(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 109687959 B
(45)授权公告日 2021.11.12

(21)申请号 201811633995.X

(22)申请日 2018.12.29

(65)同一申请的已公布的文献号
申请公布号 CN 109687959 A

(43)申请公布日 2019.04.26

(73)专利权人 上海唯链信息科技有限公司
地址 200050 上海市长宁区镇宁路465弄161号3号楼229室

(72)发明人 顾建良 马帮亚

(74)专利代理机构 上海德禾翰通律师事务所 31319
代理人 张爱民 李丹丹

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 109064151 A,2018.12.21
CN 105915338 A,2016.08.31
CN 108847937 A,2018.11.20
CN 1925401 A,2007.03.07
CN 106921496 A,2017.07.04
CN 101459505 A,2009.06.17
CN 1801029 A,2006.07.12
CN 101359991 A,2009.02.04
CN 101426190 A,2009.05.06
CN 101557289 A,2009.10.14
CN 108830711 A,2018.11.16
CN 105373955 A,2016.03.02
CN 103580872 A,2014.02.12
CN 102215488 A,2011.10.12
CN 100346249 C,2007.10.31
US 2018097638 A1,2018.04.05

审查员 郑红萍

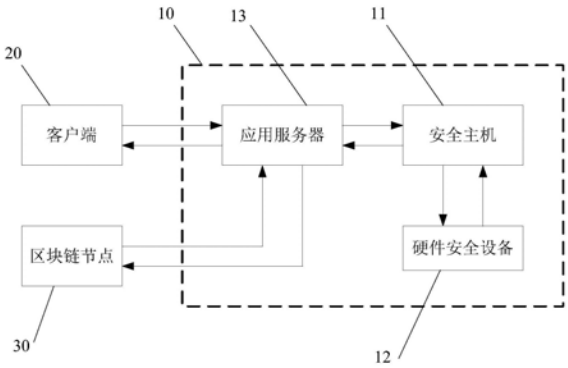
权利要求书4页 说明书7页 附图4页

(54)发明名称

密钥安全管理系统和方法、介质和计算机程序

(57)摘要

本申请公开了一种密钥安全管理系统、方法、计算机可读存储介质和计算机程序。密钥安全管理系统包括安全主机和硬件安全设备，安全主机被配置为接收第一操作请求，对第一操作请求进行验证，并在验证通过时基于第一操作请求生成第二操作请求，所述第一操作请求和所述第二操作请求都包括身份标识，硬件安全设备被配置为从安全主机接收第二操作请求，对第二操作请求进行验证，并且在验证通过时解析第二操作请求的类型，以及基于第二操作请求的类型执行和关联于身份标识的密钥对有关的操作，其中密钥对包括特定于该身份标识的一个公钥和一个私钥。



CN 109687959 B

1.一种密钥安全管理系统,其特征在于,所述密钥安全管理系统包括:

安全主机,其被配置为接收第一操作请求,验证所述第一操作请求包含的发送者的证书和签名的有效性,并在验证通过时基于所述第一操作请求生成第二操作请求,所述第一操作请求和所述第二操作请求都包括用户的身份标识和组织的身份标识,所述用户隶属于所述组织,以及

硬件安全设备,其被配置为从所述安全主机接收所述第二操作请求,验证所述第二操作请求包含的所述安全主机的证书和签名的有效性,并且在验证通过时解析所述第二操作请求的类型,以及基于所述第二操作请求的类型执行和所述用户的密钥对有关的操作,所述用户的密钥对包括一个公钥和一个私钥,所述用户的密钥对由所述硬件安全设备基于所述用户和所述组织的隶属关系按照分层确定性规则从所述组织的主根密钥对派生得到,所述用户的私钥仅在所述硬件安全设备内部使用。

2.根据权利要求1所述的密钥安全管理系统,其特征在于,基于所述第二操作请求的类型执行和所述用户的密钥对有关的操作包括:

响应于所述第二操作请求的类型是请求获取所述用户的公钥,根据所述组织的身份标识确定所述组织的主根密钥对;

基于所述用户的身份标识和分层确定性规则确定所述用户的密钥对生成路径;

基于所述用户的密钥对生成路径和所述组织的主根密钥对派生出所述用户的密钥对;以及

将所述用户的密钥对中的公钥发送给所述安全主机。

3.根据权利要求1所述的密钥安全管理系统,其特征在于,所述第二操作请求还包括所述用户的待签名数据,

其中,基于所述第二操作请求的类型执行和所述用户的密钥对有关的操作包括:

响应于所述第二操作请求的类型是请求对所述待签名数据进行签名,根据所述组织的身份标识确定所述组织的主根密钥对;

基于所述用户的身份标识和分层确定性规则确定所述用户的密钥对生成路径;

基于所述用户的密钥对生成路径和所述组织的主根密钥对派生出所述用户的密钥对;

利用所述用户的密钥对中的私钥对所述待签名数据进行签名以得到签名数据;以及

将所述签名数据发送给所述安全主机。

4.根据权利要求2或3所述的密钥安全管理系统,其特征在于,基于所述用户的身份标识确定所述用户的密钥对生成路径包括:

对所述用户的身份标识和所述组织的身份标识的组合执行哈希运算以得到哈希值;以及

基于所述哈希值和所述分层确定性规则确定所述用户的密钥对生成路径。

5.根据权利要求3所述的密钥安全管理系统,在利用所述用户的密钥对中的私钥对所述待签名数据进行签名之后,所述硬件安全设备还被配置为:

销毁所述用户的密钥对中的私钥。

6.根据权利要求1所述的密钥安全管理系统,其特征在于,所述密钥安全管理系统还包括:

应用服务器,其被配置为根据外部节点的请求生成所述第一操作请求,并且向所述安

全主机发送所述第一操作请求，

其中，所述硬件安全设备与所述安全主机位于同一安全网域内，由所述安全主机作为所述应用服务器访问所述硬件安全设备的网关。

7.根据权利要求1所述的密钥安全管理系统，其中验证所述第一操作请求包含的发送者的证书和签名的有效性包括：

解析所述第一操作请求以获取其中包含的发送者证书和发送者签名，所述发送者证书包含所述发送者的身份标识、所述发送者的允许业务类型列表和所述发送者证书的有效期；

利用所述发送者的公钥对所述发送者签名进行解密，以获取所述第一操作请求所请求的业务类型；

将所述第一操作请求所请求的业务类型与所述发送者证书中所包含的允许业务类型列表进行比较以确定是否允许所述第一操作请求所请求的业务类型；

验证所述发送者证书是否处于所述发送者证书的有效期内；以及

从区块链获取所述发送者证书的状态以验证所述发送者证书的状态。

8.根据权利要求1所述的密钥安全管理系统，其中验证所述第二操作请求包含的所述安全主机的证书和签名的有效性包括：

解析所述第二操作请求以获取其中包含的安全主机证书和安全主机签名，所述安全主机证书包含所述安全主机的身份标识、所述安全主机的允许业务类型列表和所述安全主机证书的有效期；

利用所述安全主机的公钥对所述安全主机签名进行解密，以确定所述第二操作请求是否由所述安全主机签名；

验证所述安全主机证书是否处于所述安全主机证书的有效期内。

9.一种密钥安全管理方法，其特征在于，所述方法包括：

由安全主机接收第一操作请求；

由所述安全主机验证所述第一操作请求包含的发送者的证书和签名的有效性，并在验证通过时基于所述第一操作请求生成第二操作请求，所述第一操作请求和所述第二操作请求都包括用户的身份标识和组织的身份标识，所述用户隶属于所述组织；

由硬件安全设备从所述安全主机接收所述第二操作请求，验证所述第二操作请求包含的所述安全主机的证书和签名的有效性，并在验证通过时解析所述第二操作请求的类型；以及

由所述硬件安全设备基于所述第二操作请求的类型执行和所述用户的密钥对有关的操作，所述用户的密钥对包括一个公钥和一个私钥，所述用户的密钥对由所述硬件安全设备基于所述用户和所述组织的隶属关系按照分层确定性规则从所述组织的主根密钥对派生得到，所述用户的私钥仅在所述硬件安全设备内部使用。

10.根据权利要求9所述的方法，其特征在于，基于所述第二操作请求的类型执行和所述用户的密钥对有关的操作包括：

响应于所述第二操作请求的类型是请求获取所述用户的公钥，根据所述组织的身份标识确定所述组织的主根密钥对；

基于所述用户的身份标识和分层确定性规则确定所述用户的密钥对生成路径；

基于所述用户的密钥对生成路径和所述组织的主根密钥对派生出所述用户的密钥对；以及

将所述用户的密钥对中的公钥发送给所述安全主机。

11.根据权利要求9所述的方法，其特征在于，所述第二操作请求还包括所述用户的待签名数据，

其中，基于所述第二操作请求的类型执行和所述用户的密钥对有关的操作包括：

响应于所述第二操作请求的类型是请求对所述待签名数据进行签名，根据所述组织的身份标识确定所述组织的主根密钥对；

基于所述用户的身份标识和分层确定性规则确定所述用户的密钥对生成路径；

基于所述用户的密钥对生成路径和所述组织的主根密钥对派生出所述用户的密钥对；

利用所述用户的密钥对中的私钥对所述待签名数据进行签名以得到签名数据；以及

将所述签名数据发送给所述安全主机。

12.根据权利要求10或11所述的方法，其特征在于，基于所述用户的身份标识确定所述用户的密钥对生成路径包括：

对所述用户的身份标识和所述组织的身份标识的组合执行哈希运算以得到哈希值；以及

基于所述哈希值和所述分层确定性规则确定所述用户的密钥对生成路径。

13.根据权利要求11所述的方法，其特征在于，在利用所述用户的密钥对中的私钥对所述待签名数据进行签名之后，所述方法包括：

销毁所述用户的密钥对中的私钥。

14.根据权利要求9所述的方法，其中接收第一操作请求包括：

由所述安全主机从应用服务器接收所述第一操作请求，其中，所述硬件安全设备与所述安全主机位于同一安全网域内，由所述安全主机作为所述应用服务器访问所述硬件安全设备的网关。

15.根据权利要求9所述的方法，其中验证所述第一操作请求包含的发送者的证书和签名的有效性包括：

解析所述第一操作请求以获取其中包含的发送者证书和发送者签名，所述发送者证书包含所述发送者的身份标识、所述发送者的允许业务类型列表和所述发送者证书的有效期；

利用所述发送者的公钥对所述发送者签名进行解密，以获取所述第一操作请求所请求的业务类型；

将所述第一操作请求所请求的业务类型与所述发送者证书中所包含的允许业务类型列表进行比较以确定是否允许所述第一操作请求所请求的业务类型；

验证所述发送者证书是否处于所述发送者证书的有效期内；以及

从区块链获取所述发送者证书的状态以验证所述发送者证书的状态。

16.根据权利要求9所述的方法，其中验证所述第二操作请求包含的所述安全主机的证书和签名的有效性包括：

解析所述第二操作请求以获取其中包含的安全主机证书和安全主机签名，所述安全主机证书包含所述安全主机的身份标识、所述安全主机的允许业务类型列表和所述安全主机

证书的有效期;

利用所述安全主机的公钥对所述安全主机签名进行解密,以确定所述第二操作请求是否由所述安全主机签名;以及

验证所述安全主机证书是否处于所述安全主机证书的有效期内。

17.一种非易失性计算机可读存储介质,其上存储有机器可执行指令,所述机器可执行指令在被计算机运行时,执行如权利要求9-16中任一项所述的方法。

密钥安全管理系统和方法、介质和计算机程序

技术领域

[0001] 本申请涉及密钥管理领域，特别涉及一种密钥安全管理系统和方法、一种非易失性存储介质和一种计算机程序。

背景技术

[0002] 随着电子商务的快速发展，交易安全问题日益受到重视。交易过程涉及到使用密钥对数据进行加密、解密和签名等过程，因此，密钥的管理安全程度的高低决定了交易过程的安全程度。密钥的管理通常包括密钥的生成、使用和销毁等方面。

[0003] 现行的加密算法可以分为对称加密算法和非对称加密算法两大类。在对称加密体制中，数据加密和解密使用相同的密钥。而在非对称加密体制中，数据的加密和解密使用不同的两个密钥，这两个密钥相互依存，组成一个密钥对，分别称为公钥和私钥。公钥可以对外公开，并且可以通过安全或非安全通道发送，而私钥则为非公开部分，除了持有者之外无人知道。假设用户A拥有一个密钥对，其包括用户的公钥P_k和私钥S_k。用户A将其公钥P_k发送给另一用户B。如果用户B想要向用户A传输数据，则他可以利用用户A的公钥P_k对该数据进行加密，并传输给用户A。用户A在接收到加密数据之后，利用其私钥S_k对加密数据进行解密，以恢复出用户B想要传输给他的数据(明文)。另一方面，如果用户A想要向用户B传输数据，则他可以利用他自己的私钥S_k对该数据进行签名，并将签名数据传输给用户B。用户B在接收到签名数据后之后，如果能够利用用户A的公钥P_k对其进行解密，则能够验证该数据是由用户A发出的。因此可以看出，利用私钥对数据进行签名使得接收方能够验证发送方的身份。由于私钥的这种特性，使得对私钥管理的安全性要求变得非常高。

[0004] 在常规的金融行业中，用户的私钥通常存储在专门的硬件，例如USB盘、IC卡等存储设备中。在使用时，需要将该硬件与计算机相连，并且计算机从存储设备中调取该私钥以执行加密操作，在这个过程中存在一定的安全隐患。

[0005] 另一方面，当前，数字资产作为企业资产的一部分，与传统资产类似，也需要与企业的资产管理系统对接。由于数字资产与普通资产本质上的不同，一个私钥对应于一个数字资产地址，因此数字资产的管理几乎完全依赖于专用于数字资产的私钥的管理，从而企业需要针对私钥的保管解决方案。在企业的正常商业活动中，考虑到企业的组织架构以及资金管理的需求，不同的子机构、部门、员工或其他用户(以下统称为企业的用户)需要有单独的数字资产账户，从而势必需要多个私钥对应不同的数字资产账户。传统的私钥体系没有相关性，意味着企业的每个用户需要单独管理自己的账户，与企业的资产管理制度匹配度不高。

发明内容

[0006] 本公开提供了一种针对企业用户的数字资产管理的密钥安全管理方案，其通过在硬件安全设备内部进行用户密钥的生成和使用等操作，使得用户私钥不会离开硬件安全设备，从而确保了用户私钥的高度安全性。

[0007] 本公开的一个方面提供了一种密钥安全管理系统。所述密钥安全管理系统包括：安全主机，其被配置为接收第一操作请求，对所述第一操作请求进行验证，并在验证通过时基于所述第一操作请求生成第二操作请求，所述第一操作请求和所述第二操作请求都包括身份标识，以及硬件安全设备，其被配置为从所述安全主机接收所述第二操作请求，对所述第二操作请求进行验证，并且在验证通过时解析所述第二操作请求的类型，以及基于所述第二操作请求的类型执行和关联于所述身份标识的一个密钥对有关的操作，所述密钥对包括特定于所述身份标识的一个公钥和一个私钥。

[0008] 本公开的另一个方面提供了一种密钥安全管理方法。所述方法包括：由安全主机接收第一操作请求；由所述安全主机对所述第一操作请求进行验证并在验证通过时基于所述第一操作请求生成第二操作请求，所述第一操作请求和所述第二操作请求都包括身份标识；由所述硬件安全设备从所述安全主机接收所述第二操作请求，对所述第二操作请求进行验证，并在验证通过时解析所述第二操作请求的类型；以及由所述硬件安全设备基于所述第二操作请求的类型执行和关联于所述身份标识的一个密钥对有关的操作，所述密钥对包括特定于所述身份标识的一个公钥和一个私钥。

[0009] 本公开的又一个方面提供了一种非易失性计算机可读存储介质，其上存储有机器可执行指令，所述机器可执行指令在被计算机运行时，执行上述方面所述的密钥安全管理方法。

[0010] 本公开的再一个方面提供了一种计算机程序，其包括机器可执行指令，所述机器可执行指令在被运行时执行上述方面所述的密钥安全管理方法。

[0011] 以上为本申请的概述，可能有简化、概括和省略细节的情况，因此本领域的技术人员应该认识到，该部分仅是示例说明性的，而不旨在以任何方式限定本申请范围。本概述部分既非旨在确定所要求保护主题的关键特征或必要特征，也非旨在用作为确定所要求保护主题的范围的辅助手段。

附图说明

[0012] 通过下面说明书和所附的权利要求书并与附图结合，将会更加充分地清楚理解本申请内容的上述和其他特征。可以理解，这些附图仅描绘了本申请内容的若干实施方式，因此不应认为是对本申请内容范围的限定。通过采用附图，本申请内容将会得到更加明确和详细地说明。

[0013] 图1示出了根据本公开的一种密钥安全管理系统的示意图；

[0014] 图2示出了根据本公开的一种密钥安全管理方法的流程图；

[0015] 图3示出了图1所示的密钥安全管理系统中的硬件安全设备的一种操作实例的流程图；

[0016] 图4示出了图1所示的密钥安全管理系统中的硬件安全设备的另一种操作实例的流程图；

[0017] 图5示出了图1所示的密钥安全管理系统中的硬件安全设备的再一种操作实例的流程图。

具体实施方式

[0018] 在下面的详细描述中，参考了构成其一部分的附图。在附图中，类似的符号通常表示类似的组成部分，除非上下文另有说明。详细描述、附图和权利要求书中描述的说明性实施方式并非旨在限定。在不偏离本申请的主题的精神或范围的情况下，可以采用其他实施方式，并且可以做出其他变化。可以理解，可以对本申请中一般性描述的、在附图中图解说明的本申请内容的各个方面进行多种不同构成的配置、替换、组合，设计，而所有这些都明确地构成本申请内容的一部分。

[0019] 图1示出了根据本公开的一种密钥安全管理系统10的示意图。如图1所示，密钥安全管理系统10包括安全主机11和硬件安全设备12。安全主机11可以为任何类型的计算机。硬件安全设备12可以是硬件安全模块(Hardware Security Module，HSM)或其他满足预定的安全认证标准，例如信息技术安全评估统一准则(Common Criteria)、美国联邦信息处理标准(FIPS)140-2等国际认证的硬件安全设备，其包括存储器(图中未示出)和处理器(图中未示出)。硬件安全设备12能够根据各种非对称密码学算法产生专用于数字资产管理的、包括公钥和私钥的密钥对。这些非对称密码学算法是本领域中公知的，在此不再赘述。

[0020] 安全主机11被配置为接收第一操作请求，对第一操作请求进行验证，并在验证通过时基于第一操作请求生成第二操作请求，其中，第一操作请求和第二操作请求都包括身份标识。身份标识可以是用户的身份标识和/或与该用户关联的组织的身份标识。本公开中的“用户”和“组织”指具有隶属关系的不同主体，“用户”隶属于与其关联的“组织”。例如，“组织”可以是一个企业，而“用户”则可以是该企业的员工、子机构、部门或者企业的其他用户或客户。每个主体具有唯一的身份标识。

[0021] 硬件安全设备12被配置为从安全主机11接收第二操作请求，对第二操作请求进行验证，并且在验证通过时解析第二操作请求的类型，以及基于第二操作请求的类型执行和关联于该身份标识的一个密钥对有关的操作。这里，该密钥对包括特定于该身份标识的一个公钥和一个私钥。在一些实现中，硬件安全设备12能够基于比特币改进提议BIP32、BIP39和BIP44中共同定义的分层确定性钱包(Hierarchical Deterministic Wallet)规则(简称为分层确定性规则)来派生出组织的密钥对和用户的密钥对。

[0022] BIP32规定了一种从一个随机种子产生分层树状结构的密钥对系列的方法，BIP39规定了从一个助记的句子导出随机种子的方法，BIP44进一步赋予了分层树状结构中各层的特殊含义。关于BIP32、BIP39和BIP44的更具体的描述可以参见相应的比特币改进协议。根据分层确定性规则，首先通过函数PBKDF2将一个助记句子转换为随机种子，然后对随机种子进行哈希运算生成与根节点对应的主根密钥对，再然后基于该主根密钥对，派生出根节点的子节点对应的子节点密钥对，再进一步基于每个子节点的密钥对，进一步派生出子节点的子节点的密钥对，如此可以一直进行下去。其中，根节点可以派生出若干子节点，每个子节点又可派生出若干子节点，从而可以基于一个随机种子派生出无穷多个层次不同的密钥对。从根节点到树状结构的每个子节点具有不同的路径，每个路径与一个子节点一一对应，因此根据根节点的密钥对和子节点的路径即可确定该路径对应的子节点的密钥对。如果将根节点对应到一个组织(例如一个公司)，将子节点对应到该组织的一个用户(例如公司的一个部门或者一个成员)，则根节点对应的主根密钥对可作为该组织的主根密钥对，子节点对应的密钥对可以作为用户的密钥对。

[0023] 在一些实施例中，密钥安全系统10还包括应用服务器13。应用服务器13可以与安全主机11位于同一网络内，也可以位于不同网络而经由例如网桥与安全主机11相连。应用服务器13被配置为接收外部节点，例如客户端20或区块链节点30的访问请求，并根据该访问请求生成至少一个第一操作请求，以及向安全主机11发送该第一操作请求。另一方面，在安全主机11和硬件安全设备12根据该第一操作请求执行了相应的操作之后，应用服务器13还可以从安全主机11接收该操作的结果并将其返回给外部节点。

[0024] 安全主机11和硬件安全设备12位于同一安全网域内，以使得应用服务器13或其他外部组件只能够通过安全主机11来访问硬件安全设备12(即安全主机11作为访问硬件安全设备12的网关)。例如，这可以通过在安全主机11处设置防火墙以及在安全主机11和硬件安全设备12之间设置安全链路来实现。

[0025] 将参考下面的图2至图5来进一步描述安全主机11和硬件安全设备12的具体功能和操作。

[0026] 图2示出了根据本公开的密钥安全管理方法100的示意图。方法100的各个步骤可分别由图1所示的相应主体执行。下面结合图1和图2分别对方法100进行详细说明。

[0027] 安全主机11被配置为接收第一操作请求(步骤110)。第一操作请求由该请求的发送者(例如如图1中所示的应用服务器13)签名并且取决于请求的业务类型而包括至少一个身份标识。第一操作请求例如可以是针对数字资产的各种操作请求，如转账请求，也可以是与数字资产无关的各种操作请求，如部署智能合约、调用智能合约等。此外，如果广义地将数字资产理解为还包括除了加密货币之外的数字所有物(例如数字文档或数字美术作品等)的话，第一操作请求也可以是针对该数字所有物的转移或存证请求。

[0028] 进一步地，安全主机11被配置为对第一操作请求进行验证(步骤120)。步骤120的验证可以包括验证第一操作请求的发送者(如应用服务器13)的证书的有效性以及签名的有效性。具体地，安全主机11解析第一操作请求以获取其中包含的应用服务器证书和应用服务器签名。该应用服务器证书包含应用服务器13的身份标识、应用服务器13的允许业务类型列表和应用服务器证书的有效期。安全主机11利用应用服务器13的公钥对应用服务器签名进行解密，以获取第一操作请求所请求的业务类型。安全主机11将第一操作请求所请求的业务类型与应用服务器证书中所包含的允许业务类型列表进行比较以确定是否允许第一操作请求所请求的业务类型。进一步的，安全主机11还可以被配置为验证应用服务器证书是否处于其有效期内。此外，在一些实现中，安全主机11还可以被配置为从区块链获取该应用服务器证书的状态以验证其状态是否有效。如果上述判断都为是，则步骤121中判断第一操作请求验证通过。

[0029] 如果第一操作请求验证通过(步骤121中判断为“是”)，则安全主机11基于第一操作请求生成第二操作请求(步骤122)并将其发送给硬件安全设备12(步骤123)。

[0030] 第二操作请求至少包括类型字段和数据字段。类型字段可以采用预定义的二进制序列进行编码，不同的二进制序列表示不同的类型。通过对类型字段进行译码，即可确定第二操作请求的类型。数据字段可以包括一个身份标识，例如组织的身份标识，或者可以包括两个身份标识，例如组织的身份标识和与该组织关联的用户的身份标识。

[0031] 第二操作请求由安全主机11用其私钥进行签名。硬件安全设备12被配置为在收到第二操作请求后，对第二操作请求进行验证(步骤130)。步骤130的验证可以包括验证安全

主机11的证书的有效性以及签名的有效性。具体地，硬件安全设备12被配置为解析第二操作请求以获取其中包含的安全主机证书和安全主机签名。该安全主机证书包含安全主机11的身份标识、安全主机11的允许业务类型列表和安全主机证书的有效期。硬件安全设备12利用安全主机11的公钥对安全主机签名进行解密，以确定第二操作请求是否由安全主机11签名。进一步的，硬件安全设备12还可以被配置为验证安全主机证书是否处于其有效期内。如果上述判断都为是，则步骤131中判断第二操作请求的验证通过。

[0032] 硬件安全设备12被进一步配置为在对第二操作请求的验证通过后(步骤131中判断为“是”)，解析第二操作请求的类型(步骤132)，并基于第二操作请求的类型执行和关联于身份标识的一个密钥对有关的操作(步骤133)。在这里，“和关联于身份标识的一个密钥对有关的操作”可以指硬件安全设备12执行的与关联于该请求中包含的身份标识的密钥对有关的任何操作。如果第二操作请求验证未通过，或者验证通过且执行完毕后，硬件安全设备12向安全主机11发送第二操作请求结果以分别指示请求失败或者返回对该请求的响应(步骤134)。相应地，该请求结果还被安全主机11发送给应用服务器13(如果有的话)(步骤124)，该结果继而还被发送给发出请求的外部节点(如客户端20或区块链节点30)(图中未示出)。

[0033] 图3示出了图1所示的密钥安全管理系统10中的硬件安全设备12的一种操作实例的流程图。在如图3中所示的实例中，在步骤132中对第二操作请求的解析结果指示第二操作请求的类型为生成组织的主根密钥对，且第二操作请求的数据字段包含该组织的身份标识。因此，在执行基于第二操作请求的类型执行和关联于身份标识的密钥对有关的操作(步骤133)时，硬件安全设备12被进一步配置为响应于第二操作请求的类型是请求生成组织的主根密钥对，首先产生随机的密钥种子(步骤1331)，然后使用该密钥种子产生组织的主根密钥对(步骤1332)，并将该主根密钥对存储在其存储器中(步骤1333)。进一步地，为了防止密钥种子被他人非法获取，硬件安全设备12被进一步配置为在产生组织的主根密钥对之后销毁该密钥种子(步骤1334)。

[0034] 在这种情况下，步骤134中的第二操作请求结果可以包括成功产生该组织的主根密钥的指示。

[0035] 图4示出了图1所示的密钥安全管理系统10中的硬件安全设备12的另一种操作实例的流程图。在如图4中所示的实例中，在步骤132中对第二操作请求的解析结果指示第二操作请求的类型为请求获取用户的公钥，且第二操作请求的数据字段包含组织的身份标识和该用户的身份标识。并且，硬件安全设备12中存储有组织的主根密钥对。因此，在执行基于第二操作请求的类型执行和关联于身份标识的密钥对有关的操作(步骤133)时，硬件安全设备12被进一步配置为响应于第二操作请求的类型是请求获取用户的公钥，根据组织的身份标识确定组织的主根密钥对(步骤1335)，基于用户的身份标识确定用户的密钥对生成路径(步骤1336)，基于用户的密钥对生成路径和组织的主根密钥对派生出用户的密钥对(步骤1337)。

[0036] 在这种情况下，步骤134中的第二操作请求结果包括用户的密钥对中的公钥。系统可以预先定义身份标识与分层确定性规则的派生出的子节点(每个用户对应于一个子节点)的路径之间的映射关系，从而可以基于用户的身份标识确定用户的密钥对生成路径。较佳地，可以对用户的身份标识和组织的身份标识的组合执行哈希运算以得到哈希值，然后

基于该哈希值和分层确定性规则)确定用户的密钥对生成路径。

[0037] 图5示出了图1所示的密钥安全管理系统10中的硬件安全设备12的再一种操作实例的流程图。在如图5中所示的实例中,在步骤132中对第二操作请求的解析结果指示第二操作请求的类型为对待签名数据进行签名,且第二操作请求的数据字段包含组织的身份标识、该用户的身份标识和该待签名数据。并且,硬件安全设备12中存储有该组织的主根密钥对。因此,在执行基于第二操作请求的类型执行和关联于身份标识的密钥对有关的操作(步骤133)时,硬件安全设备12被进一步配置为响应于第二操作请求的类型是请求对待签名数据进行签名,根据组织的身份标识确定组织的主根密钥对(步骤1339),基于用户的身份标识确定用户的密钥对生成路径(步骤1340),基于用户的密钥对生成路径和组织的主根密钥对派生出用户的密钥对(步骤1341),利用用户的密钥对中的私钥对待签名数据进行签名以得到签名数据(步骤1342)。为了防止用户的私钥被他人非法获取,硬件安全设备12被进一步配置为在签名之后销毁该用户的私钥(图中未示出)。

[0038] 在这种情况下,步骤134中的第二操作请求结果包括该签名数据。

[0039] 其中,步骤1336和/或1340具体还可以包括:对用户的身份标识和组织的身份标识的组合执行哈希运算以得到哈希值,并且基于该哈希值和分层确定性规则确定用户的密钥对生成路径。

[0040] 这里,以硬件安全设备12中事先存储有组织的主根密钥对为例来对图4和图5的操作实例进行表述,然而本领域技术人员可以理解,本公开并不局限于此。硬件安全设备12中可以不事先存储组织的主根密钥对,而是在每次请求用户的公钥或签名时,执行如图3中所示的方法流程来产生组织的主根密钥对以作为导出用户的公钥或私钥的基础。

[0041] 此外,上述图3的实例中描述了直接为组织产生特定于该组织的主根密钥对的情况。然而,本公开并不局限于此。在一些情况下,例如密钥安全管理系统10通过单个硬件安全设备12管理多个组织及其各自的用户的密钥对的情况下,可以参照如图3所示的方法产生特定于硬件安全设备12的根密钥对,并且根据该根密钥对和硬件安全设备12所管理的各个组织之间的关系派生出各个组织的主根密钥对(类似于图4和图5所示的实例中的用户密钥对的派生方式)。在这种情况下,密钥安全设备12中可以仅存储特定于该密钥安全设备12的根密钥对,而不存储任何组织或其用户的密钥对。

[0042] 此外,本文中使用的术语“证书”仅仅借用了常规技术中的用语,并不一定代表其具有与常规技术中完全相同的内涵和外延,也不代表其必然由常规技术中所称的证书授权中心发布。

[0043] 通过本公开的方法100可以看出,本公开通过主机11和硬件安全设备12对操作请求的双重认证,有效防止了非授权的访问。同时,本公开利用硬件安全设备12具有高度安全性的特点,在硬件安全设备12内部进行密钥的生成和使用等操作。用户的私钥在使用完毕后即销毁,使得在任何情况下用户的私钥都不会离开硬件安全设备12,即任何设备都无法获取用户私钥。此外,只有授权设备才能够获得用户的私钥签名,从而确保了用户私钥的高度安全性。另外,由于本公开采用基于分层确定性规则确定用户的密钥的方法,因此,对于企业内部不同的子机构、部门、员工或企业的用户或客户都需要有单独的数字资产账户的情况下,可以方便地对这些单独的数字资产账户的私钥进行管理,而无需他们自己保存私钥,从而极大地提高了数字资产管理的安全性。

[0044] 在一个或多个示例性的实施例中，还提供了一种包括机器可执行指令的非易失性计算机可读存储介质，上述指令可由计算机运行以执行本公开的密钥安全管理方法100。

[0045] 在一个或多个示例性设计中，可以用硬件、软件、固件或它们的任意组合来实现本公开所述的功能。例如，如果用软件或固件来实现，则可以将所述功能作为一个或多个指令或代码存储在计算机可读存储介质上，或者作为计算机可读存储介质上的一个或多个指令或代码来传输。

[0046] 本文公开的系统的各个组成部分可以使用分立硬件组件来实现，也可以集成地实现在一个硬件组件。例如，可以用通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑器件、分立门或者晶体管逻辑、分立硬件组件或其组合来实现或执行结合本公开所描述的各种示例性的组成部分。

[0047] 本技术领域的一般技术人员可以通过阅读说明书、公开的内容及附图和所附的权利要求书，理解和实施对披露的实施方式的其他改变。在权利要求中，措辞“包括”不排除其他的元素和步骤，并且措辞“一”、“一个”不排除复数。在本申请的实际应用中，一个零件可能执行权利要求中所引用的多个技术特征的功能。权利要求中的任何附图标记不应理解为对范围的限制。

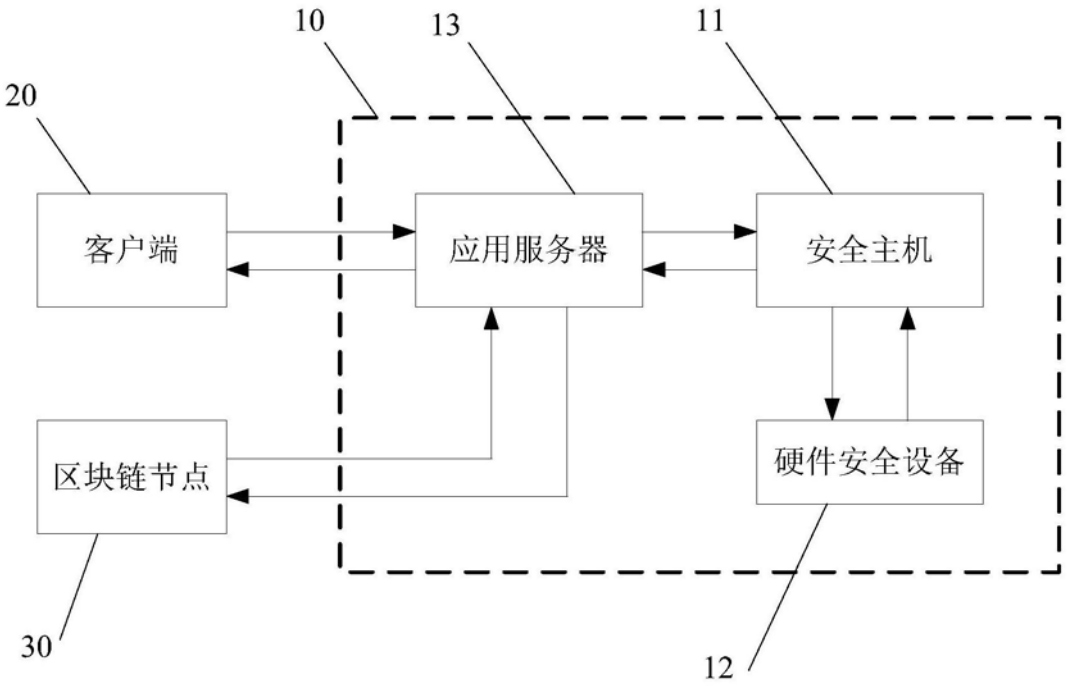


图1

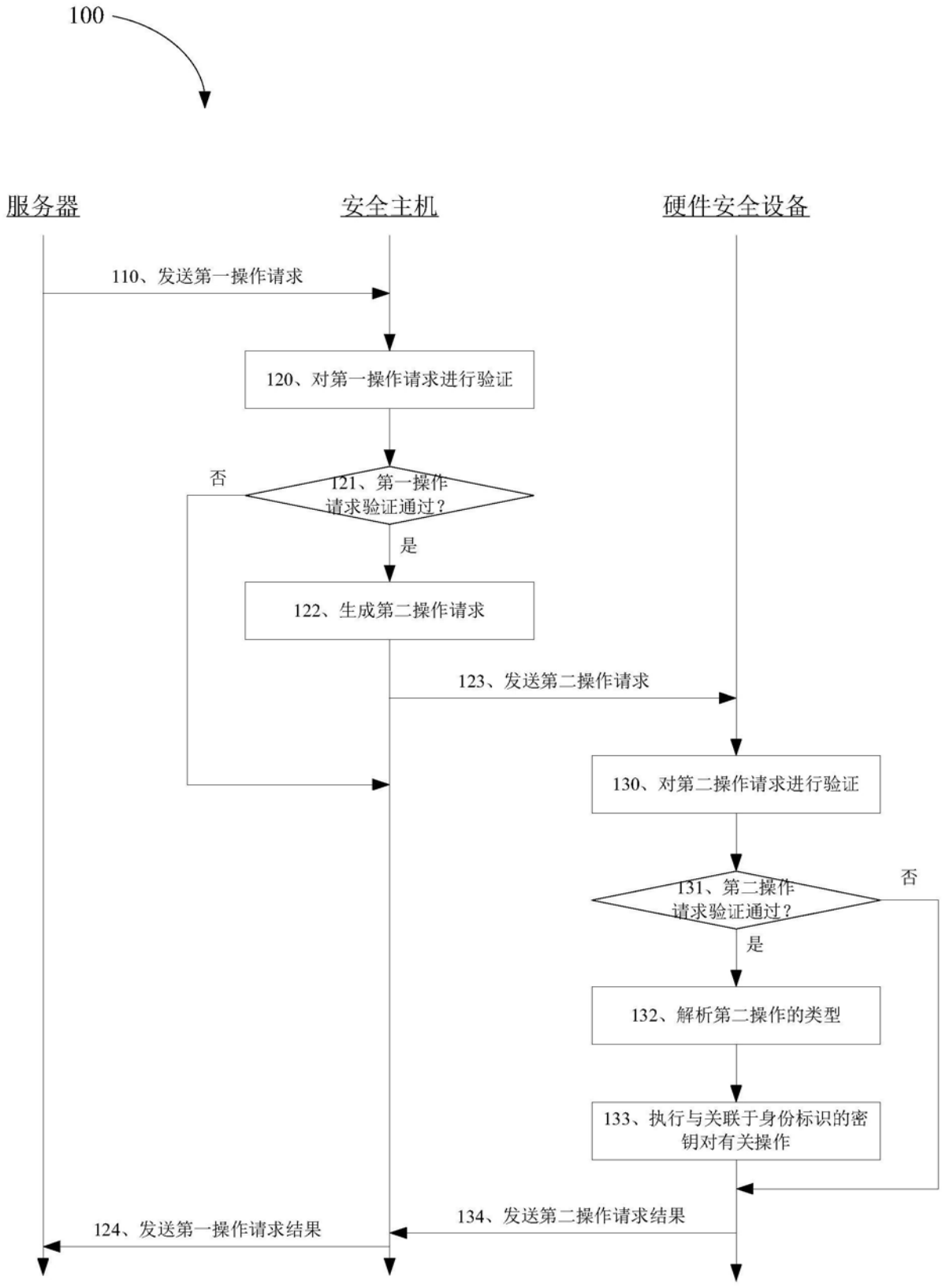

100
服务器
安全主机
硬件安全设备
110、发送第一操作请求
120、对第一操作请求进行验证
否
121、第一操作请求验证通过？
是
122、生成第二操作请求
123、发送第二操作请求
130、对第二操作请求进行验证
131、第二操作请求验证通过？
否
是
132、解析第二操作的类型
133、执行与关联于身份标识的密钥对有关操作
134、发送第二操作请求结果
124、发送第一操作请求结果

图2

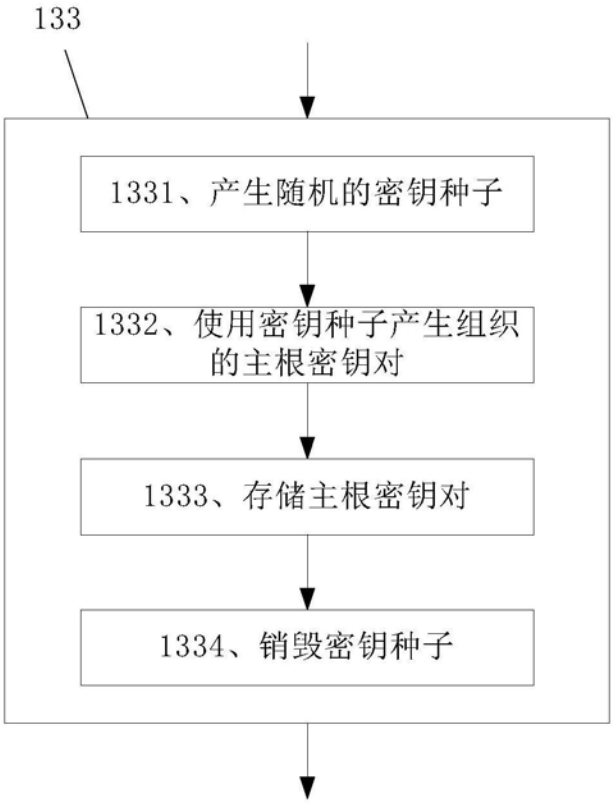

133
1331、产生随机的密钥种子
1332、使用密钥种子产生组织的主根密钥对
1333、存储主根密钥对
1334、销毁密钥种子

图3

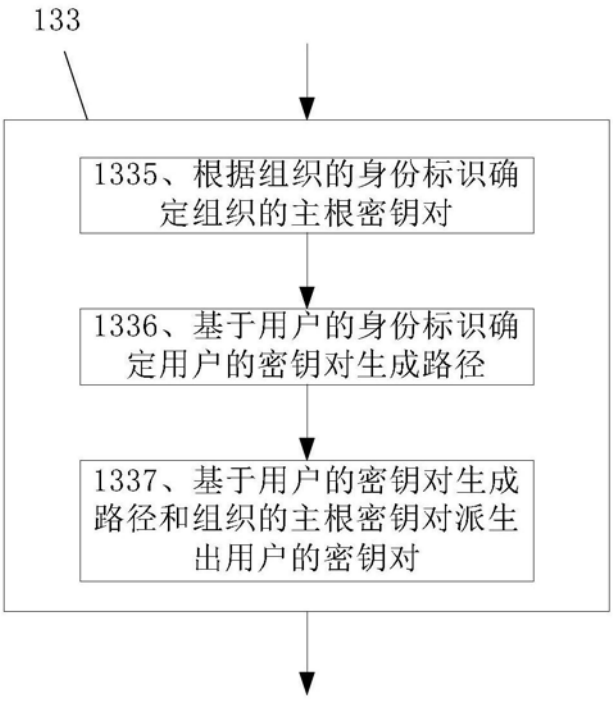

133
1335、根据组织的身份标识确定组织的主根密钥对
1336、基于用户的身份标识确定用户的密钥对生成路径
1337、基于用户的密钥对生成路径和组织的主根密钥对派生出用户的密钥对

图4

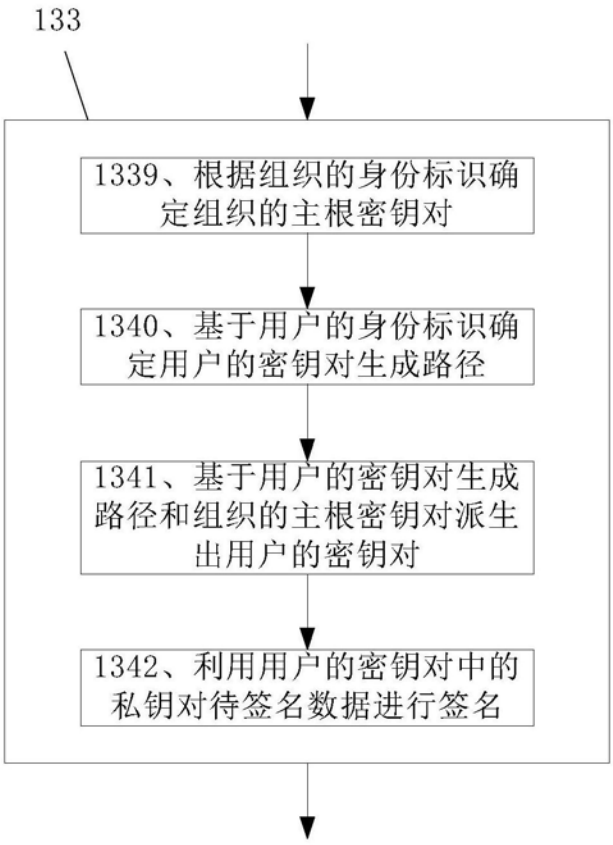

133
1339、根据组织的身份标识确定组织的主根密钥对
1340、基于用户的身份标识确定用户的密钥对生成路径
1341、基于用户的密钥对生成路径和组织的主根密钥对派生出用户的密钥对
1342、利用用户的密钥对中的私钥对待签名数据进行签名

图5