(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 112766962 A
(43)申请公布日 2021.05.07

(21)申请号 202110075996.2

(22)申请日 2021.01.20

(71)申请人 中信银行股份有限公司
地址 100020 北京市朝阳区光华路10号1号楼中信大厦20层

(72)发明人 郭燕飞 姚霖 李悝 肖文

(74)专利代理机构 北京市兰台律师事务所 11354
代理人 张峰

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 40/04(2012.01)

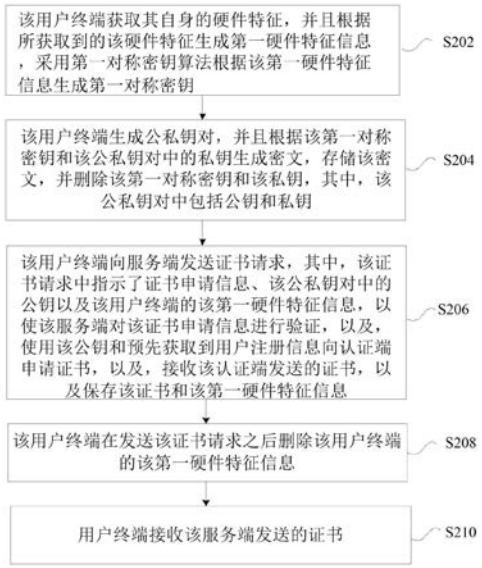
权利要求书3页 说明书13页 附图7页

(54)发明名称

证书的接收、发送方法及交易系统、存储介质、电子装置

(57)摘要

本发明实施例提供了一种证书的接收、发送方法及交易系统、存储介质，电子装置，证书的接收方法包括用户终端并且根据所获取到的硬件特征生成第一硬件特征信息，采用第一对称密钥算法根据第一硬件特征信息生成第一对称密钥；用户终端生成公私钥对，并且根据第一对称密钥和公私钥对中的私钥生成密文，存储密文，并删除第一对称密钥和私钥；用户终端向服务端发送证书请求，以使服务端对证书申请信息进行验证，以及，使用公钥和预先获取到用户注册信息向认证端申请证书，以及，接收认证端发送的证书，以及保存证书和第一硬件特征信息；用户终端在发送证书请求之后删除用户终端的第一硬件特征信息；用户终端接收服务端发送的证书。



CN 112766962 A

1.一种证书的接收方法,其特征在于,应用于用户终端,包括:

所述用户终端获取其自身的硬件特征,并且根据所获取到的所述硬件特征生成第一硬件特征信息,采用第一对称密钥算法根据所述第一硬件特征信息生成第一对称密钥;

所述用户终端生成公私钥对,并且根据所述第一对称密钥和所述公私钥对中的私钥生成密文,存储所述密文,并删除所述第一对称密钥和所述私钥,其中,所述公私钥对中包括公钥和私钥;

所述用户终端向服务端发送证书请求,其中,所述证书请求中指示了证书申请信息、所述公私钥对中的公钥以及所述用户终端的所述第一硬件特征信息,以使所述服务端对所述证书申请信息进行验证,以及,使用所述公钥和预先获取到用户注册信息向认证端申请证书,以及,接收所述认证端发送的证书,以及保存所述证书和所述第一硬件特征信息;

所述用户终端在发送所述证书请求之后删除所述用户终端的所述第一硬件特征信息;

用户终端接收所述服务端发送的证书。

2.根据权利要求1所述的证书的接收方法,其特征在于,在所述用户终端接收所述服务端发送的证书之后,所述方法还包括:

所述用户终端获取待签名的报文;

所述用户终端重新获取其自身的硬件特征,并且根据所获取到的所述硬件特征生成所述第一硬件特征信息,采用所述第一对称密钥算法根据所述第一硬件特征信息生成第二对称密钥;

所述用户终端根据所述第二对称密钥对所述用户终端所存储的所述密文进行解密,得到所述私钥;

所述用户终端根据所述私钥对所述待签名的报文和所述第一硬件特征信息进行签名,得到签名值;

所述用户终端向所述服务端发送签名消息,其中,所述签名消息中指示了用户的身份信息、所述报文以及所述签名值,以使所述服务端使用所述用户所对应的所述公钥、所述服务端所保存的所述第一硬件特征信息以及所述服务端所接收到的所述报文对所述签名消息进行验证。

3.根据权利要求1或2中任意一项所述的证书的接收方法,其特征在于,还包括以下至少之一:

所述第一硬件特征信息为所述硬件特征的哈希值;或者,

所述证书申请信息包括证书序列号和授权码;或者,

所述硬件特征包括以下至少之一:所述用户终端的硬盘序列号,所述用户终端的网卡MAC地址、所述用户终端的CPU序列号、所述用户终端的BIOS编号等。

4.一种证书的发送方法,其特征在于,应用于服务端,包括:

所述服务端接收用户终端发送的证书请求,其中,所述证书请求中指示了证书申请信息、公钥以及所述用户终端的第一硬件特征信息,所述第一硬件特征信息是所述用户终端获取其自身的硬件特征,并且根据所获取到的所述硬件特征生成的,所述公钥是所述用户终端生成的公私钥对中所包括的,所述用户终端还采用第一对称密钥算法根据所述第一硬件特征信息生成了第一对称密钥,并且根据所述第一对称密钥和所述公私钥对中的私钥生成了密文,并存储所述密文,所述用户终端不存储所述第一对称密钥、所述私钥以及所述第

一硬件特征信息,其中,所述公私钥对中包括了公钥和私钥;

所述服务端对所述证书申请信息进行验证,以及,使用所述公钥和预先获取到用户注册信息向认证端申请证书,以及,接收所述认证端发送的证书,以及保存所述证书和所述第一硬件特征信息;

所述服务端向所述用户终端发送所述证书。

5.根据权利要求4所述的证书的发送方法,其特征在于,所述服务端向所述用户终端发送所述证书之后,所述方法还包括:

接收所述用户终端发送的签名消息,其中,所述签名消息中指示了用户的身份信息、报文以及签名值,所述签名值是所述用户终端重新获取其自身的硬件特征,并且根据所获取到的所述硬件特征生成所述第一硬件特征信息,采用所述第一对称密钥算法根据所述第一硬件特征信息生成第二对称密钥,并根据所述第二对称密钥对所述用户终端所存储的所述密文进行解密得到所述私钥,并根据所述私钥对待签名的报文和所述第一硬件特征信息进行签名所得到的;

所述服务端使用所述用户所对应的所述公钥、所述服务端所保存的所述第一硬件特征信息以及所述服务端所接收到的所述报文对所述签名消息进行验证。

6.根据权利要求4或5中任意一项所述的证书的发送方法,其特征在于,还包括以下至少之一:

所述第一硬件特征信息为所述硬件特征的哈希值;或者,

所述证书申请信息包括证书序列号和授权码;或者,

所述硬件特征包括以下至少之一:所述用户终端的硬盘序列号,所述用户终端的网卡MAC地址、所述用户终端的CPU序列号、所述用户终端的BIOS编号等。

7.一种交易系统,其特征在于,包括:

服务端、用户终端,其中,

所述用户终端获取其自身的硬件特征,并且根据所获取到的所述硬件特征生成第一硬件特征信息,采用第一对称密钥算法根据所述第一硬件特征信息生成第一对称密钥;

所述用户终端生成公私钥对,并且根据所述第一对称密钥和所述公私钥对中的私钥生成密文,存储所述密文,并删除所述第一对称密钥和所述私钥,其中,所述公私钥对中包括公钥和私钥;

所述用户终端向服务端发送证书请求,其中,所述证书请求中指示了证书申请信息、所述公私钥对中的公钥以及所述用户终端的所述第一硬件特征信息;

所述用户终端在发送所述证书请求之后删除所述用户终端的所述第一硬件特征信息;

所述服务端对所述证书申请信息进行验证,以及,使用所述公钥和预先获取到用户注册信息向认证端申请证书,以及,接收所述认证端发送的证书,以及保存所述证书和所述第一硬件特征信息;

所述服务端向所述用户终端发送所述证书;

所述用户终端接收所述服务端发送的证书。

8.根据权利要求7所述的交易系统,其特征在于,还包括:

所述用户终端在接收所述服务端发送的证书之后,获取待签名的报文;

所述用户终端重新获取其自身的硬件特征,并且根据所获取到的所述硬件特征生成所

述第一硬件特征信息，采用所述第一对称密钥算法根据所述第一硬件特征信息生成第二对称密钥；

所述用户终端根据所述第二对称密钥对所述用户终端所存储的所述密文进行解密，得到所述私钥；

所述用户终端根据所述私钥对所述待签名的报文和所述第一硬件特征信息进行签名，得到签名值；

所述用户终端向所述服务端发送签名消息，其中，所述签名消息中指示了用户的身份信息、所述报文以及所述签名值；

所述服务端使用所述用户所对应的所述公钥、所述服务端所保存的所述第一硬件特征信息以及所述服务端所接收到的所述报文对所述签名消息进行验证。

9.一种计算机可读的存储介质，其特征在于，所述存储介质中存储有计算机程序，其中，所述计算机程序被设置为运行时实现所述权利要求1至3或者4至6任一项中所述的方法。

10.一种电子装置，包括存储器和处理器，其特征在于，所述存储器中存储有计算机程序，所述处理器被设置为运行所述计算机程序以实现所述权利要求1至3或者4至6任一项中所述的方法。

证书的接收、发送方法及交易系统、存储介质、电子装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种证书的接收、发送方法及交易系统、存储介质，电子装置。

背景技术

[0002] 在银行等金融机构的各种服务(例如交易程序)中，会使用数字证书体系的签名验签机制。数字证书按照存储介质的不同，可以分为硬证书(即介质证书)和软证书(即文件证书)两种，其中，通过硬件安全介质(如硬件)存放的，称为硬证书；以电子文件形式存放的，称为软证书。软证书无需数字证书介质，这就意味着，如果不对软证书的使用进行限制，则软证书可以在任何电脑上进行操作，只需下载导入即可使用，因此，存在被复制和滥用等安全风险。另外，如果存储软证书的电脑被攻破，则软证书还存在被盗用的风险。需要注意的是，一般情况下，软、硬证书中均包含了用户的私钥，如果私钥被复制、盗窃和滥用，会造成非常严重的安全事故。

[0003] 目前，针对文件证书/用户私钥被复制、盗窃和滥用等问题，有一些解决方案，例如在其使用过程中对其使用PIN码(Personal Identification Number)、口令、对称密钥等进行加密存储，这种方式主要存在以下不足：一是PIN码、口令等容易被通过暴力破解等形式获取；二是若将对文件证书进行对称加密的密钥存储在本地，仍然存在被盗用风险；三是对于将文件证书对称加密后存储在本地，对称密钥存储在服务器的方式，需要在每次交易前从服务器获取密钥对文件证书进行解密，从服务器获取密钥等敏感信息需要进行身份认证或权限校验，而这本来就是数字证书要做的事情，而且，密钥传输过程中也容易被攻击者通过窃听等方式获取。

[0004] 可见，相关技术中的私钥容易被复制、窃取、滥用导致了交易过程的不安全性。

发明内容

[0005] 本发明实施例提供了一种证书的接收、发送方法及交易系统、存储介质，电子装置，以至少解决相关技术中私钥容易被复制、窃取、滥用导致了交易过程的不安全性的问题。

[0006] 根据本发明的一个实施例，提供了一种证书的接收方法，应用于用户终端，包括：

[0007] 所述用户终端获取其自身的硬件特征，并且根据所获取到的所述硬件特征生成第一硬件特征信息，采用第一对称密钥算法根据所述第一硬件特征信息生成第一对称密钥；

[0008] 所述用户终端生成公私钥对，并且根据所述第一对称密钥和所述公私钥对中的私钥生成密文，存储所述密文，并删除所述第一对称密钥和所述私钥，其中，所述公私钥对中包括公钥和私钥；

[0009] 所述用户终端向服务端发送证书请求，其中，所述证书请求中指示了证书申请信息、所述公私钥对中的公钥以及所述用户终端的所述第一硬件特征信息，以使所述服务端对所述证书申请信息进行验证，以及，使用所述公钥和预先获取到用户注册信息向认证端

申请证书，以及，接收所述认证端发送的证书，以及保存所述证书和所述第一硬件特征信息；

[0010] 所述用户终端在发送所述证书请求之后删除所述用户终端的所述第一硬件特征信息；

[0011] 用户终端接收所述服务端发送的证书。

[0012] 示例性的，在所述用户终端接收所述服务端发送的证书之后，所述方法还包括：

[0013] 所述用户终端获取待签名的报文；

[0014] 所述用户终端重新获取其自身的硬件特征，并且根据所获取到的所述硬件特征生成所述第一硬件特征信息，采用所述第一对称密钥算法根据所述第一硬件特征信息生成第二对称密钥；

[0015] 所述用户终端根据所述第二对称密钥对所述用户终端所存储的所述密文进行解密，得到所述私钥；

[0016] 所述用户终端根据所述私钥对所述待签名的报文和所述第一硬件特征信息进行签名，得到签名值；

[0017] 所述用户终端向所述服务端发送签名消息，其中，所述签名消息中指示了用户的身份信息、所述报文以及所述签名值，以使所述服务端使用所述用户所对应的所述公钥、所述服务端所保存的所述第一硬件特征信息以及所述服务端所接收到的所述报文对所述签名消息进行验证。

[0018] 示例性的，所述第一硬件特征信息为所述硬件特征的哈希值；

[0019] 示例性的，所述证书申请信息包括证书序列号和授权码；

[0020] 示例性的，所述硬件特征包括以下至少之一：所述用户终端的硬盘序列号，所述用户终端的网卡MAC地址、所述用户终端的CPU序列号、所述用户终端的BIOS编号等。

[0021] 本实施例还提供了一种证书的发送方法，应用于服务端，包括：

[0022] 所述服务端接收用户终端发送的证书请求，其中，所述证书请求中指示了证书申请信息、公钥以及所述用户终端的第一硬件特征信息，所述第一硬件特征信息是所述用户终端获取其自身的硬件特征，并且根据所获取到的所述硬件特征生成的，所述公钥是所述用户终端生成的公私钥对中所包括的，所述用户终端还采用第一对称密钥算法根据所述第一硬件特征信息生成了第一对称密钥，并且根据所述第一对称密钥和所述公私钥对中的私钥生成了密文，并存储所述密文，所述用户终端不存储所述第一对称密钥、所述私钥以及所述第一硬件特征信息，其中，所述公私钥对中包括了公钥和私钥；

[0023] 所述服务端对所述证书申请信息进行验证，以及，使用所述公钥和预先获取到用户注册信息向认证端申请证书，以及，接收所述认证端发送的证书，以及保存所述证书和所述第一硬件特征信息；

[0024] 所述服务端向所述用户终端发送所述证书。

[0025] 在一个示例性的实施方式中，所述服务端向所述用户终端发送所述证书之后，所述方法还包括：

[0026] 接收所述用户终端发送的签名消息，其中，所述签名消息中指示了用户的身份信息、报文以及签名值，所述签名值是所述用户终端重新获取其自身的硬件特征，并且根据所获取到的所述硬件特征生成所述第一硬件特征信息，采用所述第一对称密钥算法根据所述

第一硬件特征信息生成第二对称密钥，并根据所述第二对称密钥对所述用户终端所存储的所述密文进行解密得到所述私钥，并根据所述私钥对待签名的报文和所述第一硬件特征信息进行签名所得到的；

[0027] 所述服务端使用所述用户所对应的所述公钥、所述服务端所保存的所述第一硬件特征信息以及所述服务端所接收到的所述报文对所述签名消息进行验证。

[0028] 在一个示例性的实施方式中，所述第一硬件特征信息为所述硬件特征的哈希值；

[0029] 在一个示例性的实施方式中，所述证书申请信息包括证书序列号和授权码；

[0030] 在一个示例性的实施方式中，所述硬件特征包括以下至少之一：所述用户终端的硬盘序列号，所述用户终端的网卡MAC地址、所述用户终端的CPU序列号、所述用户终端的BIOS编号等。

[0031] 本实施例还提供了一种交易系统，包括：

[0032] 服务端、用户终端，其中，

[0033] 所述用户终端获取其自身的硬件特征，并且根据所获取到的所述硬件特征生成第一硬件特征信息，采用第一对称密钥算法根据所述第一硬件特征信息生成第一对称密钥；

[0034] 所述用户终端生成公私钥对，并且根据所述第一对称密钥和所述公私钥对中的私钥生成密文，存储所述密文，并删除所述第一对称密钥和所述私钥，其中，所述公私钥对中包括公钥和私钥；

[0035] 所述用户终端向服务端发送证书请求，其中，所述证书请求中指示了证书申请信息、所述公私钥对中的公钥以及所述用户终端的所述第一硬件特征信息；

[0036] 所述用户终端在发送所述证书请求之后删除所述用户终端的所述第一硬件特征信息；

[0037] 所述服务端对所述证书申请信息进行验证，以及，使用所述公钥和预先获取到用户注册信息向认证端申请证书，以及，接收所述认证端发送的证书，以及保存所述证书和所述第一硬件特征信息；

[0038] 所述服务端向所述用户终端发送所述证书；

[0039] 所述用户终端接收所述服务端发送的证书。

[0040] 在一个示例性的实施方式中，所述用户终端在接收所述服务端发送的证书之后，获取待签名的报文；

[0041] 所述用户终端重新获取其自身的硬件特征，并且根据所获取到的所述硬件特征生成所述第一硬件特征信息，采用所述第一对称密钥算法根据所述第一硬件特征信息生成第二对称密钥；

[0042] 所述用户终端根据所述第二对称密钥对所述用户终端所存储的所述密文进行解密，得到所述私钥；

[0043] 所述用户终端根据所述私钥对所述待签名的报文和所述第一硬件特征信息进行签名，得到签名值；

[0044] 所述用户终端向所述服务端发送签名消息，其中，所述签名消息中指示了用户的身份信息、所述报文以及所述签名值；

[0045] 所述服务端使用所述用户所对应的所述公钥、所述服务端所保存的所述第一硬件特征信息以及所述服务端所接收到的所述报文对所述签名消息进行验证。

[0046] 根据本发明的又一个实施例，还提供了一种计算机可读的存储介质，所述存储介质中存储有计算机程序，其中，所述计算机程序被设置为运行时实现上述任一项方法实施例中的步骤。

[0047] 根据本发明的又一个实施例，还提供了一种电子装置，包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器被设置为运行所述计算机程序以实现上述任一项方法实施例中的步骤。

[0048] 通过本发明实施例，由于用户终端获取其自身的硬件特征，并且根据所获取到的硬件特征生成第一硬件特征信息，采用第一对称密钥算法根据第一硬件特征信息生成第一对称密钥；用户终端生成公私钥对，并且根据第一对称密钥和公私钥对中的私钥生成密文，存储密文，并删除第一对称密钥和私钥，其中，公私钥对中包括公钥和私钥；用户终端向服务端发送证书请求，其中，证书请求中指示了证书申请信息、公私钥对中的公钥以及用户终端的第一硬件特征信息，以使服务端对证书申请信息进行验证，以及，使用公钥和预先获取到用户注册信息向认证端申请证书，以及，接收认证端发送的证书，以及保存证书和第一硬件特征信息；用户终端在发送证书请求之后删除用户终端的第一硬件特征信息；用户终端接收服务端发送的证书。由于用户终端最终只保存了根据对称密钥和私钥加密所生成的密文，不保存单独的私钥、单独的对称秘钥，并且对称密钥是根据用户终端的硬件特征所生成的，与用户终端是绑定、关联的关系，因此，防止了私钥直接被复制、盗取的情况，即使密文被复制盗取，由于密文是根据用户终端自身的硬件特征所生成的，也很难在其他终端上使用，因此可以保证交易的安全性。

附图说明

[0049] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0050] 图1是本发明实施例的一种证书的接收方法的运算装置的硬件结构框图；

[0051] 图2是根据本发明实施例的证书的接收方法的流程图；

[0052] 图3是根据本发明实施例的证书的发送方法的流程图；

[0053] 图4是根据本发明实施例的交易系统的结构框图；

[0054] 图5是根据本发明示例实施方式的非对称加密算法示意图；

[0055] 图6是根据本发明示例实施方式的PKI体系架构示意图；

[0056] 图7是根据本发明示例实施方式的数字证书的产生流程示意图；

[0057] 图8是根据本发明示例实施方式的系统架构部署结构示意图；

[0058] 图9是根据本发明示例实施方式的数字证书签发流程示意图；

[0059] 图10是根据本发明示例实施方式的签名验签流程示意图；

[0060] 图11是根据本发明示例实施方式的银企直联私有云部署场景示意图；

[0061] 图12是根据本发明示例实施方式的银企直联私有云部署场景的数字证书签发流程示意图；

[0062] 图13是根据本发明示例实施方式的银企直联私有云部署场景的签名验签流程示意图。

具体实施方式

[0063] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0064] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

[0065] 实施例1

[0066] 本申请实施例一所提供的方法实施例可以在移动终端、计算机终端、服务器或者类似的运算装置中执行。以运行在运算装置上为例，图1是本发明实施例的一种证书的接收方法的运算装置的硬件结构框图。如图1所示，运算装置10可以包括一个或多个(图1中仅示出一个)处理器102(处理器102可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)和用于存储数据的存储器104，可选地，上述运算装置还可以包括用于通信功能的传输设备106以及输入输出设备108。本领域普通技术人员可以理解，图1所示的结构仅为示意，其并不对上述运算装置的结构造成限定。例如，运算装置10还可包括比图1中所示更多或者更少的组件，或者具有与图1所示不同的配置。

[0067] 存储器104可用于存储计算机程序，例如，应用软件的软件程序以及模块，如本发明实施例中的证书的接收方法对应的计算机程序，处理器102通过运行存储在存储器104内的计算机程序，从而执行各种功能应用以及数据处理，即实现上述的方法。存储器104可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器104可进一步包括相对于处理器102远程设置的存储器，这些远程存储器可以通过网络连接至运算装置10。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0068] 传输装置106用于经由一个网络接收或者发送数据。上述的网络具体实例可包括运算装置10的通信供应商提供的无线网络、有线网络。在一个实例中，传输装置106包括一个网络适配器(Network Interface Controller，简称为NIC)，其可与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置106可以为射频(Radio Frequency，简称为RF)模块，其用于通过无线方式与互联网进行通讯。

[0069] 在本实施例中提供了一种运行于上述运算装置的证书的接收方法，可以应用于用户终端，图2是根据本发明实施例的证书的接收方法的流程图，如图2所示，该流程包括如下步骤：

[0070] 步骤S202，该用户终端获取其自身的硬件特征，并且根据所获取到的该硬件特征生成第一硬件特征信息，采用第一对称密钥算法根据该第一硬件特征信息生成第一对称密钥；

[0071] 步骤S204，该用户终端生成公私钥对，并且根据该第一对称密钥和该公私钥对中的私钥生成密文，存储该密文，并删除该第一对称密钥和该私钥，其中，该公私钥对中包括公钥和私钥；

[0072] 步骤S206，该用户终端向服务端发送证书请求，其中，该证书请求中指示了证书申请信息、该公私钥对中的公钥以及该用户终端的该第一硬件特征信息，以使该服务端对该证书申请信息进行验证，以及，使用该公钥和预先获取到用户注册信息向认证端申请证书，以及，接收该认证端发送的证书，以及保存该证书和该第一硬件特征信息；

[0073] 步骤S208,该用户终端在发送该证书请求之后删除该用户终端的该第一硬件特征信息;

[0074] 步骤S210,用户终端接收该服务端发送的证书。

[0075] 通过本发明实施例的上述步骤,由于用户终端获取其自身的硬件特征,并且根据所获取到的硬件特征生成第一硬件特征信息,采用第一对称密钥算法根据第一硬件特征信息生成第一对称密钥;用户终端生成公私钥对,并且根据第一对称密钥和公私钥对中的私钥生成密文,存储密文,并删除第一对称密钥和私钥,其中,公私钥对中包括公钥和私钥;用户终端向服务端发送证书请求,其中,证书请求中指示了证书申请信息、公私钥对中的公钥以及用户终端的第一硬件特征信息,以使服务端对证书申请信息进行验证,以及,使用公钥和预先获取到用户注册信息向认证端申请证书,以及,接收认证端发送的证书,以及保存证书和第一硬件特征信息;用户终端在发送证书请求之后删除用户终端的第一硬件特征信息;用户终端接收服务端发送的证书。由于用户终端最终只保存了根据对称密钥和私钥加密所生成的密文,不保存单独的私钥、单独的对称秘钥,并且对称密钥是根据用户终端的硬件特征所生成的,与用户终端是绑定、关联的关系,因此,防止了私钥直接被复制、盗取的情况,即使密文被复制盗取,由于密文是根据用户终端自身的硬件特征所生成的,也很难在其他终端上使用,因此可以保证交易的安全性。

[0076] 示例性的,在该用户终端接收该服务端发送的证书之后,该方法还包括:

[0077] 该用户终端获取待签名的报文;

[0078] 该用户终端重新获取其自身的硬件特征,并且根据所获取到的该硬件特征生成该第一硬件特征信息,采用该第一对称密钥算法根据该第一硬件特征信息生成第二对称密钥;

[0079] 该用户终端根据该第二对称密钥对该用户终端所存储的该密文进行解密,得到该私钥;

[0080] 该用户终端根据该私钥对该待签名的报文和该第一硬件特征信息进行签名,得到签名值;

[0081] 该用户终端向该服务端发送签名消息,其中,该签名消息中指示了用户的身份信息、该报文以及该签名值,以使该服务端使用该用户所对应的该公钥、该服务端所保存的该第一硬件特征信息以及该服务端所接收到的该报文对该签名消息进行验证。

[0082] 示例性的,该第一硬件特征信息为该硬件特征的哈希值;

[0083] 示例性的,该证书申请信息包括证书序列号和授权码;

[0084] 示例性的,该硬件特征包括以下至少之一:该用户终端的硬盘序列号,该用户终端的网卡MAC地址、该用户终端的CPU序列号、该用户终端的BIOS编号等。

[0085] 本实施例还提供了一种证书的发送方法,应用于服务端,图3是根据本发明实施例的证书的发送方法的流程图,如图3所示,包括:

[0086] 步骤S301,该服务端接收用户终端发送的证书请求,其中,该证书请求中指示了证书申请信息、公钥以及该用户终端的第一硬件特征信息,该第一硬件特征信息是该用户终端获取其自身的硬件特征,并且根据所获取到的该硬件特征生成的,该公钥是该用户终端生成的公私钥对中所包括的,该用户终端还采用第一对称密钥算法根据该第一硬件特征信息生成了第一对称密钥,并且根据该第一对称密钥和该公私钥对中的私钥生成了密文,并

存储该密文，该用户终端不存储该第一对称密钥、该私钥以及该第一硬件特征信息，其中，该公私钥对中包括了公钥和私钥；

[0087] 步骤S303，该服务端对该证书申请信息进行验证，以及，使用该公钥和预先获取到用户注册信息向认证端申请证书，以及，接收该认证端发送的证书，以及保存该证书和该第一硬件特征信息；

[0088] 步骤S305，该服务端向该用户终端发送该证书。

[0089] 在一个示例性的实施方式中，该服务端向该用户终端发送该证书之后，该方法还包括：

[0090] 接收该用户终端发送的签名消息，其中，该签名消息中指示了用户的身份信息、报文以及签名值，该签名值是该用户终端重新获取其自身的硬件特征，并且根据所获取到的该硬件特征生成该第一硬件特征信息，采用该第一对称密钥算法根据该第一硬件特征信息生成第二对称密钥，并根据该第二对称密钥对该用户终端所存储的该密文进行解密得到该私钥，并根据该私钥对待签名的报文和该第一硬件特征信息进行签名所得到的；

[0091] 该服务端使用该用户所对应的该公钥、该服务端所保存的该第一硬件特征信息以及该服务端所接收到的该报文对该签名消息进行验证。

[0092] 在一个示例性的实施方式中，该第一硬件特征信息为该硬件特征的哈希值；

[0093] 在一个示例性的实施方式中，该证书申请信息包括证书序列号和授权码；

[0094] 在一个示例性的实施方式中，该硬件特征包括以下至少之一：该用户终端的硬盘序列号，该用户终端的网卡MAC地址、该用户终端的CPU序列号、该用户终端的BIOS编号等。

[0095] 本实施例还提供了一种交易系统，图4是根据本发明实施例的交易系统的结构框图，如图4，所示，包括：

[0096] 服务端42、用户终端44，其中，

[0097] 该用户终端44获取其自身的硬件特征，并且根据所获取到的该硬件特征生成第一硬件特征信息，采用第一对称密钥算法根据该第一硬件特征信息生成第一对称密钥；

[0098] 该用户终端44生成公私钥对，并且根据该第一对称密钥和该公私钥对中的私钥生成密文，存储该密文，并删除该第一对称密钥和该私钥，其中，该公私钥对中包括公钥和私钥；

[0099] 该用户终端44向服务端42发送证书请求，其中，该证书请求中指示了证书申请信息、该公私钥对中的公钥以及该用户终端的该第一硬件特征信息；

[0100] 该用户终端44在发送该证书请求之后删除该用户终端的该第一硬件特征信息；

[0101] 该服务端42对该证书申请信息进行验证，以及，使用该公钥和预先获取到用户注册信息向认证端申请证书，以及，接收该认证端发送的证书，以及保存该证书和该第一硬件特征信息；

[0102] 该服务端42向该用户终端44发送该证书；

[0103] 该用户终端44接收该服务端42发送的证书。

[0104] 通过本发明实施例的上述系统，由于用户终端最终只保存了根据对称密钥和私钥加密所生成的密文，不保存单独的私钥、单独的对称秘钥，并且对称密钥是根据用户终端的硬件特征所生成的，与用户终端是绑定、关联的关系，因此，防止了私钥直接被复制、盗取的情况，即使密文被复制盗取，由于密文是根据用户终端自身的硬件特征所生成的，也很难在

其他终端上使用,因此可以保证交易的安全性。

[0105] 在一个示例性的实施方式中,该用户终端在接收该服务端发送的证书之后,获取待签名的报文;

[0106] 该用户终端重新获取其自身的硬件特征,并且根据所获取到的该硬件特征生成该第一硬件特征信息,采用该第一对称密钥算法根据该第一硬件特征信息生成第二对称密钥;

[0107] 该用户终端根据该第二对称密钥对该用户终端所存储的该密文进行解密,得到该私钥;

[0108] 该用户终端根据该私钥对该待签名的报文和该第一硬件特征信息进行签名,得到签名值;

[0109] 该用户终端向该服务端发送签名消息,其中,该签名消息中指示了用户的身份信息、该报文以及该签名值;

[0110] 该服务端使用该用户所对应的该公钥、该服务端所保存的该第一硬件特征信息以及该服务端所接收到的该报文对该签名消息进行验证。

[0111] 示例实施方式

[0112] 以下结合具体实施场景对本发明实施例进行进一步解释说明。

[0113] 图5是根据本发明示例实施方式的非对称加密算法示意图,如图5所示,非对称加密算法作为计算机通信安全的基石,在保证数据安全方面起着重要的作用。非对称加密算法的加密和解密可以使用不同的规则,只要这两种规则之间存在某种对应关系即可。具体流程可以简单说明如下:例如,Alice根据算法生成两把密钥(公钥和私钥),其中私钥是保密的,公钥是公开的,供要与其通信的其它人使用;B获取Alice公钥,并用它来加密;Alice得到B加密后的信息,用私钥进行解密,完成通信。

[0114] PKI(Public Key Infrastructure,公开秘钥基础设施)是以非对称加密技术为基础,以数据机密性、完整性、身份认证和行为不可抵抗性为安全目的,来实施和提供安全服务的具有普适性的安全基础设施。数字证书是PKI中最重要的、最基本的数据要素,PKI提供的各种服务(机密性、完整性、非否认等等),都要通过证书来实现。

[0115] 图6是根据本发明示例实施方式的PKI体系架构示意图,如图6所示,其中,CA代表CA(Certificate Authority)认证机构,RA(Registration Authority)代表注册机构,终端实体也就是PKI订户,资料库负责发布数字证书和证书撤销列表,PKI用户指使用别人证书的实体,CRL代表证书撤销列表。

[0116] 示例性的,图7是根据本发明示例实施方式的数字证书的产生流程示意图,如图7所示,一个合法数字证书的产生流程如下:

[0117] PKI订户自己产生使用的非对称加密算法的公私钥对(pk,sk),向RA提交信息其基本信息和自己的公钥(即pk),自己保存产生的私钥(即sk);

[0118] RA审核用户提交信息的真实性是否符合相关规定,通过后发送给CA;

[0119] CA使用自己的私钥对相关内容进行数字签名,生成数字证书,发送给资料库;

[0120] 资料库负责发布数字证书;

[0121] 证书发布后,PKI用户可以查询、验证和使用证书。

[0122] 数字证书认证是网上银行系统常用的认证方式,其又可分为软证书和硬证书等不

同形式。由于软证书存在被盗取风险，其安全性不如硬证书高，但目前部分业务系统和应用场景中无法引入硬件证书存储介质等形式，因此仍然沿袭使用软证书进行安全认证的方式。

[0123] 示例性的，利用数字证书进行报文签名的流程如下：

[0124] 用户数字证书发布后，当用户想要向服务器发送交易报文时，就使用自己的私钥调用事先协商好的签名算法对交易报文进行签名，并将报文和报文签名一起发送给服务器；

[0125] 服务器接收到报文数据后，抽取用户身份信息，使用用户的公钥对报文签名进行合法性验证，验证通过则表明报文是此用户发送的合法报文，否则拒绝。

[0126] 数字证书认证是网上银行系统常用的认证方式，其又可分为软证书和硬证书等不同形式。由于软证书存在被盗取风险，其安全性不如硬证书高，但目前部分业务系统和应用场景中无法引入硬件证书存储介质等形式，因此仍然沿袭使用软证书进行安全认证的方式。此种场景下用户的私钥保护就变得尤为关键，为解决现有技术方案中无法同时满足文件证书/用户私钥设备绑定、安全保护和用户私钥隐私性要求的问题，提出本技术方案。使用本方案中的方法可以实现在此场景下软证书和用户私钥的安全保护和设备绑定，满足安全性和监管的要求。

[0127] 图8是根据本发明示例实施方式的系统架构部署结构示意图，如图8所示，整体的系统架构部署情况为：

[0128] 系统整体架构包括了以下部分：

[0129] CA(Certificate Authority)认证机构：负责数字证书签发

[0130] 服务器：包括证书申请模块、报文验签模块、其他功能模块等组成部分。其中，证书申请模块负责接收用户发送的公钥信息，进行数字证书申请；报文验签模块负责对用户发送的报文签名进行合法性验证；其他功能模块除了完成业务相关功能外，还负责在用户注册阶段现场收集用户信息并向用户颁发用于证书申请的授权码。

[0131] 用户终端：用户保存文件证书和用户私钥的终端，其中客户端文件证书的安全保护和设备绑定功能在文件证书安全保护模块中进行实现。

[0132] 用户：使用系统和文件证书的用户。

[0133] 图9是根据本发明示例实施方式的数字证书签发流程示意图，如图9所示，数字证书签发流程如下：

[0134] 首先，对数字证书签发流程符号定义予以说明：

[0135] H()：哈希函数；

[0136] ||：连接符号，a||b＝ab；

[0137] getac()：自定义的硬件特征码获取函数；

[0138] $C＝ENC_K(m)$：对称加密算法，密钥是k，加密的消息是m，输出密文C；

[0139] $M＝DEC_k(c)$：对称解密算法，密钥是k，输入的密文是c，输出明文M；

[0140] Y＝KDF(x)：密钥导出函数，输入x，输出对称密钥Y；

[0141] ID：用户身份唯一标识；

[0142] $m_{sig}＝sig_{kd}(H(m))$：签名算法sig，签名私钥是kd，签名的消息是H(m)，输出的数字签名值是m_{sig}；

[0143] $verify_{kp}(m_{sig},H(m))=0/1$:签名验证函数verify,签名验签的公钥是kp,签名的消息是H(m),签名值是m_{sig},输出0/1,代表验签不通过或通过。

[0144] 以下结合图9和实际应用场景对数字证书签发流程进行进一步说明:

[0145] 用户在营业厅办理签约手续,进行用户信息注册,领取证书申请授权码;

[0146] 用户终端安装文件证书安全保护模块,安装后输入证书申请授权码;

[0147] 用户终端收到证书申请授权码后,使用自定义的硬件特征码获取函数getac()获取本机硬件特征码ac(可包含硬盘序列号,网卡MAC地址、CPU序列号、BIOS编码等任意一种或多种的组合),将特征码的哈希值H(ac)作为密钥导出函数KDF的输入,产生对称密钥k=KDF(H(ac));调用公钥密码算法的公私钥对生成算法,产生公私钥对(kp,kd),用k对kd进行对称加密产生密文$c=ENC_k(kd)$,保存c,删除k、kd,清理内存;

[0148] 之后,用户通过安全信道(如线下等方式),将(证书申请授权码||kp||H(ac))发送给服务器,之后删除H(ac),清理内存;

[0149] 服务器的证书申请模块首先验证证书申请授权码是否是未使用过的合法验证码,验证通过后,使用kp和客户的注册信息向CA机构申请数字证书;

[0150] CA验证相关信息,进行数字证书签发和发布,同时,返回success消息(表示证书签发成功)。

[0151] 服务器保存用户标识ID、用户发送过来的哈希值H(ac)和用户证书,将success消息(表示证书签发成功)发送给用户终端,流程结束。

[0152] 图10是根据本发明示例实施方式的签名验签流程示意图,如图10所示,签名验签流程如下:

[0153] 假设用户身份标识为ID,需要签名的消息为m,用户终端侧保存了用户私钥加密后的密文c;

[0154] 用户终端计算k=KDF(H(getac())),其中,H、getac()为上述签发过程中使用的哈希函数和硬件特征码获取函数,使用密钥k对本机存储的c进行对称算法解密$DEC_K(c)$,获得签名私钥kd。(DEC是解密算法)

[0155] 用户终端使用kd对报文m和H(ac)的哈希值进行签名:$m_{sig}=sig_{kd}(H(m||H(getac())))$,向服务器发送消息$(ID||m||m_{sig})$,删除所有计算中间结果,清理内存;例如清除解密得到的私钥、以及清除签名后得到的签名值;

[0156] 服务器接收到消息后,使用用户身份标识为ID的用户对应的用户证书公钥kp和特征码ac的哈希值H(ac)验证签名$verify_{kp}(m_{sig},H(m||H(ac)))$,通过则处理报文m,不通过返回拒绝reject消息。

[0157] 需要说明的是,在一个示例性的实施方式中,整个过程中用户终端的特征码都是使用特征码提取方法getac()动态获取,不可存储或者预置特征码的值。

[0158] 通过本实施例,在数字证书产生过程中,用户自己产生数字证书对应的公私钥对,以设备特征码等信息作为密钥导出函数的输入,导出对称密钥,并使用此对称密钥对用户私钥进行加密,将设备特征码和公钥发给服务器申请用户证书;通过本实施例,在交易过程中,每次交易前程序自动获取本机设备特征等相关参数作为密钥导出函数的输入,产生对称密钥,从而解密用户私钥;同时,每次签名不仅对交易报文签名,还需对用户特征码的哈希值进行签名。

[0159] 通过上述数字证书产生和签名验签过程中与设备特征码的双重绑定机制实现用户私钥和设备的绑定,保证用户私钥不能被复制和滥用;同时,用户私钥只有用户自己加密保管,服务器端无法获得,并且,每次用户恢复私钥均需要动态计算加密的对称密钥,使用后立即删除和内存清理,且对称密钥的密钥导出函数保密且捆绑在本设备终端的程序中,保证了用户对其私钥隐私性的要求。

[0160] 以下以银行场景为例,进一步解释本发明实施例:

[0161] 用户终端可以通过银企直联模块与银行对接的企业客户系统部署在私有云场景中,有一种场景是:私有云机房硬件机器上不允许插入硬件UKEY,导致目前的UKEY不能满足要求,故无法使用传统的银企直连Ukey硬证书解决方案(如Ukey插在银企直连系统部署的电脑上的情况)。在此场景中,用户明确要求使用文件证书,并且用户私钥只有用户自己知悉,银行侧服务器不能留存;而行业监管标准中又给出了用户文件证书必须与设备绑定、不出设备等监管要求。为同时满足此部分用户的需求及监管、安全的要求,使用了本发明中给出的技术方案。

[0162] 图11是根据本发明示例实施方式的银企直联私有云部署场景示意图,如图11所示,整体方案中主要涉及以下几个系统/子系统:

[0163] CFCA认证机构:根CA,其证书签发和管理系统负责数字证书签发和管理。

[0164] 以及,银行内相关系统;

[0165] 以及,网银系统:银行对公业务公司网银系统。

[0166] 内管系统:公司网银客户签约系统,向CFCA完成数字证书的申请,营业厅柜员、客户经理操作,可通过Ukey形式直接向CFCA申请证书,亦可向软证书申请客户颁发证书申请的两码(证书序列号&授权码);

[0167] 前置机:CFCA部署在银行内的前置机,用户提供证书申请两码(证书序列号&授权码)通过前置机向CFCA进行数字证书申请服务;

[0168] 银企直联系统:部署在客户侧,直联业务发起端系统,负责报文接受和转发,发送前需要根据功能要求执行签名操作。

[0169] 客户和客户ERP系统:客户业务系统,通过银企直联系统调用我行网银接口进行交易。

[0170] 图12是根据本发明示例实施方式的银企直联私有云部署场景的数字证书签发流程示意图,如图12所示,数字证书签发流程包括:

[0171] 银企直联系统预置SSL/TLS证书,默认与前置机和网银之间通过加密专线通道交互;

[0172] 软证书安全保护程序(以下简称“小程序”)作为银企直联系统的一个子功能,在安装之前应对安装程序进行代码混淆、加壳保护,防止逆向;

[0173] 客户在营业厅通过内管系统办理签约手续,进行客户信息注册,领取证书申请的两码(证书序列号和授权码);

[0174] 客户机房的客户终端上安装了银企直联系统,安装后客户输入证书申请的两码(证书序列号和授权码);

[0175] 小程序收到证书申请两码后,使用自定义的硬件特征码获取函数getac()获取本机硬件特征码ac(包含硬盘序列号,网卡MAC地址、CPU序列号等),将特征码的哈希值H(ac)

作为密钥导出函数KDF的输入，产生密钥对称密钥k＝KDF(H(ac))；调用公私钥对生成算法，产生公私钥对(kp,kd)，用k对kd加密产生c＝ENC_k(kd)，保存c，删除k、kd，清理内存；之后，银企直联系统通过SSL加密专线信道，将(证书申请两码||kp||H(ac))发送给前置机，之后删除H(ac)，清理内存；

[0176] 前置机首先验证证书申请授权码是否是未使用过的合法验证码，通过后将两码、kp和客户的注册信息发送给CFCA申请数字证书；

[0177] CFCA验证两码和相关信息，进行数字证书签发，将证书返回给前置机；

[0178] 前置机将数字证书返回给银企直联系统，同时，将用户的唯一身份标识、数字证书和其H(ac)值通过安全通道发送给网银系统，网银系统保存用户的数字证书和此用户对应的H(ac)值。

[0179] 图13是根据本发明示例实施方式的银企直联私有云部署场景的签名验签流程示意图，如图13所示，签名验签流程包括：

[0180] 客户ERP系统向银企直连系统发送需要签名的报文m；

[0181] 银企直连系统中小程序功能计算k＝KDF(H(getac()))，使用密钥k对本机存储的c进行解密DEC_K(c)，获得签名私钥kd。

[0182] 使用kd对报文m和特征码ac的哈希值进行签名：m_{sig}＝sig_{kd}(H(m||H(getac()))，向网银系统发送消息(ID||m||m_{sig})；

[0183] 网银系统收到消息后，使用用户对应的证书公钥kp、本地保存的特征码ac的哈希值H(ac)、接收到的报文m一起验证签名，即$verify_{kp}$(m_{sig},H(m||H(ac))，若验证通过则处理报文m，不通过返回拒绝reject消息。

[0184] 需要说明的是，在一个示例性的实施方式中，整个过程中银企直联系统侧的特征码都是使用特征码提取方法getac()动态获取，不可存储或者预置特征码的值。

[0185] 另外，具体实现中，也可以对客户证书和私钥一起加密保存，签名后将客户证书与签名一起发送，进行后续的验证。

[0186] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0187] 本发明的实施例还提供了一种计算机可读的存储介质，该存储介质中存储有计算机程序，其中，该计算机程序被设置为运行时实现上述任一项方法实施例中的步骤。可选地，本实施例中的具体示例可以参考上述实施例及可选实施方式中所描述的示例，本实施例在此不再赘述。

[0188] 可选地，在本实施例中，上述存储介质可以包括但不限于：U盘、只读存储器(Read-Only Memory，简称为ROM)、随机存取存储器(Random Access Memory，简称为RAM)、移动硬盘、磁碟或者光盘等各种可以存储计算机程序的介质。

[0189] 本发明的实施例还提供了一种电子装置，包括存储器和处理器，该存储器中存储有计算机程序，该处理器被设置为运行计算机程序以实现上述任一项方法实施例中的步

骤。

[0190] 可选地，上述电子装置还可以包括传输设备以及输入输出设备，其中，该传输设备和上述处理器连接，该输入输出设备和上述处理器连接。

[0191] 可选地，本实施例中的具体示例可以参考上述实施例及可选实施方式中所描述的示例，本实施例在此不再赘述。

[0192] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0193] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

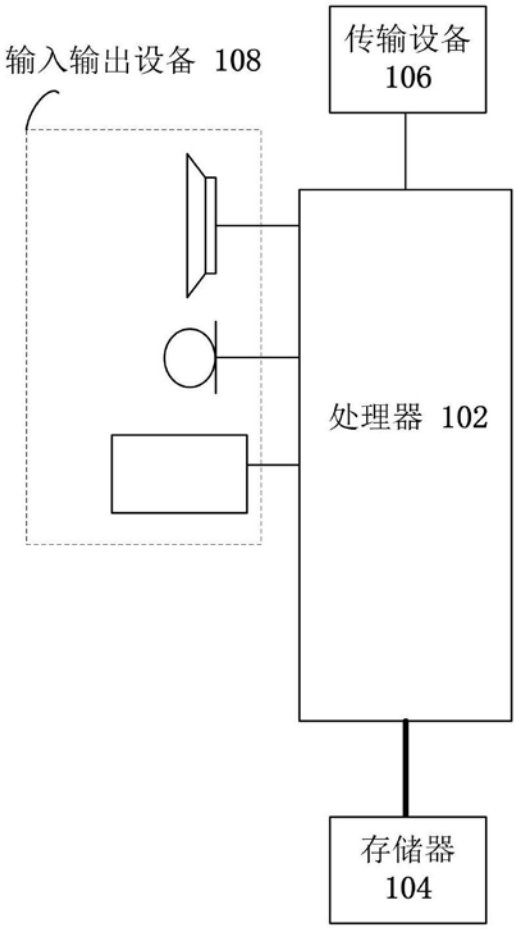


图1

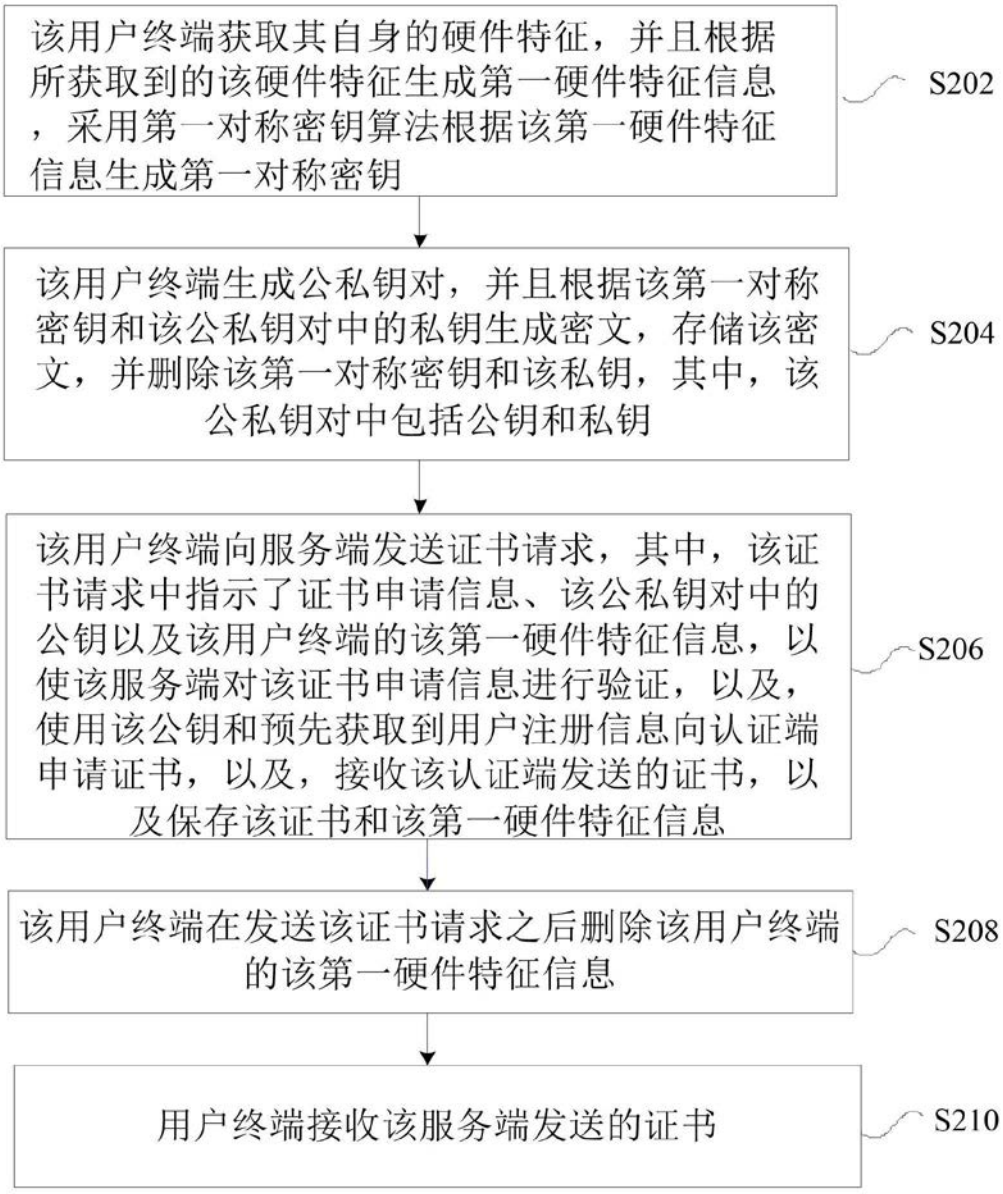

该用户终端获取其自身的硬件特征，并且根据所获取到的该硬件特征生成第一硬件特征信息，采用第一对称密钥算法根据该第一硬件特征信息生成第一对称密钥
S202
该用户终端生成公私钥对，并且根据该第一对称密钥和该公私钥对中的私钥生成密文，存储该密文，并删除该第一对称密钥和该私钥，其中，该公私钥对中包括公钥和私钥
S204
该用户终端向服务端发送证书请求，其中，该证书请求中指示了证书申请信息、该公私钥对中的公钥以及该用户终端的该第一硬件特征信息，以使该服务端对该证书申请信息进行验证，以及，使用该公钥和预先获取到用户注册信息向认证端申请证书，以及，接收该认证端发送的证书，以及保存该证书和该第一硬件特征信息
S206
该用户终端在发送该证书请求之后删除该用户终端的该第一硬件特征信息
S208
用户终端接收该服务端发送的证书
S210

图2

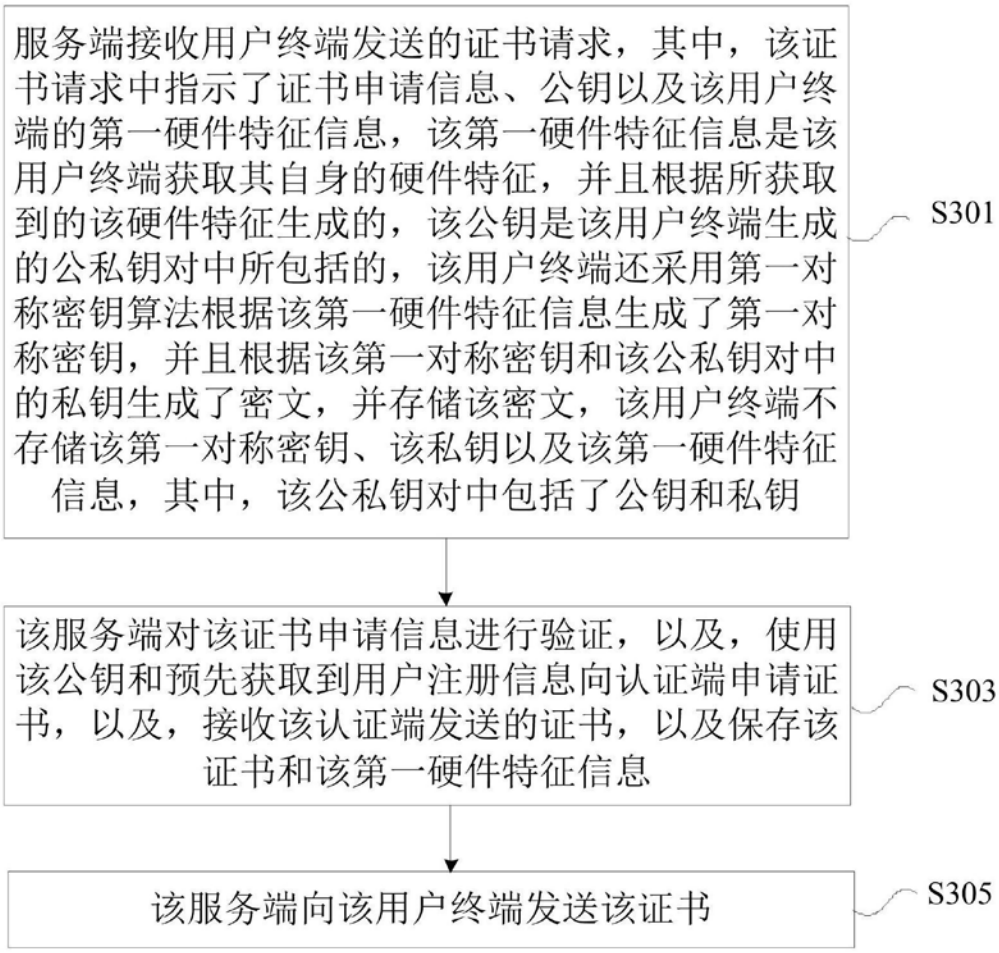

服务端接收用户终端发送的证书请求，其中，该证书请求中指示了证书申请信息、公钥以及该用户终端的第一硬件特征信息，该第一硬件特征信息是该用户终端获取其自身的硬件特征，并且根据所获取到的该硬件特征生成的，该公钥是该用户终端生成的公私钥对中所包括的，该用户终端还采用第一对称密钥算法根据该第一硬件特征信息生成了第一对称密钥，并且根据该第一对称密钥和该公私钥对中的私钥生成了密文，并存储该密文，该用户终端不存储该第一对称密钥、该私钥以及该第一硬件特征信息，其中，该公私钥对中包括了公钥和私钥
S301
该服务端对该证书申请信息进行验证，以及，使用该公钥和预先获取到用户注册信息向认证端申请证书，以及，接收该认证端发送的证书，以及保存该证书和该第一硬件特征信息
S303
该服务端向该用户终端发送该证书
S305

图3

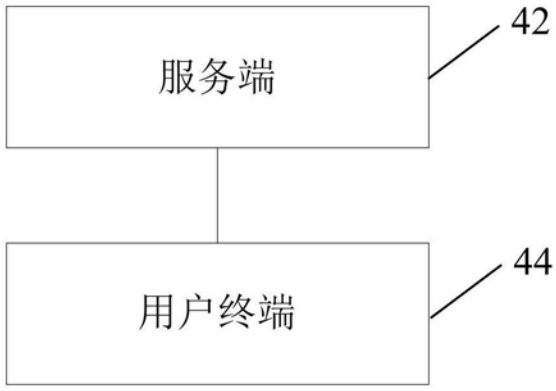

服务端
42
用户终端
44

图4

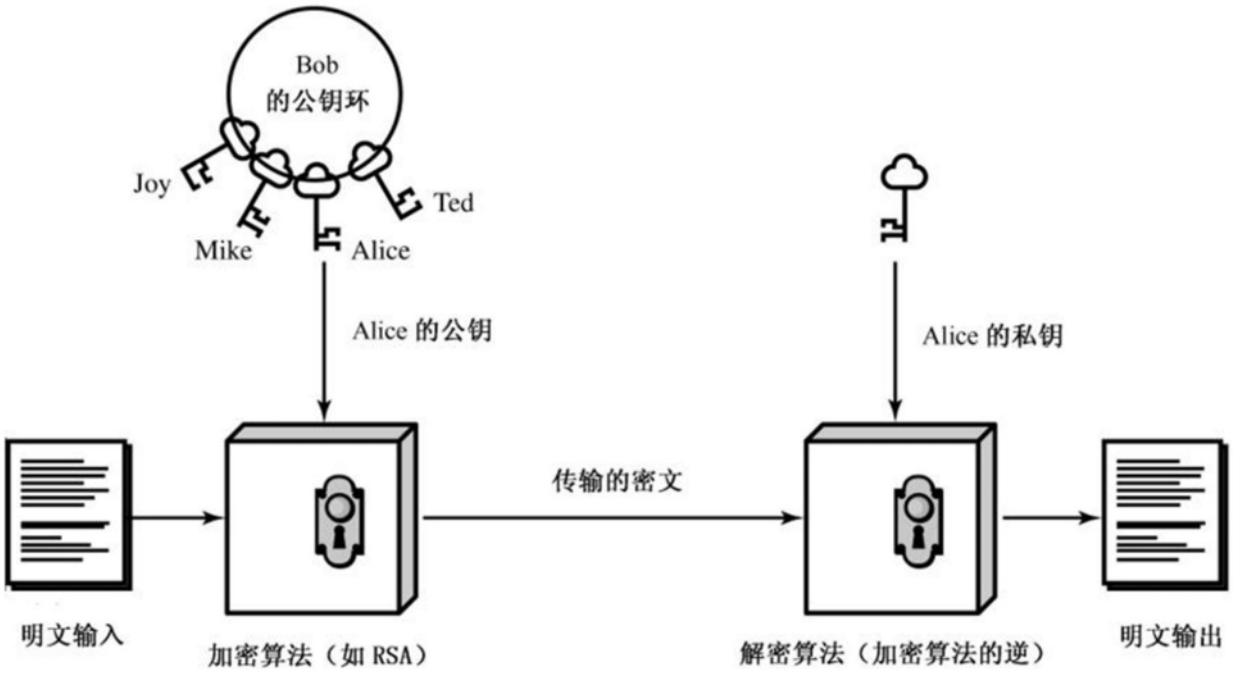

Bob
的公钥环
Joy
Ted
Mike
Alice
Alice 的公钥
Alice 的私钥
传输的密文
明文输入
加密算法（如 RSA）
解密算法（加密算法的逆）
明文输出

图5

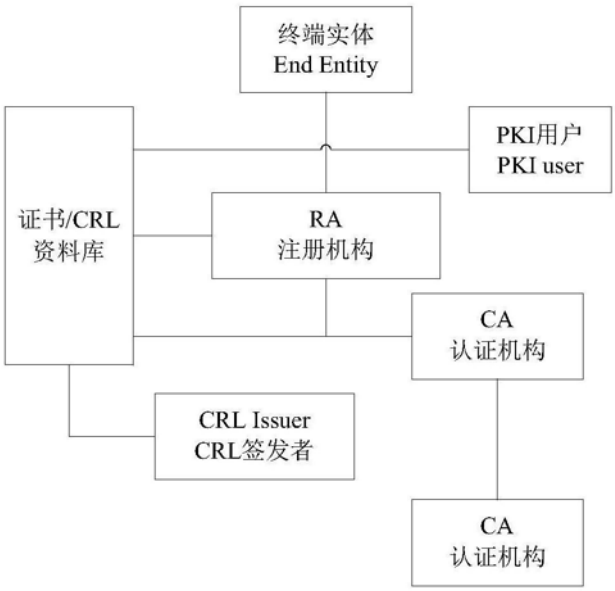

终端实体
End Entity
PKI用户
PKI user
证书/CRL
资料库
RA
注册机构
CA
认证机构
CRL Issuer
CRL签发者
CA
认证机构

图6


PKI订户
1
RA
2
CA
3
证书/CRL资料库
4
5
PKI用户

图7

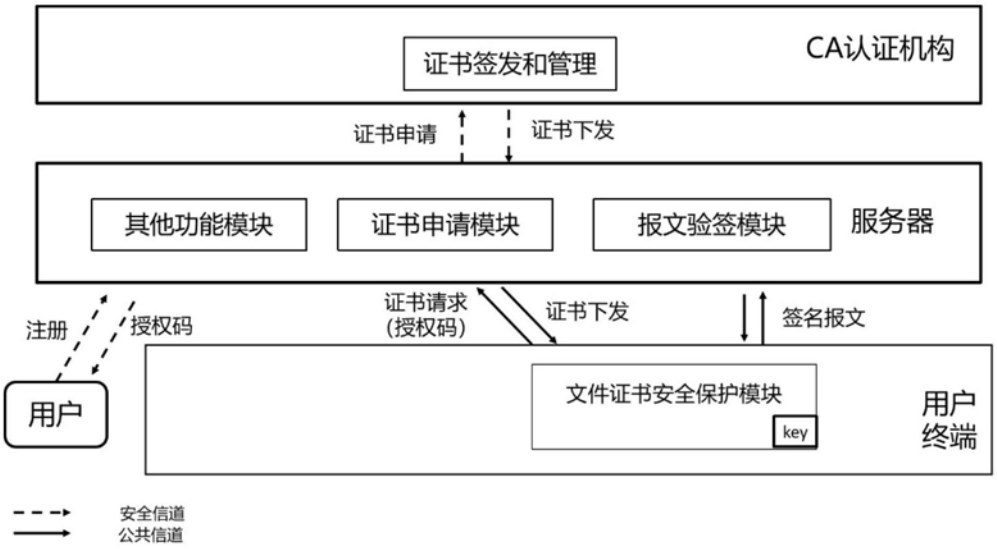

CA认证机构
证书签发和管理
证书申请
证书下发
其他功能模块
证书申请模块
报文验签模块
服务器
注册
授权码
证书请求
(授权码)
证书下发
签名报文
用户
文件证书安全保护模块
key
用户
终端
安全信道
公共信道

图8

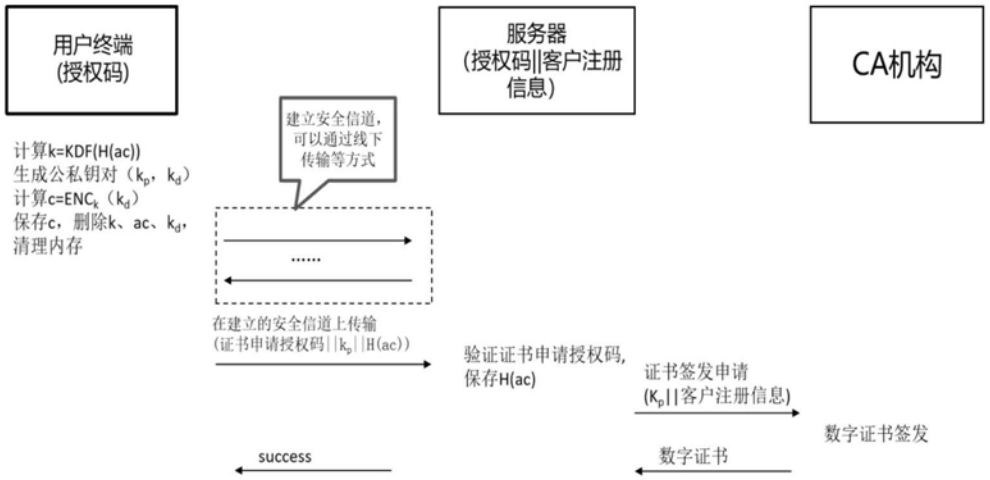

用户终端
(授权码)
服务器
(授权码||客户注册
信息)
CA机构
计算k=KDF(H(ac))
生成公私钥对（k_p，k_d）
计算c=ENC$_k$（k_d）
保存c，删除k、ac、k_d，
清理内存
建立安全信道，
可以通过线下
传输等方式
.....
在建立的安全信道上传输
(证书申请授权码||k_p||H(ac))
验证证书申请授权码，
保存H(ac)
证书签发申请
(K_p||客户注册信息)
数字证书签发
success
数字证书

图9

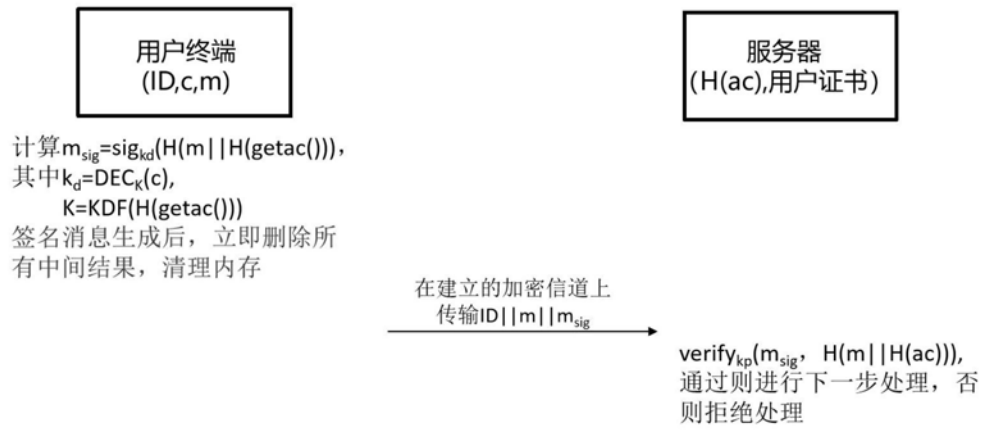

用户终端
(ID,c,m)
服务器
(H(ac),用户证书)
计算$m_{sig}=sig_{kd}(H(m||H(getac())))$,
其中$k_d=DEC_K(c)$,
$K=KDF(H(getac()))$
签名消息生成后，立即删除所有中间结果，清理内存
在建立的加密信道上
传输ID||m||m_{sig}
$verify_{kp}(m_{sig}, H(m||H(ac)))$,
通过则进行下一步处理，否则拒绝处理

图10

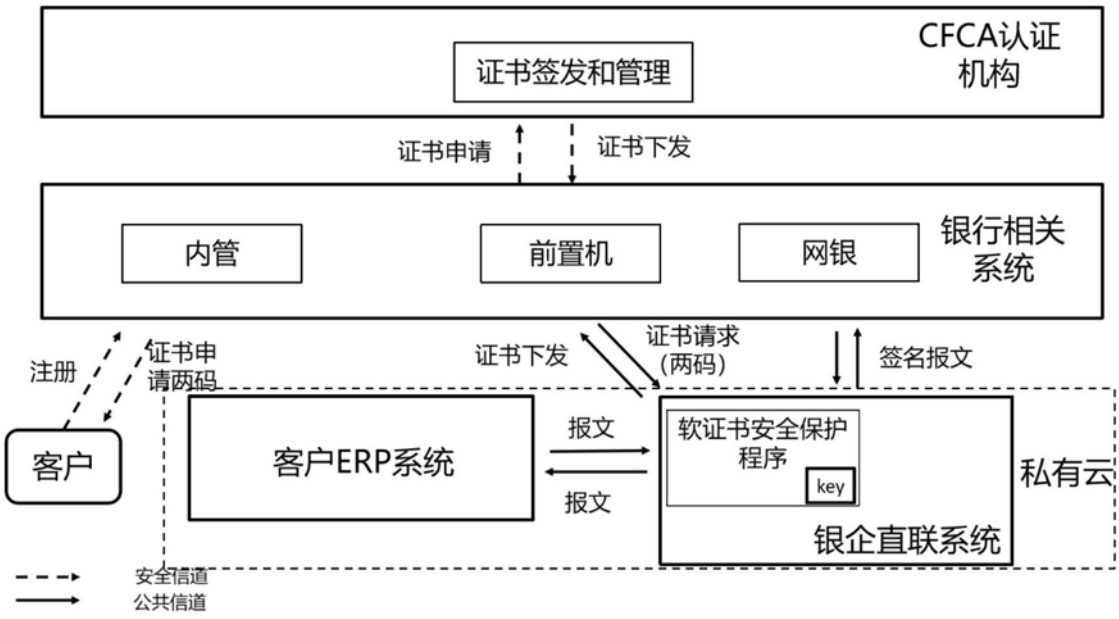

CFCA认证机构
证书签发和管理
证书申请
证书下发
银行相关系统
内管
前置机
网银
注册
证书申请两码
证书下发
证书请求(两码)
签名报文
客户
客户ERP系统
报文
报文
软证书安全保护程序
key
银企直联系统
私有云
安全信道
公共信道

图11

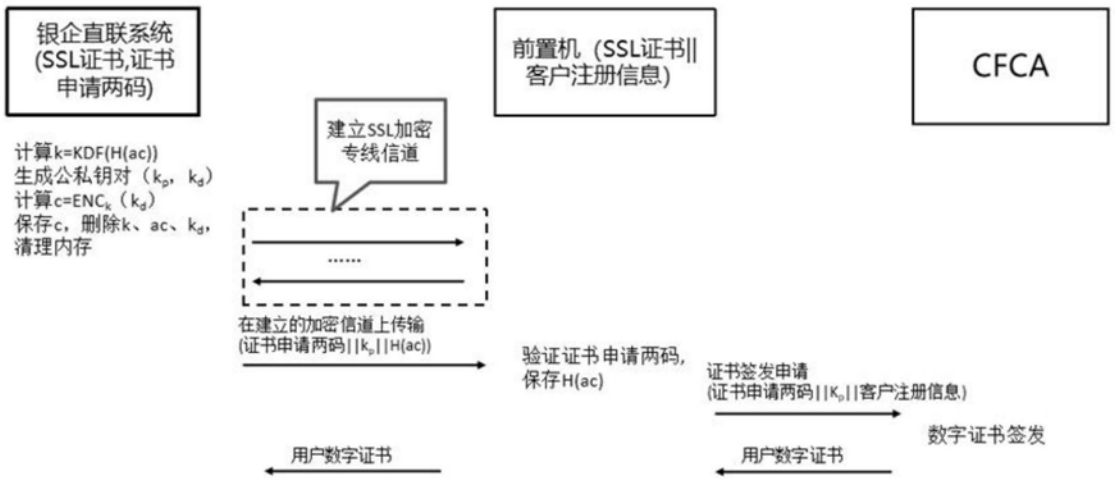

银企直联系统
(SSL证书,证书
申请两码)
前置机（SSL证书||
客户注册信息)
CFCA
建立SSL加密
专线信道
计算k=KDF(H(ac))
生成公私钥对（k_p，k_d）
计算c=ENC_k（k_d）
保存c，删除k、ac、k_d，
清理内存
.....
在建立的加密信道上传输
(证书申请两码||k_p||H(ac))
验证证书申请两码，
保存H(ac)
证书签发申请
(证书申请两码||K_p||客户注册信息)
数字证书签发
用户数字证书
用户数字证书

图12

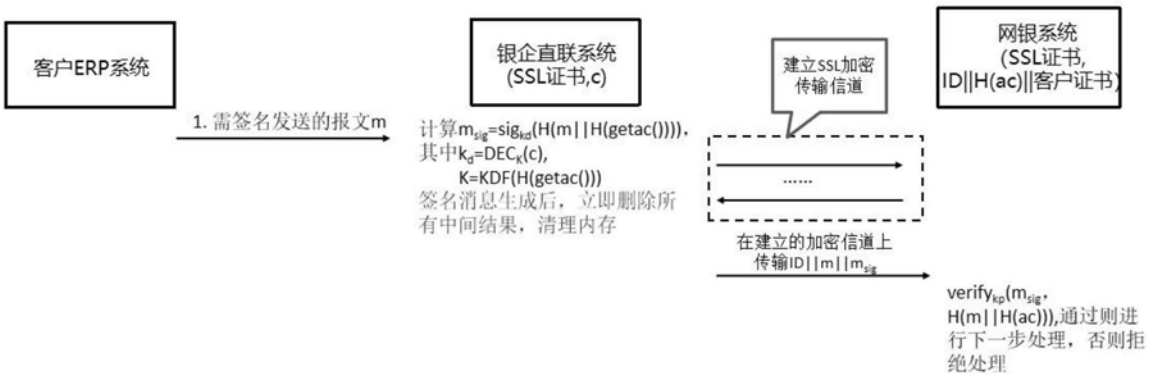

客户ERP系统
1. 需签名发送的报文m
银企直联系统
(SSL证书,c)
计算$m_{sig}=sig_{kd}(H(m||H(getac())))$，
其中$k_d=DEC_K(c)$,
K=KDF(H(getac()))
签名消息生成后，立即删除所
有中间结果，清理内存
建立SSL加密
传输信道
网银系统
(SSL证书,
ID||H(ac)||客户证书)
.....
在建立的加密信道上
传输ID||m||m_{sig}
$verify_{kp}(m_{sig}$，
H(m||H(ac))),通过则进
行下一步处理，否则拒
绝处理

图13