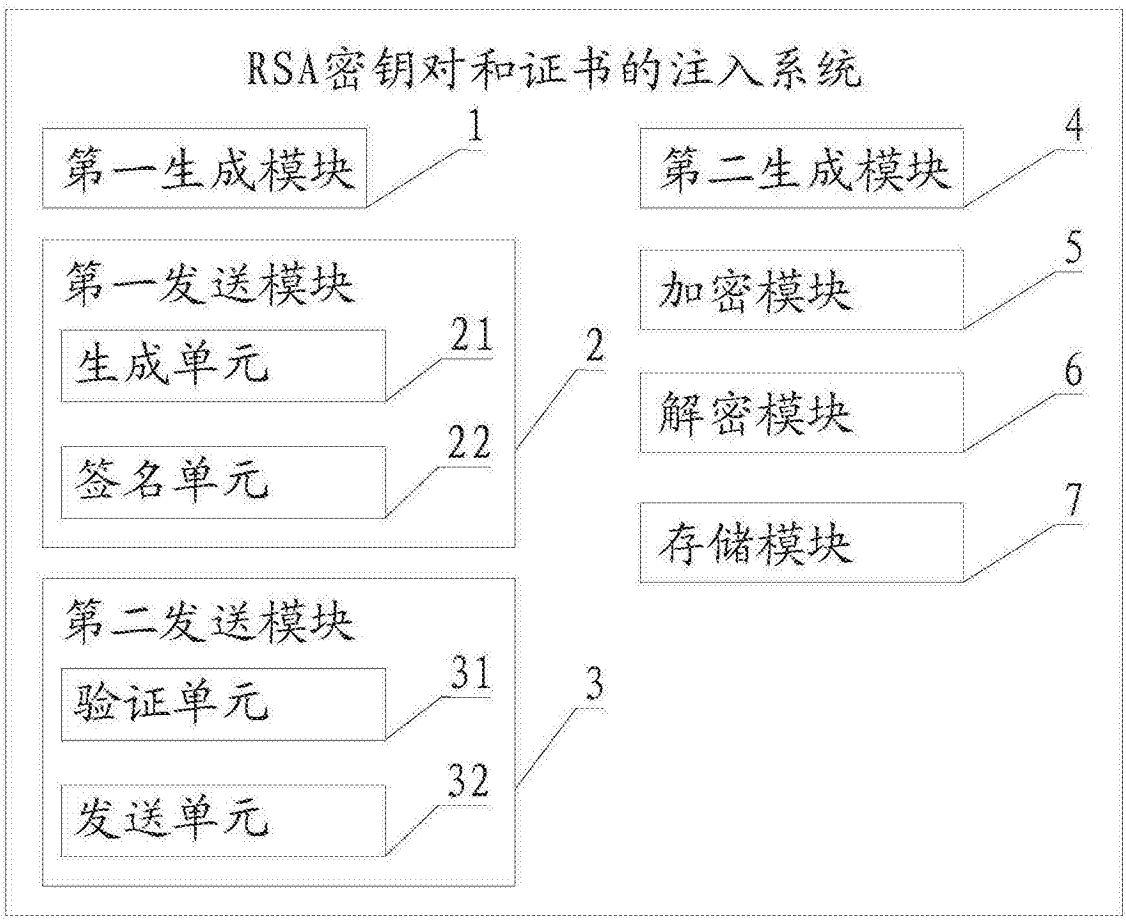

RSA密钥对和证书的注入系统
第一生成模块
1
第二生成模块
4
第一发送模块
生成单元
21
签名单元
22
2
加密模块
5
解密模块
6
存储模块
7
第二发送模块
验证单元
31
发送单元
32
3

图6