Certificate No. 8623511

Patent Certificate of Invention

Title of Invention:	Methods and apparatus for digital signatures
Patentee:	Sebastien Armleder
Address:	c/o Cryptnox SA, Cardinal Mermillod 36, 1227 Carouge, Switzerland
Inventor:	Sebastien Armleder
Patent Number:	ZL 202211056164.7
Announcement Number:	CN 115776374 B
Date of Filing:	August 31, 2022
Date of Announcing Grant of Patent:	January 2, 2026
Applicant On the Date of Filing:	Sebastien Armleder
Inventor On the Date of Filing:	Sebastien Armleder

According to the Chinese Patent Law, after examination, the China National Intellectual Property Administration decides to grant the patent and make announcement. The patent shall take effect as of the announcement date. For legal information such as validity of the patent right and change of the patentee, please refer to the Patent Register.

Director of China National Intellectual Property Administration:
Changyu Shen
January 2, 2026

证书号第8623511号

专利公告信息

发明专利证书

发 明 名 称：用于数字签名的方法和装置

专 利 权 人：塞巴斯蒂安·阿姆莱德

地　　址：瑞士卡鲁日

发　明　人：塞巴斯蒂安·阿姆莱德

专　利　号：ZL 2022 1 1056164.7　　授权公告号：CN 115776374 B

专利申请日：2022年08月31日　　授权公告日：2026年01月02日

申请日时申请人：塞巴斯蒂安·阿姆莱德

申请日时发明人：塞巴斯蒂安·阿姆莱德

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，并予以公告。

专利权自授权公告之日起生效。专利权有效性及专利权人变更等法律信息以专利登记簿记载为准。

局长
申长雨

国家知识产权局
2026年01月02日

(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115776374 B
(45)授权公告日 2026.01.02

(21)申请号 202211056164.7

(22)申请日 2022.08.31

(65)同一申请的已公布的文献号
申请公布号 CN 115776374 A

(43)申请公布日 2023.03.10

(30)优先权数据
21195614.9 2021.09.08 EP
22150341.0 2022.01.05 EP

(73)专利权人 塞巴斯蒂安·阿姆莱德
地址 瑞士卡鲁日

(72)发明人 塞巴斯蒂安·阿姆莱德

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 王伟楠 姚文杰

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
US 2018262341 A1,2018.09.13
WO 2014106181 A2,2014.07.03
EP 3474209 A1,2019.04.24

审查员 李普昕

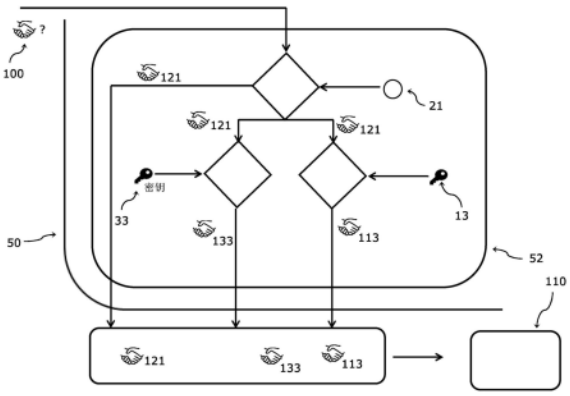
权利要求书3页 说明书15页 附图11页

(54)发明名称

用于数字签名的方法和装置

(57)摘要

本发明提供了用于数字签名的方法和装置。本发明涉及一种包括安全部的数据处理装置,其中,安全部包括私钥、未加密的私有证书密钥和基于私有证书密钥生成的种子,其中,私钥、未加密的私有证书密钥和种子不能从安全部中提取。本发明还涉及一种方法,其中,该方法使用数据处理装置,该方法包括:安全部接收签署请求;在安全部中,生成使用从种子得出的私钥签署的签名,并且使用未加密的私有证书密钥来签署签名,由此生成使用未加密的私有证书密钥签署的签名;以及输出使用从种子得出的私钥签署的签名和使用未加密的私有证书密钥签署的签名。



CN 115776374 B

1.一种数据处理装置(50),包括安全部(52),

其中,所述安全部(52)包括:

私钥(13),

未加密的私有证书密钥(33),以及

基于所述未加密的私有证书密钥(33)生成的种子(21),

其中,所述私钥(13)、所述未加密的私有证书密钥(33)和所述种子(21)不能从所述安全部(52)提取,

其中,所述数据处理装置(50)包括签署的数字系统证书(36),其中,使用与所述私有证书密钥(33)对应的公共证书密钥(34)来签署所述签署的数字系统证书(36),并且其中,所述签署的数字系统证书(36)基于个人用户数据(82)、签署的数字证书(16)和所述公共证书密钥(34)。

2.根据权利要求1所述的数据处理装置(50),其中,所述数据处理装置(50)包括所述签署的数字证书(16)。

3.根据权利要求1所述的数据处理装置(50),其中,所述安全部(52)包括随机数生成器(11)。

4.根据权利要求3所述的数据处理装置(50),其中,所述数据处理装置包括由所述随机数生成器(11)生成的序列号(12)。

5.根据权利要求1所述的数据处理装置(50),其中,所述数据处理装置(50)是智能卡,其中,所述智能卡具有近场通信功能。

6.根据权利要求1所述的数据处理装置(50),其中,所述数据处理装置(50)被配置成:仅允许通过所述未加密的私有证书密钥(33)来签署通过从种子(21)得出的密钥签署的数据结构。

7.根据权利要求1所述的数据处理装置(50),其中,所述数据处理装置(50)被配置成:仅允许通过所述私钥(13)来签署通过从种子(21)得出的密钥签署的数据结构。

8.根据权利要求1所述的数据处理装置(50),其中,所述安全部(52)包括远程公钥(202)。

9.根据权利要求1至8中任一项所述的数据处理装置(50),其中,所述数据处理装置(50)能够通过一种方法获得,其中,所述方法包括:

提供数据处理装置(50),其中,所述数据处理装置(50)包括所述安全部(52),其中,所述安全部(52)包括不能从所述安全部(52)提取的私钥(13),其中,所述安全部(52)包括与所述私钥(13)对应的公钥(14),

所述数据处理装置提供签署请求(15)、所述公钥(14)和序列号(12),

基于所述签署请求(15)、所述公钥(14)和所述签署请求(15),外部数据处理装置(60)生成所述签署的数字证书(16),以及

将所述签署的数字证书(16)提供给所述数据处理装置(50),

将所述签署的数字证书(16)提供给数据处理系统(70),

所述数据处理系统(70)从用户(80)接收个人用户数据(82),

将所述公共证书密钥(34)提供给所述数据处理系统(70),

所述数据处理系统(70)基于所述个人用户数据(82)、所述签署的数字证书(16)和所述

公共证书密钥(34)来生成使用所述公共证书密钥(34)签署的所签署的数字系统证书(36)，

将所述签署的数字系统证书(36)提供给所述数据处理装置(50)，

生成所述公共证书密钥(34)和所述对应的私有证书密钥(33)，

使用所述公钥(14)对所述私有证书密钥(33)进行加密，从而生成包装的密钥(40)，以及

将所述包装的密钥(40)提供给所述数据处理装置的安全部(52)，

在所述安全部(52)中，使用所述私钥(13)对所述包装的密钥(40)进行解密，从而获得所述私有证书密钥(33)，

在所述安全部(52)中，基于所述私有证书密钥(33)来生成所述种子(21)。

10.一种使用数据处理装置(50)的方法，所述数据处理装置(50)包括安全部(52)，

其中，所述安全部(52)包括：

私钥(13)，

未加密的私有证书密钥(33)，以及

基于所述未加密的私有证书密钥(33)生成的种子(21)，

其中，所述私钥(13)、所述未加密的私有证书密钥(33)和所述种子(21)不能从所述安全部(52)提取，

所述方法包括：

所述安全部(52)接收签署请求(100)，

在所述安全部(52)中，生成使用从种子(21)得出的私钥签署的签名(121)，以及使用未加密的私有证书密钥(33)签署所述签名(121)，从而生成使用所述未加密的私有证书密钥(33)签署的签名(133)，

输出使用从所述种子(21)得出的私钥签署的签名(121)和使用所述未加密的私有证书密钥(33)签署的签名(133)。

11.根据权利要求10所述的方法，其中，所述方法还包括：

在所述安全部(52)中，使用私钥(13)来签署所述签名(121)，从而生成使用所述私钥(13)签署的签名(113)，

将使用所述私钥(13)签署的签名(113)以及使用从所述种子(21)得出的私钥签署的签名(121)和使用所述未加密的私有证书密钥签署的签名(133)一起输出。

12.根据权利要求10所述的方法，其中，所述数据处理装置(50)包括签署的数字证书(16)，

其中，所述方法还包括：将所述签署的数字证书(16)以及使用从所述种子(21)得出的私钥签署的签名(121)和使用所述未加密的私有证书密钥签署的签名(133)一起输出。

13.根据权利要求10所述的方法，

其中，所述数据处理装置(50)包括签署的数字系统证书(36)，其中，使用与所述私有证书密钥(33)对应的公共证书密钥(34)来签署所述签署的数字系统证书(36)，并且其中，所述签署的数字系统证书(36)基于个人用户数据(82)、签署的数字证书(16)和所述公共证书密钥(34)，

其中，所述方法还包括：将所述签署的数字系统证书(36)以及使用从所述种子(21)得出的私钥签署的签名(121)和使用所述未加密的私有证书密钥签署的签名(133)一起输出。

14.根据权利要求10至13中任一项所述的方法，

其中，所述数据处理装置(50)的安全部(52)包括远程公钥(202)，

其中，所述方法还包括：

远程签名系统(20)接收所述签署请求(100)，

所述远程签名系统(20)使用与远程公钥(202)对应的远程私钥(200)来签署所述签署请求(100)，从而生成预签名(210)，

所述安全部(52)接收所述预签名(210)，以及

在所述安全部(52)中，使用所述远程公钥(202)来验证所述预签名(210)是使用所述远程私钥(200)签署的签署请求(100)，

其中，根据使用所述远程公钥(202)成功验证所述预签名(210)是使用所述远程私钥(200)签署的签署请求(100)，在所述安全部(52)中生成至少一个签名(121、133、113、250)并输出所述至少一个签名(121、133、113、250)。

15.根据权利要求10所述的方法，其中，所述数据处理装置(50)是根据权利要求1至8中任一项所述的数据处理装置。

用于数字签名的方法和装置

技术领域

[0001] 本发明涉及数字签名。例如,数字签名可以用于签署区块链交易、智能合约或提供时间戳。

背景技术

[0002] 虽然已知提供数字签名的许多方法,但是特别是在可追溯性和防伪安全性方面,它们具有某些缺点和不足。

发明内容

[0003] 本发明试图克服或至少减轻现有技术方法的缺点和不足。因此,本发明的目的是提供一种例如在可追溯性和/或防伪安全性方面相对于现有技术改进的用于数字签名的技术。

[0004] 本发明满足了这些目的。

[0005] 在第一方面,本发明涉及一种方法。该方法包括:提供数据处理装置,其中,数据处理装置包括安全部,其中,安全部包括不能从安全部提取的私钥,其中,安全部包括与私钥对应的公钥;数据处理装置提供签署请求、公钥和序列号;外部数据处理装置基于签署请求、公钥和签署请求来生成签署的数字证书;以及将签署的数字证书提供给数据处理装置。应当理解,根据第一方面的方法涉及设置和初始化数据处理装置。为了区分初始化前和初始化后的数据处理装置,还可以将尚未被初始化的数据处理装置称为本地或初始数据处理装置。

[0006] 安全部可以包括不能从安全部提取的随机数生成器,并且该方法可以包括:随机数生成器生成序列号。

[0007] 可以基于来自随机数生成器的输出来生成私钥。

[0008] 数据处理装置可以是智能卡。

[0009] 智能卡可以具有近场通信功能。

[0010] 该方法可以包括:将签署的数字证书提供给数据处理系统;数据处理系统从用户接收个人用户数据;将公共证书密钥提供至数据处理系统;数据处理系统基于个人用户数据、签署的数字证书和公共证书密钥来生成使用公共证书密钥签署的签署的数字系统证书;以及将签署的数字系统证书提供给数据处理装置。应当理解,将公共证书密钥提供给数据处理系统还包括:由数据处理系统生成公共证书密钥。

[0011] 该方法可以包括:生成公共证书密钥和对应的私有证书密钥;使用公钥对私有证书密钥进行加密,从而生成包装的密钥;以及将包装的密钥提供给数据处理装置的安全部。

[0012] 生成公共证书密钥和对应的私有证书密钥,使用公钥对私有证书密钥进行加密,从而生成包装的密钥,以及将包装的密钥提供给数据处理装置的安全部可以由数据处理系统执行,并且其中,包装的密钥从数据处理系统被提供给数据处理装置的安全部。

[0013] 生成公共证书密钥和对应的私有证书密钥,使用公钥对私有证书密钥进行加密,

从而生成包装的密钥,以及将包装的密钥提供给数据处理装置的安全部可以由另一数据处理系统来执行;该方法还可以包括:将公钥从数据处理装置提供给另一数据处理系统;其中,将公共证书密钥提供给数据处理系统包括:将公共证书密钥从另一数据处理系统提供给数据处理系统。

[0014] 该方法可以包括:在安全部中,使用私钥对包装的密钥进行解密,从而获得私有证书密钥。

[0015] 该方法可以包括:在安全部中,基于私有证书密钥来生成种子。

[0016] 通过所描述的方法,可以设置和初始化数据处理装置。应当理解,在执行该方法之后,数据处理装置包括签署的数字证书和签署的数字系统证书(由公共证书密钥签署)。此外,数据处理装置的安全部还包括种子、私钥和私有证书密钥。

[0017] 在另一方面,本发明涉及一种用于初始化包括安全部的数据处理装置的初始化方法,其中,该初始化方法包括:在远程签名系统中生成包括远程私钥和远程公钥的远程非对称密钥对,将远程公钥提供给数据处理装置的安全部,并且生成签署凭证,其中,远程签名系统被配置成:在接收到签署凭证时签署数据结构。

[0018] 签署凭证可以由远程签名系统生成。

[0019] 初始化方法还可以包括:将签署凭证提供给数据处理装置,例如提供给数据处理装置的安全部。

[0020] 本发明还涉及一种组合方法。该组合方法包括如以上所讨论的方法和如以上所讨论的初始化方法。该方法的数据处理装置是初始化方法的数据处理装置。应当理解,该方法的安全部是初始化方法的安全部。

[0021] 在另一方面,本发明涉及一种包括安全部的数据处理装置;其中,安全部包括私钥、未加密的私有证书密钥以及基于私有证书密钥生成的种子,其中,私钥、未加密的私有证书密钥和种子不能从安全部提取。

[0022] 这样的数据处理装置例如通过根据第一方面的方法获得的数据处理装置可以具有改进的功能。

[0023] 特别地,通过种子和私有证书密钥,数据处理装置可以签署签名,例如然后可以被输出(例如,被广播)的交易的签名。

[0024] 例如,通过使用可以由外部实体提供的未加密的私有证书密钥,可以提供附加的验证。例如,私有证书密钥可以由识别的实体发布,并且如果使用由这样的实体发布的密钥,则另一用户可以仅识别签名,从而提供白名单功能。

[0025] 数据处理装置可以包括签署的数字证书。

[0026] 安全部包括随机数生成器。

[0027] 数据处理装置可以是智能卡。

[0028] 智能卡可以具有近场通信功能。

[0029] 数据处理装置可以包括由随机数生成器生成的序列号。

[0030] 数据处理装置可以包括签署的数字系统证书,其中,签署的数字系统证书是使用与私有证书密钥对应的公共证书密钥签署的,并且其中,签署的数字系统证书基于个人用户数据、签署的数字证书和公共证书密钥。

[0031] 由于数据处理装置可以包括签署的数字证书和/或签署的数字系统证书,所以这

些证书中的任何证书也可以被附加至交易的签名,使得本技术还使得数据处理装置的用户能够在需要或期望的情况下提供标识基础。

[0032] 该数据处理装置可能是可获得的,并且优选地可以通过如以前所讨论的方法而获得。

[0033] 所描述的技术特别是所描述的用于初始化数据处理装置的方法还允许:例如在数据处理装置丢失的情况下生成具有对应功能的数据处理装置。具体地,私有证书密钥可以再次以相同的方式被包装并被提供给另一数据处理装置(即,由公钥包装),并且以相同的方式被解密。因此,例如在数据处理装置丢失的情况下,也可以向另一数据处理装置提供未加密的私有证书密钥和从未加密的私有证书密钥得出的种子,从而向另一数据处理装置提供相应的功能。相应的考虑也适用于数字系统证书,在提供用户的新标识的情况下,也可以向数字系统证书提供大部分对应的数据。总之,本技术的实施方式因此还允许备份解决方案的实现。

[0034] 还将理解,所描述的技术允许撤销所描述的证书。也就是说,例如,在数据处理装置丢失的情况下,生成证书之一的外部实体可以撤销对应的证书,从而提高数据处理装置的安全性。

[0035] 应当理解,在某些情况下,数据处理装置的证书中的至少一个也可以与签署的签名一起输出。这允许检查证书是否仍然有效。

[0036] 此外,如所讨论的,未加密的私有证书密钥仅存在于数据处理装置的安全部中并且不能从安全部中提取。因此,相应的数据处理装置也不能被用户伪造。

[0037] 数据处理装置可以被配置成仅允许通过未加密的私有证书密钥来签署通过从种子得出的密钥签署的数据结构。

[0038] 数据处理装置可以被配置成仅允许通过密钥来签署通过从种子得出的密钥签署的数据结构。

[0039] 本发明还涉及一种数据处理装置,其中,该数据处理装置包括安全部,其中,安全部包括远程公钥。

[0040] 可以通过以上所讨论的初始化方法来初始化数据处理装置。

[0041] 在所有方面,安全部可以包括远程公钥。

[0042] 可以通过以上所讨论的组合方法来获得数据处理装置。

[0043] 远程公钥可以对应于存储在远程签名系统中的远程私钥。

[0044] 数据处理装置还可以包括签署凭证以触发由远程签名系统的签名。

[0045] 在又一方面,本发明涉及一种方法,其中,该方法使用根据前述装置实施方式中任一项所述的数据处理装置,该方法包括:

[0046] 安全部接收签署请求,

[0047] 在安全部中,生成至少一个签名,以及

[0048] 输出至少一个签名。

[0049] 该方法可以使用以上所讨论的数据处理装置。生成至少一个签名可以包括:生成使用从种子得出的私钥签署的签名,并且使用未加密的私有证书密钥来签署签名,从而生成使用未加密的私有证书密钥签署的签名,并且输出至少一个签名可以包括:输出使用从种子得出的私钥签署的签名和使用未加密的私有证书密钥签署的签名。

[0050] 该方法还可以包括:在安全部中,使用私钥来签署签名,从而生成使用私钥签署的签名;以及将使用私钥签署的签名以及使用从种子得出的私钥签署的签名和使用未加密的私有证书密钥签署的签名一起输出。

[0051] 该方法可以使用以前所讨论的数据处理装置,并且该方法还可以包括:将签署的数字证书以及使用从种子得出的私钥签署的签名和使用未加密的私有证书密钥签署的签名一起输出。

[0052] 该方法可以使用如以前所讨论的数据处理装置,并且该方法还可以包括:将签署的数字系统证书以及使用从种子得出的私钥签署的签名和使用未加密的私有证书密钥签署的签名一起输出。

[0053] 该方法还可以包括:远程签名系统接收签署请求,远程签名系统使用与远程公钥对应的远程私钥对签署请求进行签署,从而生成预签名,安全部接收预签名,并且在安全部中使用远程公钥来验证预签名是使用远程私钥签署的签署请求,其中,根据使用远程公钥成功验证预签名是使用远程私钥签署的签署请求,在安全部中生成至少一个签名并输出所述至少一个签名。

[0054] 该方法还可以包括:远程签名系统接收签署凭证,其中,远程签名系统使用与远程公钥对应的远程私钥对签署请求进行签署,从而可以根据远程签名系统接收签署凭证来生成预签名。

[0055] 该方法还可以包括:禁用远程签名系统使用远程私钥进行签署的能力。

[0056] 通过使用该技术,数据处理装置的签名功能被链接至远程签名系统,该远程签名系统可以是基于云的。特别地,数据处理装置(例如,智能卡)的签名功能取决于接收预签名(即,使用远程签名系统的远程私钥签署的签署请求)的数据处理装置。仅当数据处理装置接收到由远程签名系统签署的预签名时,数据处理装置才对签署请求进行签署。

[0057] 这允许通过远程签名系统的签署功能来控制数据处理装置的签署功能。例如,在数据处理装置丢失的情况下,可以阻止远程签名系统中的相应远程私钥,从而阻止数据处理装置的签署功能,这例如在数据处理装置被盗的情况下可以增加防止欺诈的安全性。

[0058] 本发明还由以下编号的实施方式限定。

[0059] 下面,将讨论方法实施方式。通过字母M后跟数字来简写这些实施方式。每当在本文中提及方法实施方式时,都意指那些实施方式。

[0060] M1.一种方法,包括:

[0061] 提供数据处理装置(50),其中,数据处理装置(50)包括安全部(52),其中,安全部(52)包括不能从安全部(52)提取的私钥(13),其中,安全部(52)包括与私钥(13)对应的公钥(14),

[0062] 数据处理装置提供签署请求(15)、公钥(14)和序列号(12),

[0063] 基于签署请求(15)、公钥(14)和签署请求(15),外部数据处理装置(60)生成签署的数字证书(16),以及

[0064] 将所签署的数字证书(16)提供给数据处理装置(50)。

[0065] M2.根据前述实施方式所述的方法,其中,安全部(11)包括不能从安全部(52)提取的随机数生成器(11),其中,所述方法包括:随机数生成器(11)生成序列号(12)。

[0066] M3.根据前述实施方式所述的方法,其中,基于来自随机数生成器(11)的输出来生

成私钥(13)。

[0067] M4.根据前述实施方式中任一项所述的方法,其中,数据处理装置(50)是智能卡。

[0068] M5.根据前述实施方式所述的方法,其中,智能卡具有近场通信功能。

[0069] M6.根据前述实施方式中任一项所述的方法,其中,所述方法包括:

[0070] 将签署的数字证书(16)提供给数据处理系统(70),

[0071] 数据处理系统(70)从用户(80)接收个人用户数据(82),

[0072] 将公共证书密钥(34)提供给数据处理系统(70),

[0073] 数据处理系统(70)基于个人用户数据(82)、签署的数字证书(16)和公共证书密钥(34)来生成使用公共证书密钥(34)签署的签署的数字系统证书(36),

[0074] 将签署的数字系统证书(36)提供给数据处理装置(50)。

[0075] M7.根据前述实施方式所述的方法,其中,所述方法包括:

[0076] 生成公共证书密钥(34)和对应的私有证书密钥(33),

[0077] 使用公钥(14)对私有证书密钥(33)进行加密,从而生成包装的密钥(40),以及

[0078] 将包装的密钥(40)提供给数据处理装置的安全部(52)。

[0079] M8.根据前述实施方式所述的方法,其中,

[0080] 由数据处理系统(70)执行以下操作:生成公共证书密钥(34)和对应的私有证书密钥(33),使用公钥(14)对私有证书密钥(33)进行加密,从而生成包装的密钥(40),以及将包装的密钥(40)提供给数据处理装置的安全部(52),并且其中,包装的密钥(40)从数据处理系统(70)被提供给数据处理装置(50)的安全部(52)。[图2a]

[0081] M9.根据倒数第二实施方式所述的方法,其中,

[0082] 由另一数据处理系统(72)执行以下操作:生成公共证书密钥(34)和对应的私有证书密钥(33),使用公钥(14)对私有证书密钥(33)进行加密,从而生成包装的密钥(40),以及将包装的密钥(40)提供给数据处理装置的安全部(52),

[0083] 其中,所述方法还包括:将公钥(14)从数据处理装置(50)提供给另一数据处理系统(72),

[0084] 其中,将公共证书密钥(34)提供给数据处理系统(70)包括:将公共证书密钥(34)从另一数据处理系统(72)提供给数据处理系统(70)。

[0085] [图2b]

[0086] M10.根据三个前述实施方式中任一项所述的方法,其中,所述方法包括:

[0087] 在安全部(52)中,使用私钥(13)对包装的密钥(40)进行解密,从而获得私有证书密钥(33)。

[0088] M11.根据前述实施方式所述的方法,其中,所述方法包括:

[0089] 在安全部(52)中,基于私有证书密钥(33)来生成种子(21)。

[0090] 下面,将讨论初始化实施方式。通过字母I后跟数字来简写这些实施方式。每当在本文中提及初始化实施方式时,都意指那些实施方式。

[0091] I1.一种用于初始化数据处理装置(50)的初始化方法,所述数据处理装置(50)包括安全部(52),其中,所述初始化方法包括:

[0092] 在远程签名系统(20)中生成包括远程私钥(200)和远程公钥(202)的远程非对称密钥对(200、202),

[0093] 将远程公钥(202)提供给数据处理装置的安全部(52),以及

[0094] 生成签署凭证(220),其中,远程签名系统(20)被配置成:在接收到签署凭证(220)时签署数据结构。

[0095] I2.根据前述实施方式所述的初始化方法,其中,签署凭证(220)由远程签名系统(20)生成。

[0096] I3.根据两个前述实施方式中任一项所述的初始化方法,还包括:将签署凭证(220)提供给数据处理装置(50),例如将签署凭证(220)提供给数据处理装置(50)的安全部(52)。

[0097] C1.一种组合方法,其中,该组合方法包括根据前述方法实施方式中任一项所述的方法和根据前述初始化实施方式中任一项所述的初始化方法,其中,所述方法的数据处理装置(50)是初始化方法的数据处理装置(50)。

[0098] 应当理解,所述方法的安全部是初始化方法的安全部。

[0099] 下面,将讨论装置实施方式。通过字母A后跟数字来简写这些实施方式。每当在本文中提及装置实施方式时,都意指这些实施方式。

[0100] A1.一种数据处理装置(50),包括安全部(52),

[0101] 其中,安全部(52)包括:

[0102] 私钥(13),

[0103] 未加密的私有证书密钥(33),以及

[0104] 基于私有证书密钥(33)生成的种子(21),

[0105] 其中,私钥(13)、未加密的私有证书密钥(33)和种子(21)不能从安全部(52)提取。

[0106] A2.根据前述实施方式所述的数据处理装置(50),其中,数据处理装置(50)包括签署的数字证书(16)。

[0107] A3.根据前述装置实施方式中任一项所述的数据处理装置(50),其中,安全部(52)包括随机数生成器(11)。

[0108] A4.根据前述装置实施方式中任一项所述的数据处理装置(50),其中,数据处理装置(50)是智能卡。

[0109] A5.根据前述实施方式所述的数据处理装置(50),其中,智能卡具有近场通信功能。

[0110] A6.根据具有实施方式A3的特征的前述实施方式中任一项所述的数据处理装置(50),其中,数据处理装置包括由随机数生成器(11)生成的序列号(12)。

[0111] A7.根据前述装置实施方式中任一项所述的数据处理装置(50),其中,数据处理装置(50)包括签署的数字系统证书(36),其中,签署的数字系统证书(36)是使用与私有证书密钥(33)对应的公共证书密钥(34)签署的,并且其中,签署的数字系统证书(36)基于个人用户数据(82)、签署的数字证书(16)和公共证书密钥(34)。

[0112] A8.根据前述装置实施方式中任一项所述的数据处理装置(50),其中,数据处理装置(50)是可获得的,并且优选地,数据处理装置(50)通过根据实施方式M11所述的方法而获得。

[0113] A9.根据前述装置实施方式中任一项所述的数据处理装置(50),其中,数据处理装置(50)被配置成:仅允许通过未加密的私有证书密钥(33)来签署通过从种子(21)得出的密

钥签署的数据结构。

[0114] A10.根据前述装置实施方式中任一项所述的数据处理装置(50),其中,数据处理装置(50)被配置成:仅允许通过私钥(13)来签署通过从种子(21)得出的密钥签署的数据结构。

[0115] A11.一种数据处理装置(50),其中,数据处理装置(50)包括安全部(52),其中,安全部(52)包括远程公钥(202)。

[0116] A12.根据前述实施方式所述的数据处理装置(50),其中,通过根据前述初始化实施方式中任一项所述的初始化方法来初始化数据处理装置(50)。

[0117] A13.根据实施方式A1至A10中任一项所述的数据处理装置(50),其中,安全部(52)包括远程公钥(202)。

[0118] A14.根据前述实施方式所述的数据处理装置(50),其中,通过根据实施方式C1所述的组合方法来获得数据处理装置(50)。

[0119] A15.根据四个前述实施方式中任一项所述的数据处理装置(50),其中,远程公钥(202)与存储在远程签名系统(20)中的远程私钥(200)对应。

[0120] A16.根据前述实施方式所述的数据处理装置(50),其中,数据处理装置(50)还包括签署凭证(20),以触发由远程签名系统(20)的签名。

[0121] N1.一种方法,其中,所述方法使用根据前述装置实施方式中任一项所述的数据处理装置(50),所述方法包括:

[0122] 安全部(52)接收签署请求(100),

[0123] 在安全部(52)中,生成至少一个签名(121、133、113、250),以及

[0124] 输出至少一个签名(121、133、113、250)。

[0125] N2.根据前述实施方式所述的方法,其中,所述方法使用根据具有实施方式A1的特征的前述装置实施方式中任一项所述的数据处理装置(50),其中,

[0126] 生成至少一个签名(121、133、113、250)包括:生成使用从种子(21)得出的私钥签署的签名(121)以及使用未加密的私有证书密钥(33)来签署签名(121),从而生成使用未加密的私有证书密钥(33)签署的签名(133),以及

[0127] 输出至少一个签名(121、133、113、250)包括:输出使用从种子(21)得出的私钥签署的签名(121)和使用未加密的私有证书密钥(33)签署的签名(133)。

[0128] N3.根据前述实施方式所述的方法,其中,所述方法还包括:

[0129] 在安全部(52)中,使用私钥(13)来签署签名(121),从而生成使用私钥(13)签署的签名(113),

[0130] 将使用私钥(13)签署的签名(113)以及使用从种子(21)得出的私钥签署的签名(121)和使用未加密的私有证书密钥签署的签名(133)一起输出。

[0131] N4.根据两个前述实施方式中任一项所述的方法,其中,所述方法使用根据具有实施方式A2的特征的前述装置实施方式中任一项所述的数据处理装置(50),

[0132] 其中,所述方法还包括:将签署的数字证书(16)以及使用从种子(21)得出的私钥签署的签名(121)和使用未加密的私有证书密钥签署的签名(133)一起输出。

[0133] N5.根据三个前述实施方式中任一项所述的方法,其中,所述方法使用根据具有实施方式A7的特征的前述装置实施方式中任一项所述的数据处理装置(50),

[0134] 其中,所述方法还包括:将签署的数字系统证书(36)以及使用从种子(21)得出的私钥签署的签名(121)和使用未加密的私有证书密钥签署的签名(133)一起输出。

[0135] N6.根据五个前述实施方式中任一项所述的方法,其中,所述方法使用根据具有实施方式A11或A13的特征的前述装置实施方式中任一项所述的数据处理装置,其中,所述方法还包括:

[0136] 远程签名系统(20)接收签署请求(100),

[0137] 远程签名系统(20)使用与远程公钥(202)对应的远程私钥(200)对签署请求(100)进行签署,从而生成预签名(210);

[0138] 安全部(52)接收预签名(210),以及

[0139] 在安全部(52)中使用远程公钥(202)验证预签名(210)是使用远程私钥(200)签署的签署请求(100),

[0140] 其中,根据使用远程公钥(202)成功验证预签名(210)是使用远程私钥(200)签署的签署请求(100),在安全部(52)中生成至少一个签名(121、133、113、250)并输出所述至少一个签名(121、133、113、250)。

[0141] N7.根据前述实施方式所述的方法,

[0142] 其中,所述方法还包括:远程签名系统(20)接收签署凭证(220),

[0143] 其中,根据远程签名系统(20)接收到签署凭证(220),远程签名系统(20)使用与远程公钥(202)对应的远程私钥(200)对签署请求(100)进行签署,从而生成预签名(210)。

[0144] N8.根据两个前述实施方式中任一项所述的方法,

[0145] 其中,所述方法还包括:禁用远程签名系统(20)使用远程私钥(200)进行签署的能力。

附图说明

[0146] 现在将参照附图来描述本技术的实施方式,并且实施方式应当被理解为说明而非限制本技术的范围。

[0147] 图1描绘了根据本技术的实施方式的数据处理装置的设置;

[0148] 图2a描绘了根据本技术的实施方式的数据处理装置的初始化;

[0149] 图2b描绘了根据本技术的另一实施方式的数据处理装置的另一初始化;

[0150] 图3更详细地描绘了本技术的实施方式的初始化的步骤;

[0151] 图4描绘了根据本技术的实施方式的签署过程;

[0152] 图5描绘了与图1对应的数据处理装置的设置的流程图;

[0153] 图6描绘了与图2a或图2b和图3对应的数据处理装置的初始化的流程图;

[0154] 图7描绘了与图5对应的签署过程的流程图;

[0155] 图8描绘了根据本技术的实施方式的数据处理装置的另一初始化(其可以与图2a/图2b的初始化一起使用或独立于图2a/图2b的初始化被使用);

[0156] 图9描绘了根据本技术的实施方式的签署过程;以及

[0157] 图10描绘了根据本技术的实施方式的另一签署过程。

具体实施方式

[0158] 图1描绘了可以被实现为智能卡(例如,具有近场通信(NFC)功能的智能卡)的数据处理装置50。在下文中,还将提及智能卡50,但是技术人员将理解,数据处理装置50也可以以与智能卡不同的方式来实现,而与是提及智能卡还是数据处理装置无关。在其初始化之前,数据处理装置50也可以被称为原始或本地数据处理装置50。

[0159] 数据处理装置50包括安全部52,该安全部52也可以被称为安全飞地(secure enclave)52。安全部52可以提供硬件和软件保护,用于保持安全部52中的数据的保密性。更具体地,数据处理装置50(例如,智能卡)可以被编程,使得只有所定义的数据可以离开安全部52,而其他数据不能离开安全部52。安全部52可以包括一个或更多个安全微控制器和一个或更多个安全存储器部件。

[0160] 安全部52包括随机数生成器11(并且应当理解,该术语还包括伪随机数生成器)。

[0161] 在第一步骤S1(也参见图5)中,随机数生成器11生成随机序列号12。此外,在步骤S2中,在安全部52中生成私钥13和公钥14对。密钥13、14是非对称密码密钥。这可以基于由随机数生成器11生成的随机数,并且应当理解,步骤S2是在步骤S1之后执行还是在步骤S1之前执行并不重要。数据处理装置50被配置成使得不能从安全部52提取私钥13。

[0162] 在另一步骤S3中,随机序列号12、公钥14和签署请求15被提供至外部数据处理装置60,并且在步骤S4中,外部数据处理装置60例如通过使用根证书来生成并签署数字证书16。

[0163] 数字证书16可以是X509数字证书并且由外部数据处理装置60的根证书签署。数字证书16包含序列号12、公钥14,并且还可以包含与数据处理装置50的类型有关的信息。数字证书16可以提供与卡上数字签名和解密相关的功能。

[0164] 在另一步骤S5中,数字证书16被提供给数据处理装置50。在该步骤之后,数据处理装置50的序列号12是唯一的,并且由于数字证书16而不能被伪造。

[0165] 应当理解,结合图1描述的步骤S1至S5通常涉及数据处理装置50(例如智能卡50)的工厂设置。

[0166] 如图2a和图6所描绘的,在步骤T1中,可以通过使用数据处理系统70来验证用户80的身份,数据处理系统70也可以被称为第三方认证系统70或第三方认证机构70。应当理解,数据处理系统70通常包括处理器和存储数据的存储器。在身份验证过程期间,用户可以向数据处理系统70提供个人数据82。

[0167] 在另一步骤T2中,数据处理系统70生成公共证书密钥34和私有证书密钥33对。应当理解,这些密钥是正常的非对称密码密钥,并且这些密钥是“证书”密钥的规范应当仅将它们与密钥13和14区分开。因此应当理解,证书密钥33、34与密钥13、14不同。

[0168] 在步骤T3中,提供公共证书密钥34和个人用户数据82,此外,提供所签署的数字证书16(后者来自数据处理装置50),并且基于此生成证书签署请求90。在所描绘的实施方式中,该步骤T3在数据处理系统70中被执行。然而,应当理解,该步骤T3也可以在数据处理系统70外部被执行。

[0169] 可以在数据处理系统70中执行另一步骤T4,其中,步骤T4可以包括不同的子步骤。在子步骤T4a中,可以验证数字证书16的真实性。在子步骤T4b中,可以生成使用公共证书密钥34签署的数字证书36,其将被称为数字系统证书36(仅为了将其术语与数字证书16区分

开)。数字系统证书36可以包括个人用户数据82(例如,用户的姓名、用户的护照ID和/或用户的地址)、公共证书密钥34和所签署的数字证书16。在子步骤T4c中,可以使用公钥14对私有证书密钥33进行加密,从而生成包装的(或加密的)私有证书密钥40(在这方面,需要注意的是,公钥14包含在所签署的数字证书16中并因此也包含在证书签署请求90中)。

[0170] 在步骤T5中,将包装的私有证书密钥40和数字系统证书36提供给数据处理装置50。

[0171] 然而,尽管在图2a所描绘的实施方式中描述了由数据处理系统70执行的许多功能,但是应当理解,这仅仅是示例性的,并且这些功能和步骤也可以由不同的系统来执行。这在图2b中示例性地被描绘。图2b中所描绘的实施方式的功能大部分对应于图2a中所描绘的实施方式的功能。然而,图2b中的实施方式包括另一数据处理系统72,并且一些功能在该另一数据处理系统72中被实现,该另一数据处理系统72通常包括处理器和存储器。附加数据处理系统72可以是例如硬件安全模块。

[0172] 具体地,另一数据处理系统72可以生成公共证书密钥34和私有证书密钥33对(即,步骤T2,参见图6),并且公共证书密钥34可以被提供给数据处理系统70。在数据处理系统70中,公共证书密钥34被用来生成证书签署请求90(步骤T3)并生成使用公共证书密钥34签署的数字系统证书36(如先前所讨论的)。此外,该数字证书密钥然后可以被提供给数据处理装置50。

[0173] 此外,可以将公钥14从数据处理装置50提供给附加数据处理系统72(其中,应当理解的是,可以从数据处理装置50的安全部52中提取公钥14)。此外,在附加数据处理系统72中,可以使用公钥14来包装(即,加密)私有证书密钥33(子步骤T4c),从而生成包装的私有证书密钥40,然后可以将该包装的私有证书密钥40提供给数据处理装置(步骤T5的一部分)。

[0174] 图3描绘了数据处理装置50的放大部分,以进一步说明在处理装置50接收到包装的证书密钥40之后执行的附加步骤。如所描绘的,包装的证书密钥40被提供给数据处理装置50的安全部52。

[0175] 在安全部52中执行的步骤T6中,借助于私钥13对包装的证书密钥40进行解密,从而得出不能从安全部52中提取的未加密的私有证书密钥33。在安全部52中执行的步骤T7中,基于未加密的私有证书密钥33,生成种子21。例如,可以经由数据处理装置50的安全部52内部的硬编码秘密得出函数从未加密的私有证书密钥33生成种子21。例如,种子21可以是BIP32种子,并且可以通过多个SHA256和AES加密算法来得出种子21。

[0176] 因此,在完成步骤T7之后,在数据处理装置50的安全部52中存在种子21。

[0177] 通常,应当理解,步骤T1至T7可能涉及数据处理装置的初始化。通过初始化,数据处理装置50可以配备有附加的功能。

[0178] 例如,可以如结合图4和图7所讨论的那样使用数据处理装置50。

[0179] 在步骤U1中,签署请求100被提供给数据处理装置50,更具体地,被提供给数据处理装置50的安全部52。例如,签署请求100可以是与区块链网络上的交易有关的签署请求100或者与智能合约有关的签署请求。

[0180] 在步骤U2中,相应的签署请求得到满足,即,用于该请求的相应签名121被生成。基于签署请求100和从种子21得出的私钥来生成签名121,并且应当理解,不能从安全部52中

提取种子21和从种子21得出的私钥二者。

[0181] 在步骤U3中,还使用私有证书密钥33来签署签名121并因此生成证书签名133,该证书签名133是使用私有证书密钥33签署的签名121。

[0182] 在步骤U4中,还可以使用私钥13来签署签名121并因此可以生成密钥签名133,该密钥签名133是使用私钥13签署的签名121。

[0183] 数据处理装置50可以被配置成(例如,硬编码成)使得私有证书密钥33和私钥13可以仅用于对先前通过从种子21得出的密钥签署的数据结构进行签署。

[0184] 在步骤U5中,签名121、证书签名133和密钥签名113(如果存在)可以从数据处理装置50被输出,例如,这些数据可以被广播并且可以被提供给例如区块链节点以引起区块链交易。然而,应当理解,本技术不限于区块链实现,而是还可以结合例如智能合约、时间戳或合规数据来使用。

[0185] 应当理解,种子21是基于私有证书密钥33(参见图3)生成的。因此,仅当数据处理装置50已经如前所述被初始化时才能生成所签署的交易签名121(否则,数据处理装置50将无法访问种子21)。这也适用于所签署的交易签名133和113,因为它们基于所签署的交易签名121(基于种子21,种子21又基于适当的初始化)。对于所签署的交易签名133,对正确初始化的依赖性还由被私有证书密钥33签署的交易签名133引起,私有证书密钥33也仅在成功初始化之后才出现在数据处理装置50上。

[0186] 如所讨论的,数据处理装置50可以被配置成使得它可以仅签署数字签名(例如,生成签名121、133和113),而不签署与数字签名不同的数据结构。此外,数据处理装置50还可以被配置成使得私有证书密钥33和私钥13可以仅用于签署已经通过从种子21得出的密钥签署的签名。通过限制可以签署数据结构的能力,可以大大降低伪造的风险。

[0187] 此外,应当理解,数据处理装置50还可以输出所签署的数字证书16和/或使用公钥34签署的数字系统证书36。

[0188] 下面参照图8和图10来描述本技术的其他实施方式。

[0189] 应当理解,图8是用于初始化数据处理装置50的初始化过程。还应当理解,结合图8所讨论的初始化步骤可以是结合图2a或图2b所讨论的附加的初始化步骤。也就是说,技术人员将理解,除了参照图2a和/或图2b所描述的步骤之外,还可以执行参照图8所描述的步骤。然而,也可以独立于结合图2a和图2b描述的步骤来执行结合图8所讨论的初始化步骤。

[0190] 图9和图10描绘了可以使用以图8中描绘的步骤初始化的数据处理装置50来执行的签署过程。

[0191] 更具体地,图10描绘了通常与参照图4所讨论的签署过程对应的签署过程,但包括附加特征。应当理解,图10中所描绘的签署过程是基于图10的具有附加步骤的签署过程,如下面将讨论的。

[0192] 图8再次描绘了数据处理装置50,该数据处理装置50可以是以前所讨论的数据处理装置,更具体地,图8再次描绘了数据处理装置50的初始化步骤。此外,图8还描绘了远程签名系统20。远程签名系统20生成包括远程私钥200和远程公钥202的远程非对称密钥对。应当理解,远程私钥200和远程公钥202中的术语“远程”不应当限制这些密钥的特性,而是将这些密钥200、202与本说明书中使用的其他密钥区分开。在生成这些远程密钥200、202之后,将远程公钥202从远程签名系统20发送至数据处理装置50,更具体地,发送至数据处理

装置50的安全部52。

[0193] 此外,生成与远程密钥200、202对应的签署凭证220,并且还将签署凭证220发送至例如数据处理装置50。例如,签署凭证可以被存储在数据处理装置50的安全部52中。然而,应当理解,这仅是示例性的,并且签署凭证220也可以不存在于数据处理装置50上,而是可以例如被存储在别处。

[0194] 在图8中,描绘了签署凭证220和远程公钥202被分别发送至数据处理装置50。然而,应当理解,这仅仅是示例性的,并且签署凭证220和远程公钥202也可以同时被发送。此外,应当理解,参照图8所描述的步骤也涉及初始化,还应当理解,签署凭证220和远程公钥202也可以与包装的私有证书密钥40同时被发送(如果使用图2a和/或图2b的初始化)。

[0195] 当稍后向远程签名系统20提供签署凭证220时,远程签名系统20将签署所提供的数据结构(例如,交易请求)。

[0196] 应当理解,除了结合图2a/图2b和图3所讨论的步骤之外,还可以执行图8所描绘的步骤(例如,在图2a/图2b和图3的步骤之前、同时或之后),然而,它们也可以独立地被执行。如果除了结合图2a/图2b和图3所讨论的步骤之外还执行图8的步骤,则已经经历组合的初始化过程的数据处理装置50包括数字系统证书36和远程公钥202以及(在安全部52中)未包装的私有证书密钥33、种子21和签署凭证220。

[0197] 在图9中描绘了用于生成签名的另一实施方式。应当理解,图9中所描绘的实施方式的一些步骤与图4中所描绘的步骤对应,并且在图4和图9中使用对应的附图标记。

[0198] 更具体地,图9描绘了使用包括结合图8所讨论的步骤的初始化过程初始化的数据处理装置50的签名生成。

[0199] 因此,数据处理装置50具有安全部52,并且远程公钥202被存储在安全部52中。此外,在图9中所描绘的签名生成中使用签署凭证220。签署凭证220可以例如被存储在数据处理装置50的安全部52中。然而,应当理解,这是可选的。

[0200] 如图9所描绘的,签名过程使用签署请求100。签署请求100被提供给远程签名系统20。此外,签署凭证220被提供给远程签名系统20。在所描绘的实施方式中,签署凭证220从数据处理装置50的安全部52被提供给远程签名系统20。然而,应当理解,这仅仅是示例性的,并且签署凭证220也可以以不同的方式被提供给远程签名系统20。

[0201] 远程签名系统20包括远程私钥200。应当理解,远程私钥200中的术语“远程”不应当限制该私钥200的特性,而是将该私钥200与本说明书中使用的其他私钥区分开。

[0202] 在接收到正确的签署凭证220之后,远程签名系统20基于签署请求100和远程私钥200来生成预签名210,从而生成预签名210,该预签名210是由远程私钥200签署的签署请求。因此,将理解的是,预签名210的生成取决于正确的签署凭证220的接收。

[0203] 因此,签署凭证220指示远程签名系统20应当提供预签名210。

[0204] 在所描绘的实施方式中,将签署凭证220从数据处理装置50提供给远程签名系统20。更具体地,签署凭证220被存储在数据处理装置50的安全部52中。然而,应当理解,这仅仅是示例性的,并且签署凭证220也可以被存储在例如另一装置上,并且从这样的其他装置被提供给远程签名系统20。

[0205] 预签名210被发送至数据处理装置50,更具体地,被发送至数据处理装置50的安全部52。此外,签署请求100也被提供给数据处理装置的安全部52。例如,签署请求100可以从

远程签名系统10被发送至数据处理装置50的安全部52。然而,应当理解,这仅仅是示例性的,并且签署请求100也可以以不同的方式被提供给数据处理装置50的安全部52。

[0206] 数据处理装置50的安全部52包括与远程私钥200对应的远程公钥202。通过远程公钥202,数据处理装置50确定预签名210是否有效,即,签署请求100是否已经由远程私钥200签署。

[0207] 如果是这种情况,则基于签署请求100和签名例程来生成至少一个签名250。例如,一起由附图标记260表示的至少一个签名密钥和/或种子可以用于在安全部52中生成至少一个签名250。所述至少一个签名250可以被广播并且可以被提供给例如区块链节点110以引起区块链交易。然而,应当理解,本技术不限于区块链实现,而是还可以结合例如智能合约、时间戳或合规数据来使用。

[0208] 因此,结合图8和图9所描述的实施方式允许不同的密钥管理。通过结合图8和图9所描述的实施方式,远程签名系统20也用于签署。

[0209] 因此,例如在数据处理装置50丢失的情况下,远程签名系统20可以用于锁定数据处理装置50的签署功能。换句话说,可以抑制对远程签名系统20的访问,或者使用远程密钥对200、210,从而安全地锁定数据处理装置50的功能。应当理解,这允许暂时地或永久地锁定数据处理装置50的功能。

[0210] 例如,在以上述方式初始化的数据处理装置50丢失的情况下,可以在远程签名系统20处抑制相应的远程密钥对200、210。因此,可能不再使用数据处理装置50。

[0211] 此外,可以以相同的方式(特别是利用相同的种子21)但是利用新的远程密钥对200、210来设置和初始化新的数据处理装置50。因此,可以设置和初始化对应的数据处理装置50。

[0212] 总之,该实施方式因此允许数据处理装置50被远程激活、去激活,例如暂时地被阻止或明确地被阻止,以及被替换而无需替换种子。

[0213] 图10描绘了通常与图9中描绘的签名生成对应的签名生成的实施方式。然而,在该实施方式中,描绘了签名例程的更多细节。

[0214] 也就是说,图10中的实施方式是图9中所讨论的实施方式的一个可能的实现,其中讨论了签名例程的更多细节。

[0215] 特别地,应当理解,直到确定预签名210的有效性的点为止,图10中所描绘的过程与图9中所描绘的过程相同,因此可以参考直到该点为止的图9的描述。

[0216] 如果是这种情况,即,当确定签署请求100已经由远程私钥200签署时,签署请求100经受包括先前参照图4描述的步骤的签名例程。

[0217] 换句话说,图10描绘了图9(直到确定签署请求100已经由远程私钥签署为止)和图4(从向安全部提供签署请求100开始)的实施方式的组合。

[0218] 因此,可以组合上面参照图4和图9描述的优点。每当在本说明书中使用诸如“大约”、“基本上”或“大概”的相对术语时,这样的术语还应被解释为还包括确切的术语。也就是说,例如,“基本上直的”应被解释为还包括“(精确地)直的”。

[0219] 每当在上面或此外在所附权利要求中叙述步骤时,应该注意的是,在本文中叙述步骤的顺序可能是偶然的。也就是说,除非另有说明或者除非对技术人员是清楚的,否则叙述步骤的顺序可能是偶然的。也就是说,当本文献陈述例如一种方法包括步骤(A)和步骤

(B)时,这不一定意指步骤(A)在步骤(B)之前,而是也有可能步骤(A)(至少部分地)与步骤(B)同时执行,或者步骤(B)在步骤(A)之前。此外,当步骤(X)据说在另一步骤(Z)之前时,这并不意味着在步骤(X)与步骤(Z)之间没有步骤。也就是说,步骤(Z)之前的步骤(X)涵盖步骤(X)在步骤(Z)之前直接被执行的情况,而且步骤(Z)之前的步骤(X)涵盖(X)在一个或更多个步骤(Y1)、.....、接着是步骤(Z)之前被执行的情况。相应的考虑在使用比如“之后”或“之前”的术语时适用。

[0220] 虽然在上文中,已经参照附图描述了优选实施方式,但是技术人员将理解的是,仅出于说明目的而提供了这些实施方式,并且这些实施方式决不应当被解释为限制通过权利要求限定的本发明的范围。

[0221]

11	随机数生成器
12	随机序列号
13	私钥
14	与私钥 13 对应的公钥
15	签署请求
16	所签署的数字证书
20	远程签名系统
21	用于私钥生成的种子
33	由认证装置生成的私钥，被称为私有证书密钥
34	与私钥 33 对应的公钥，被称为公共证书密钥
36	使用公钥 34 签署的数字证书
40	使用公钥 14 加密的私钥 33
50	数据处理装置，例如智能卡
52	安全部
60	外部数据处理装置

[0222]

70	数据处理系统
72	另一数据处理系统
80	用户
82	个人用户数据
90	证书签署请求
100	签署请求
110	区块链节点
113	进一步使用私钥 33 签署的交易签名 121
121	使用从种子 21 得出的私钥签署的交易签名
133	进一步使用私钥 13 签署的交易签名 121
200	远程私钥
202	远程公钥
210	预签名
220	签署凭证
250	至少一个签名
260	签名密钥和/或种子

[0223] 表:本说明书中所使用的附图标记

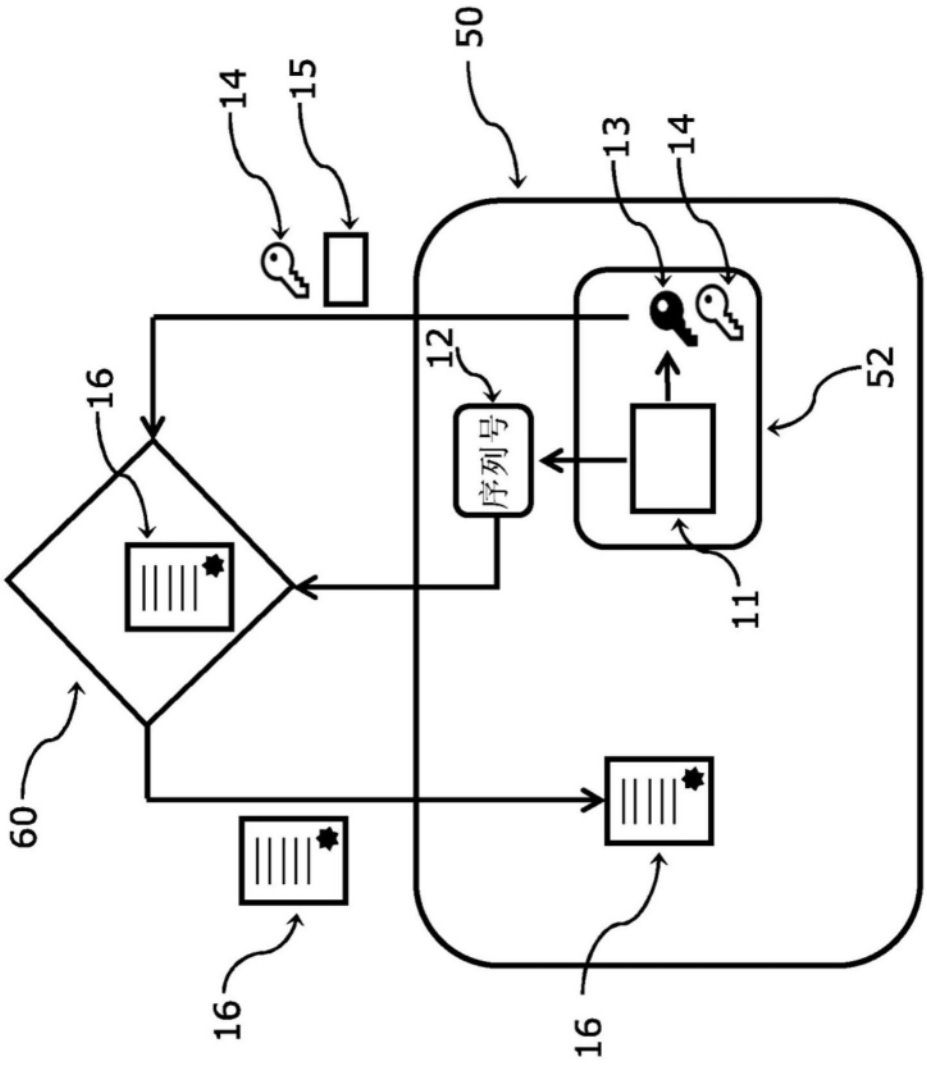


图1

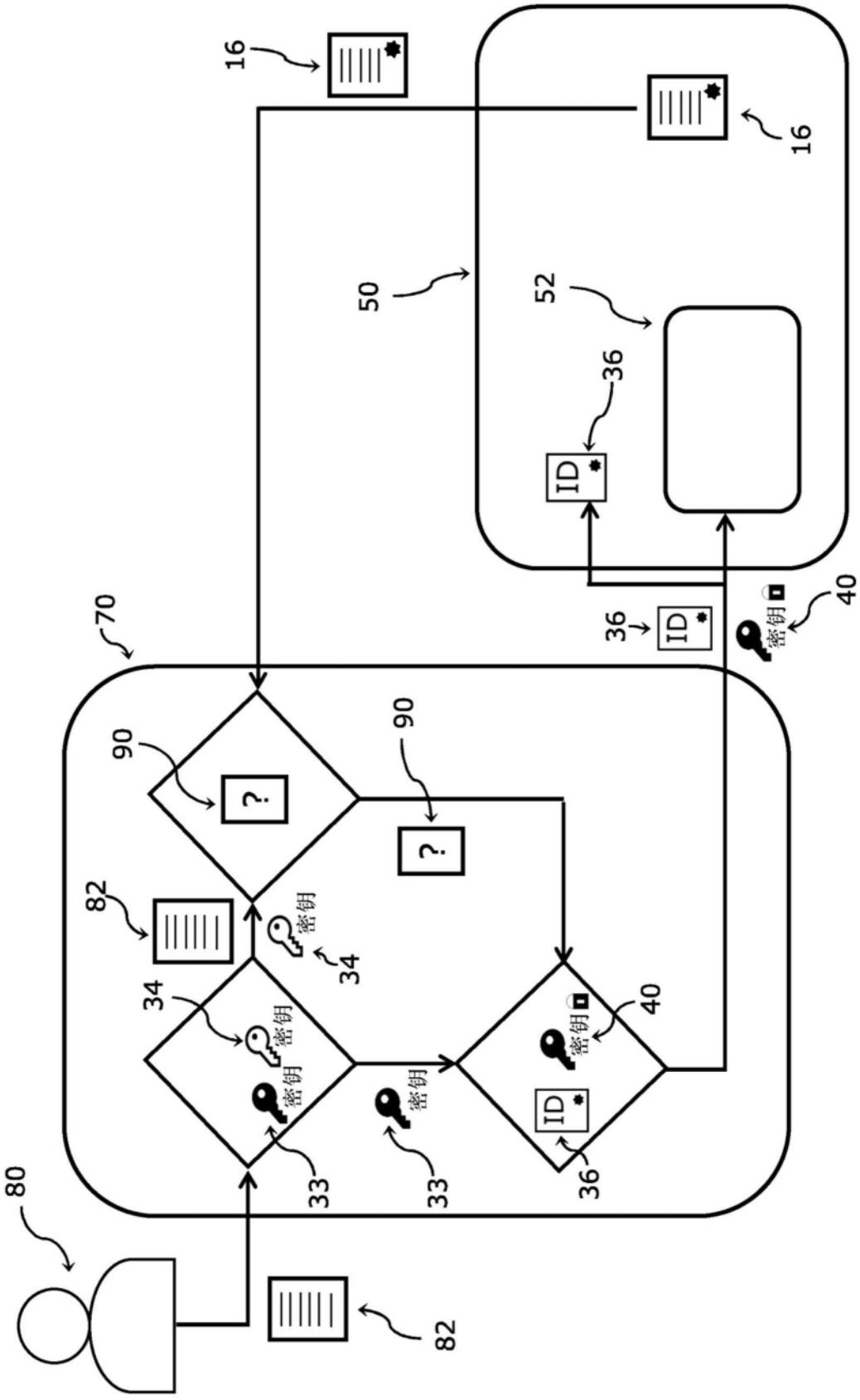

16
16
50
52
36
ID
36
ID
密钥
40
70
90
?
90
?
82
密钥
34
34
密钥
密钥
密钥
40
ID
33
33
36
80
82

图2a

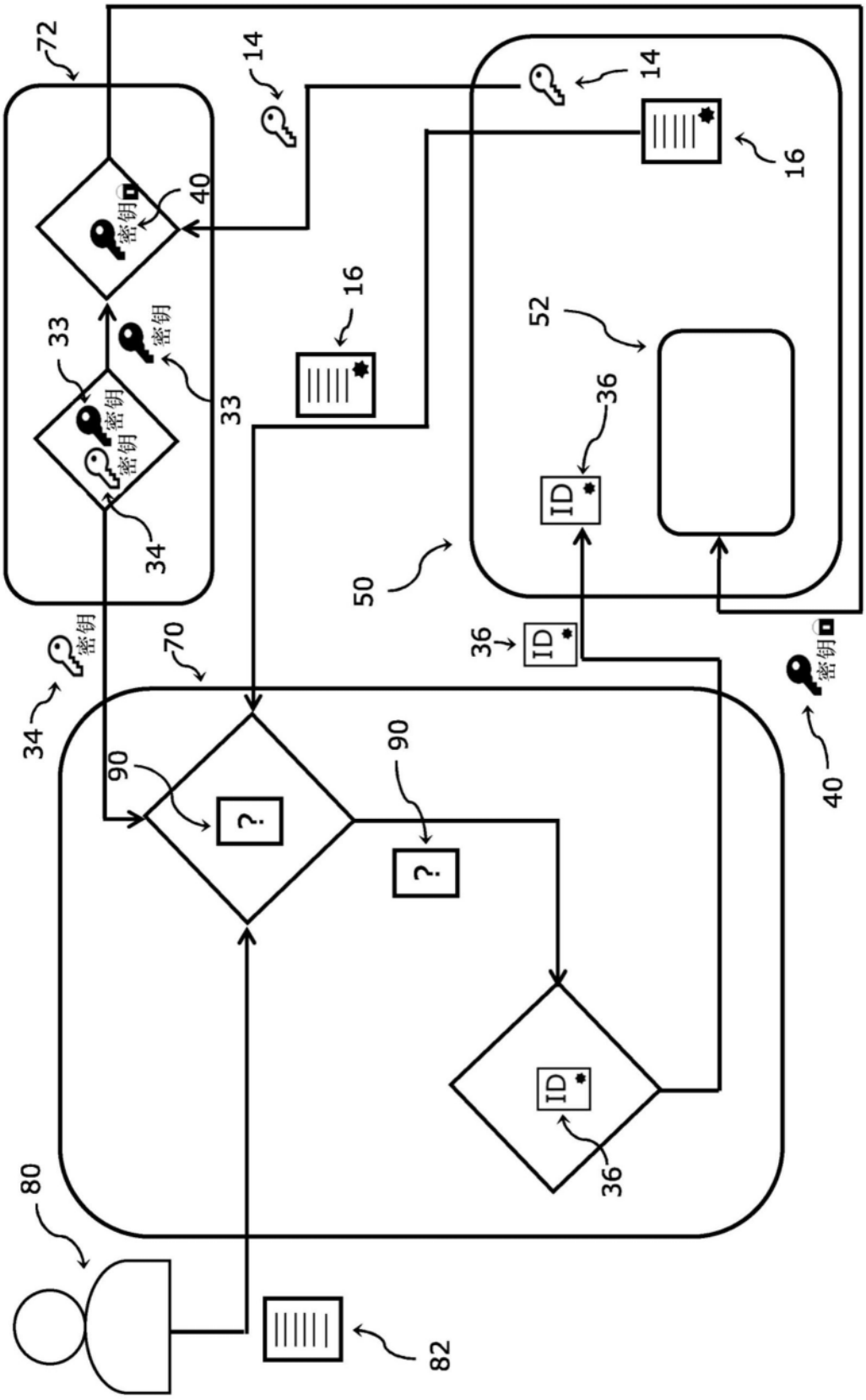

72
14
14
16
40
密钥
16
52
33
密钥
密钥
33
36
34
ID
50
密钥
70
36
ID
密钥
34
40
90
90
?
?
ID
36
80
82

图2b

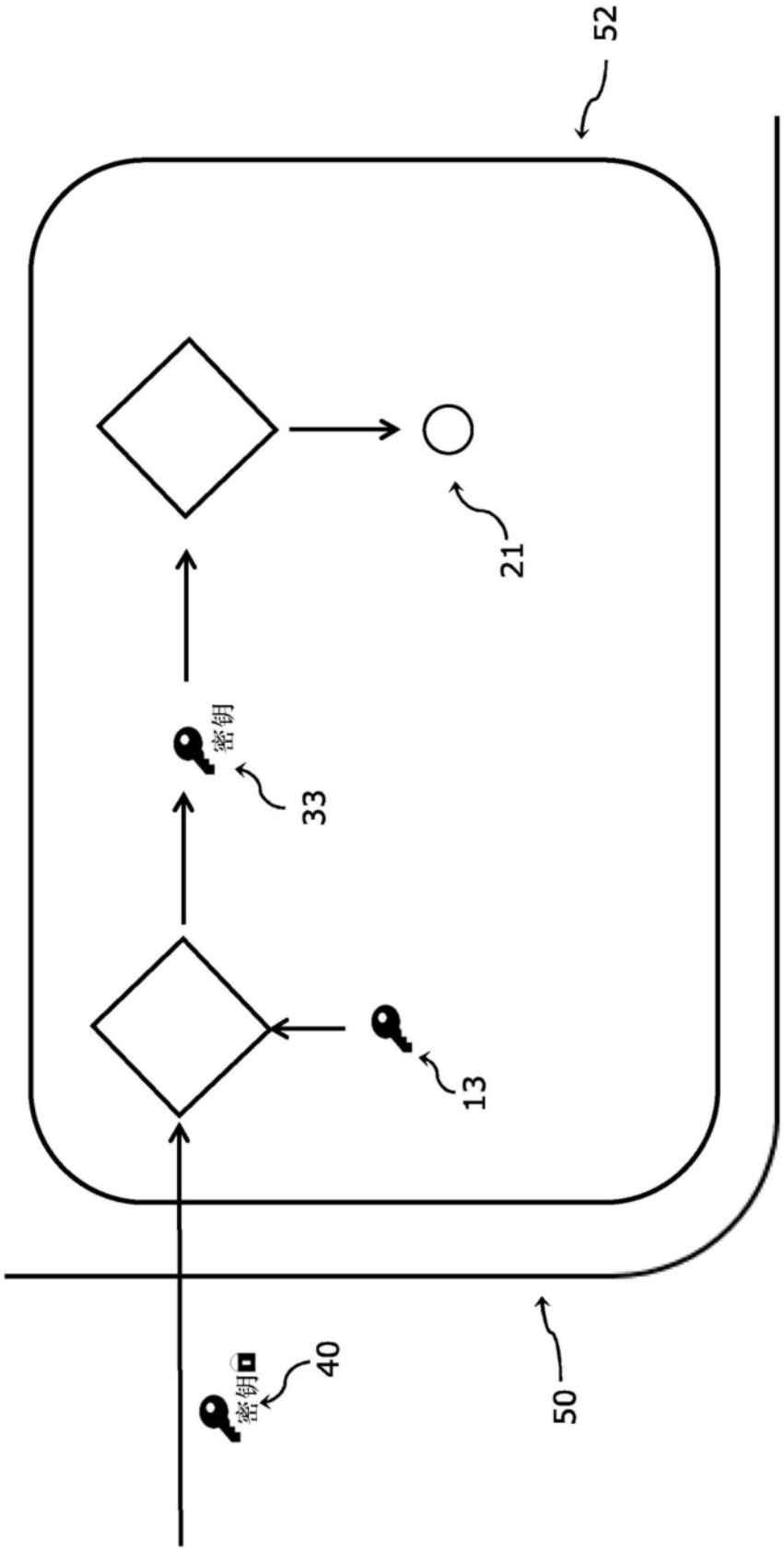


图3

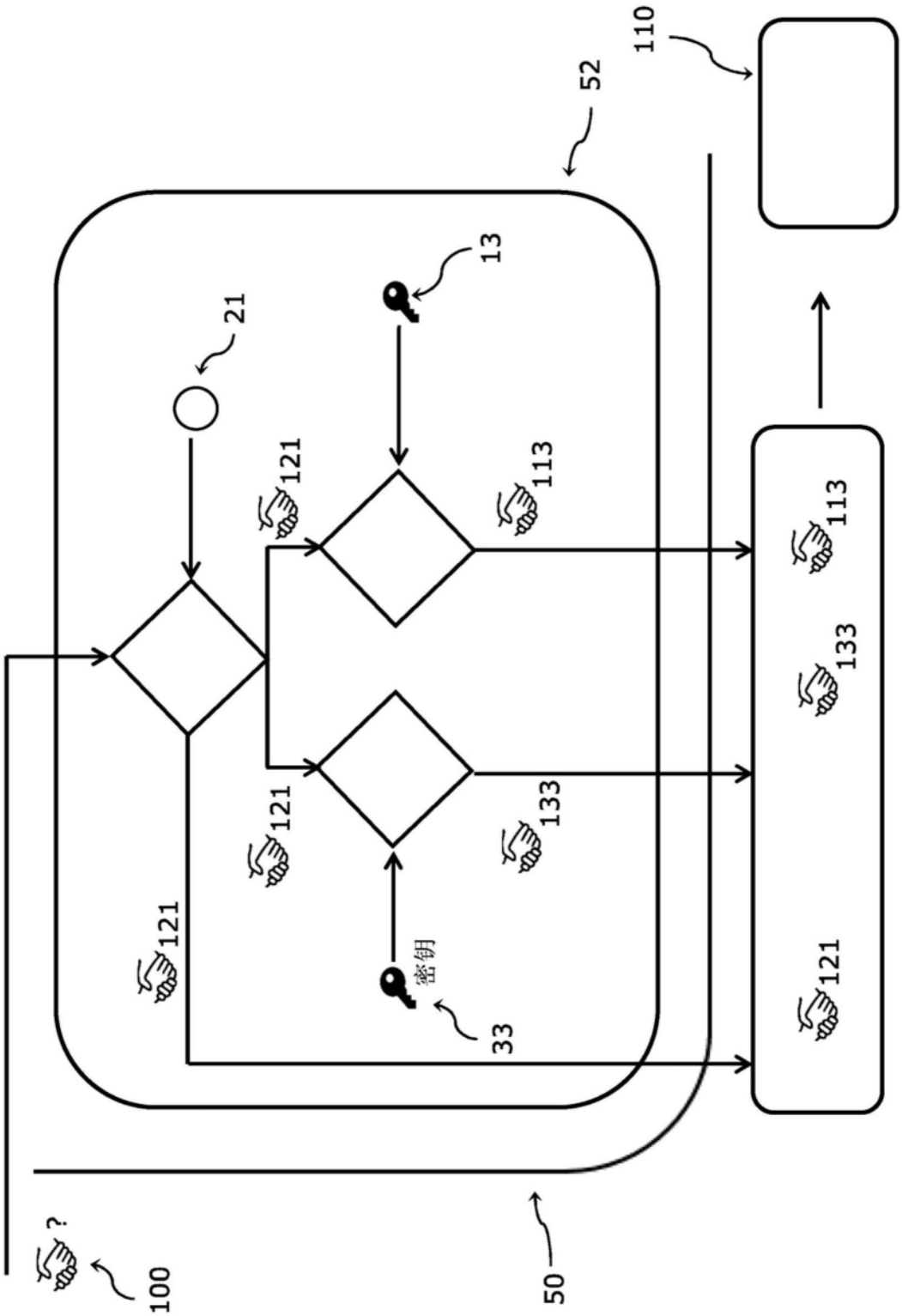


图4

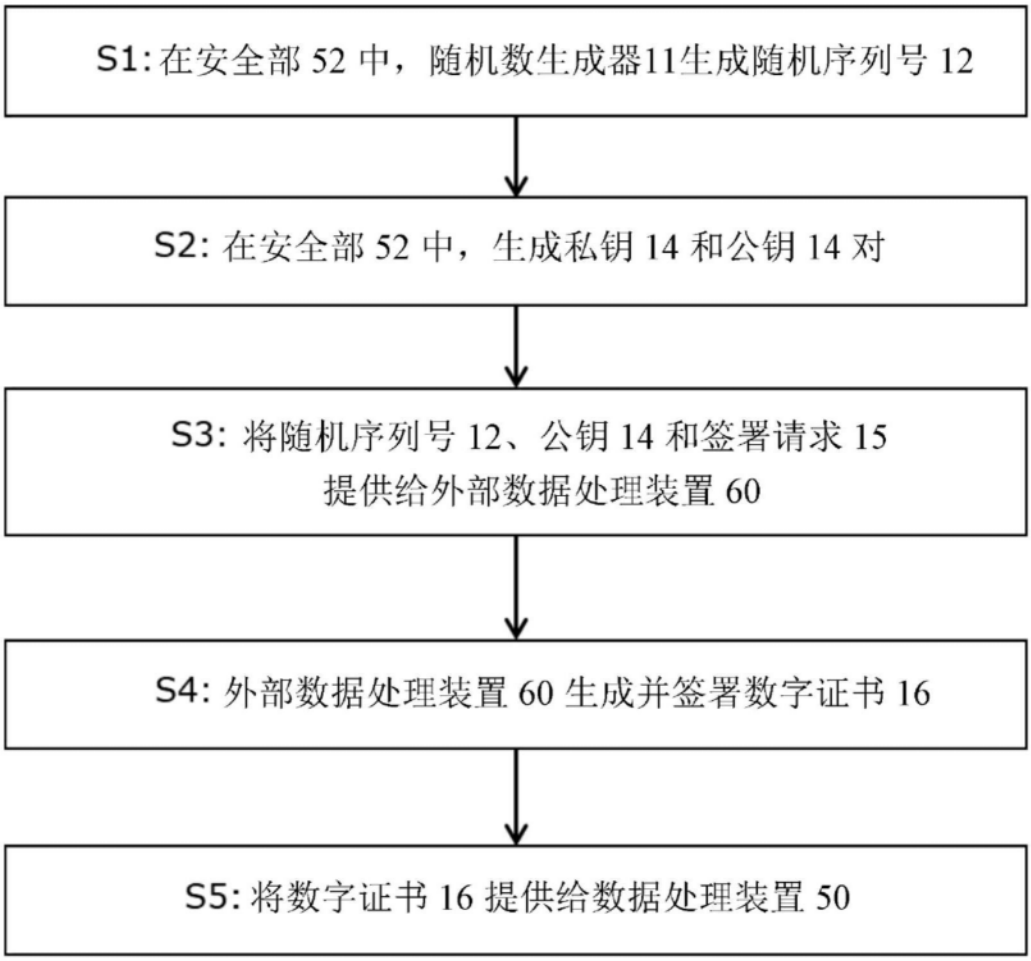

S1: 在安全部 52 中，随机数生成器11生成随机序列号 12
S2: 在安全部 52 中，生成私钥 14 和公钥 14 对
S3: 将随机序列号 12、公钥 14 和签署请求 15
提供给外部数据处理装置 60
S4: 外部数据处理装置 60 生成并签署数字证书 16
S5: 将数字证书 16 提供给数据处理装置 50

图5

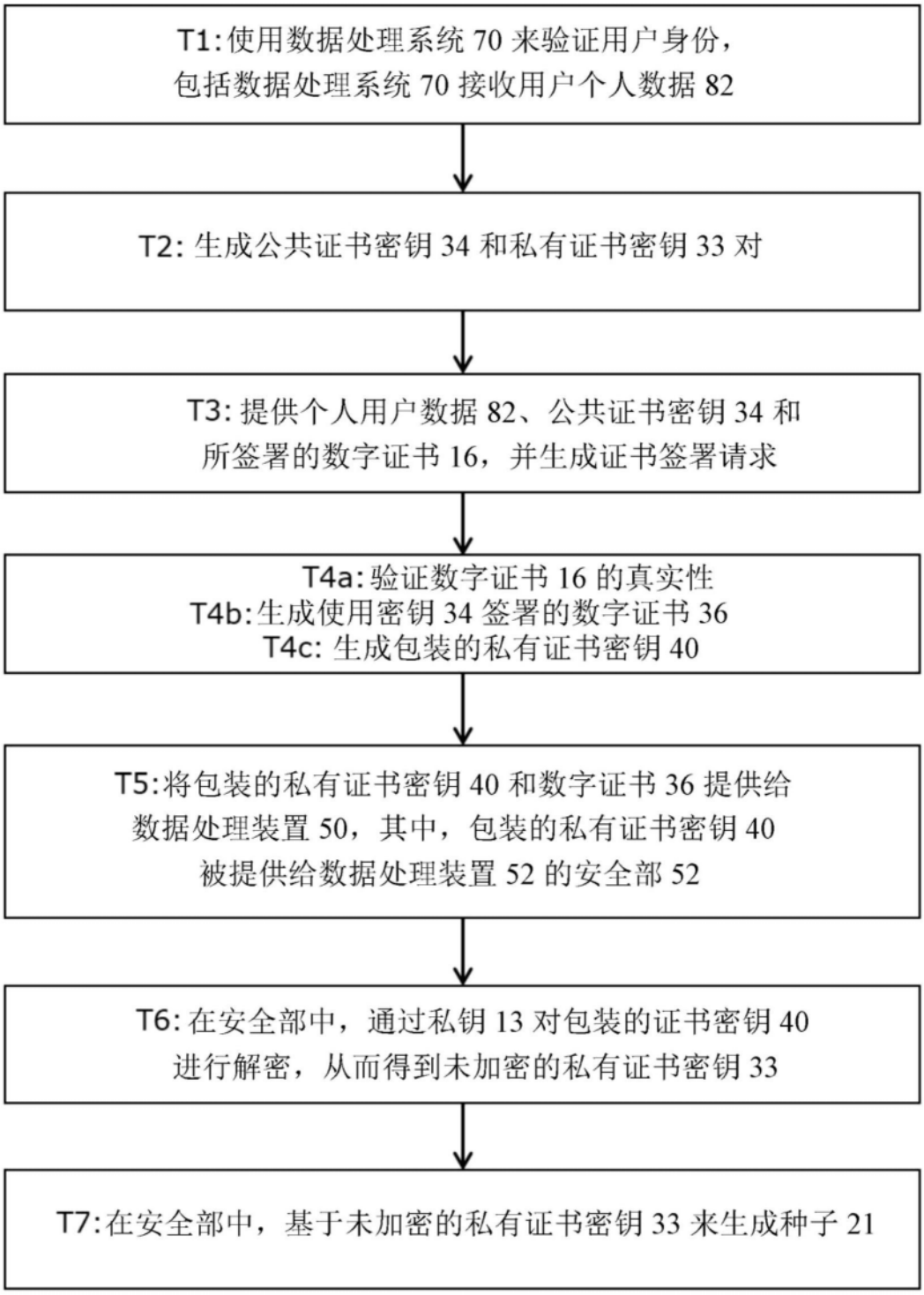

T1:使用数据处理系统 70 来验证用户身份，
包括数据处理系统 70 接收用户个人数据 82
T2: 生成公共证书密钥 34 和私有证书密钥 33 对
T3: 提供个人用户数据 82、公共证书密钥 34 和
所签署的数字证书 16，并生成证书签署请求
T4a:验证数字证书 16 的真实性
T4b:生成使用密钥 34 签署的数字证书 36
T4c: 生成包装的私有证书密钥 40
T5:将包装的私有证书密钥 40 和数字证书 36 提供给
数据处理装置 50，其中，包装的私有证书密钥 40
被提供给数据处理装置 52 的安全部 52
T6:在安全部中，通过私钥 13 对包装的证书密钥 40
进行解密，从而得到未加密的私有证书密钥 33
T7:在安全部中，基于未加密的私有证书密钥 33 来生成种子 21

图6

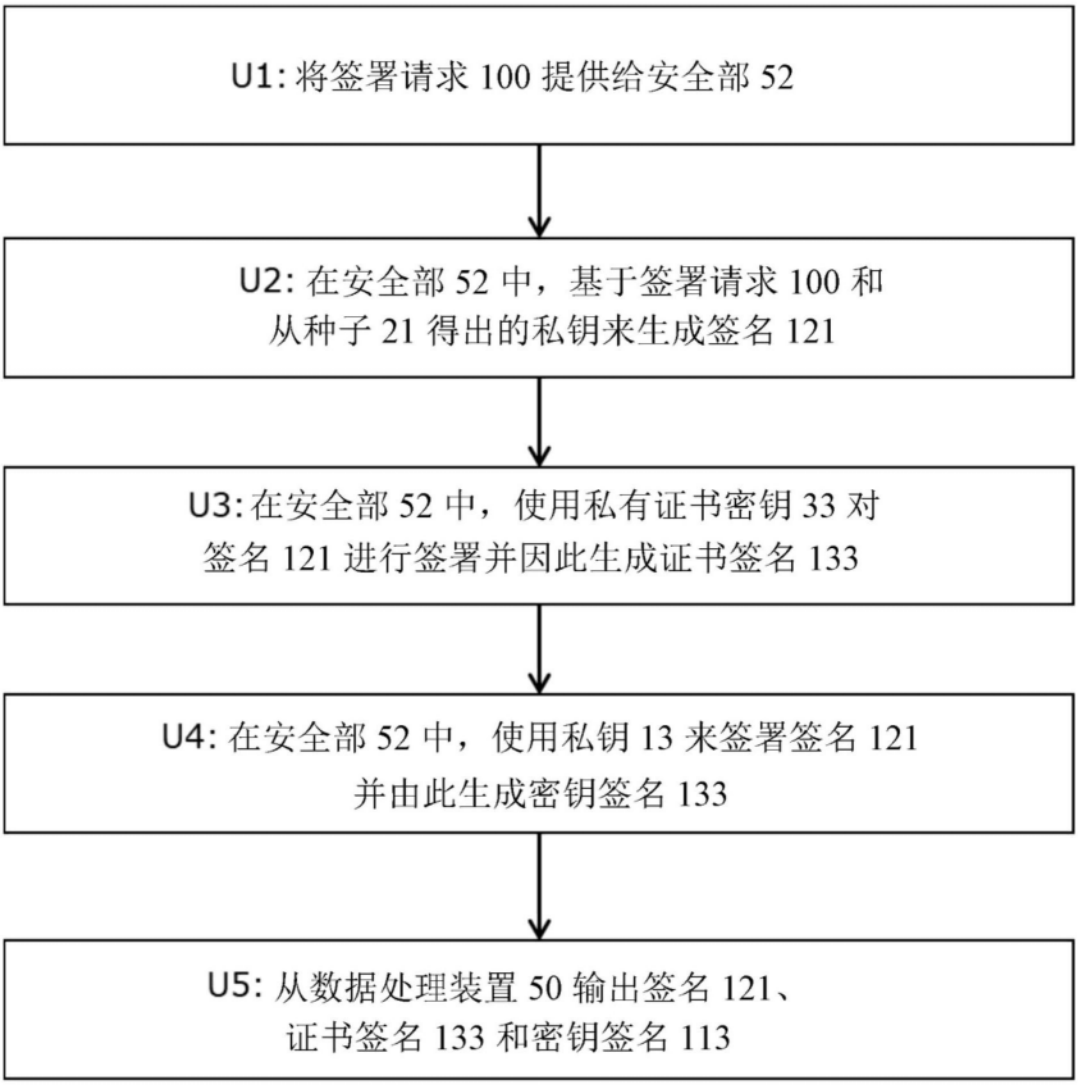

U1: 将签署请求 100 提供给安全部 52
U2: 在安全部 52 中，基于签署请求 100 和
从种子 21 得出的私钥来生成签名 121
U3: 在安全部 52 中，使用私有证书密钥 33 对
签名 121 进行签署并因此生成证书签名 133
U4: 在安全部 52 中，使用私钥 13 来签署签名 121
并由此生成密钥签名 133
U5: 从数据处理装置 50 输出签名 121、
证书签名 133 和密钥签名 113

图7

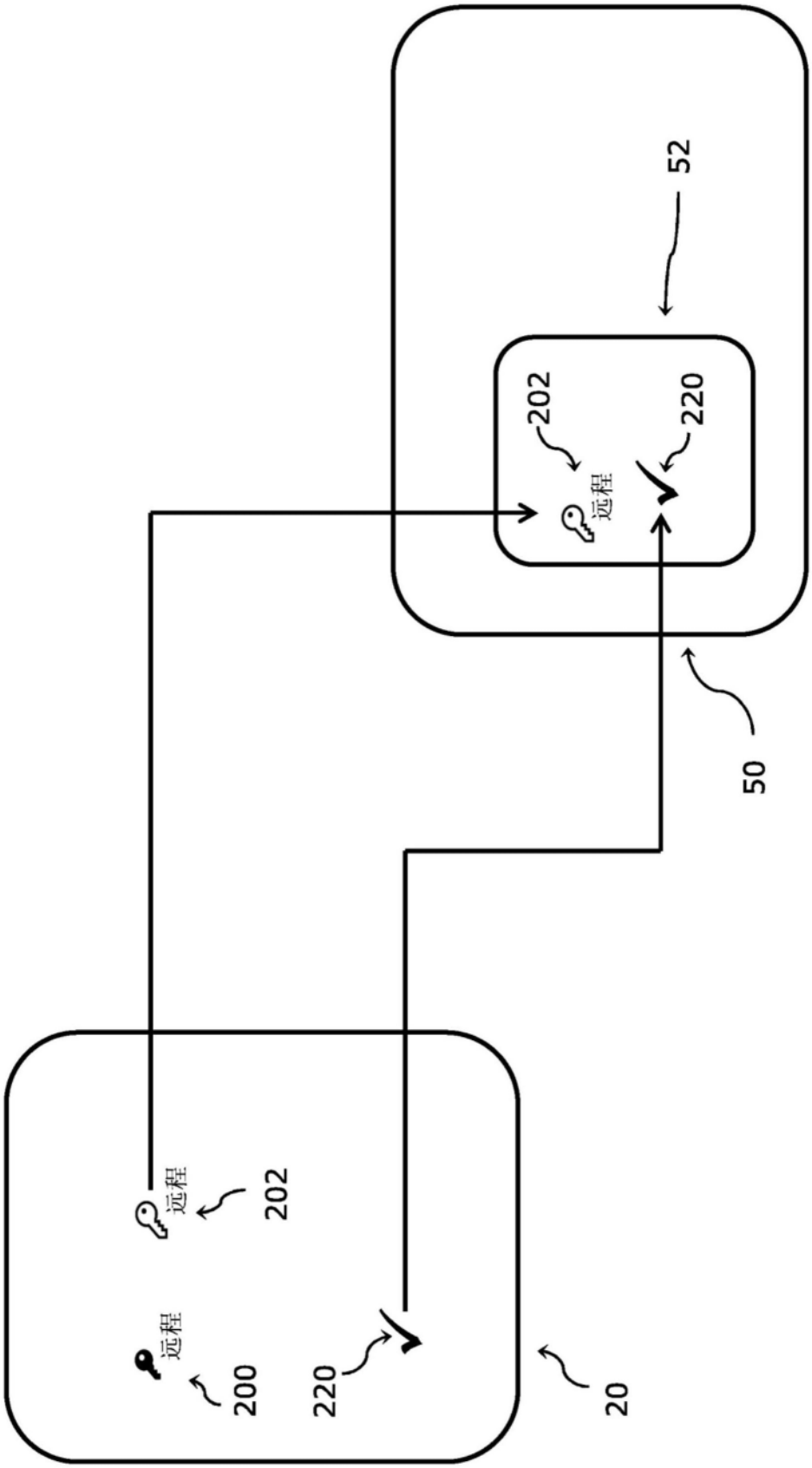


图8

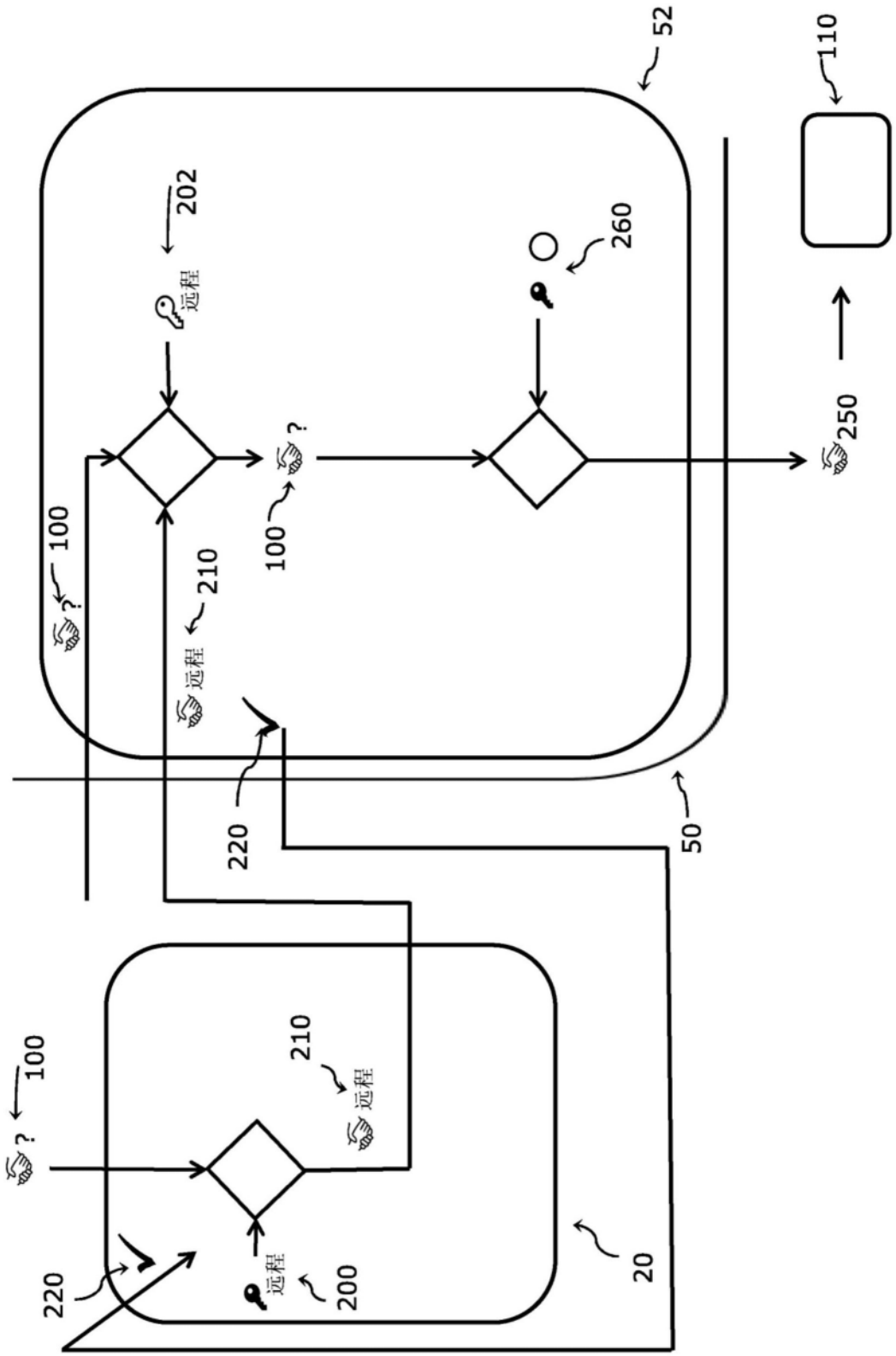

52
110
202
远程
260
250
100
?
210
远程
220
50
100
?
210
远程
100
?
220
远程
200
20

图9

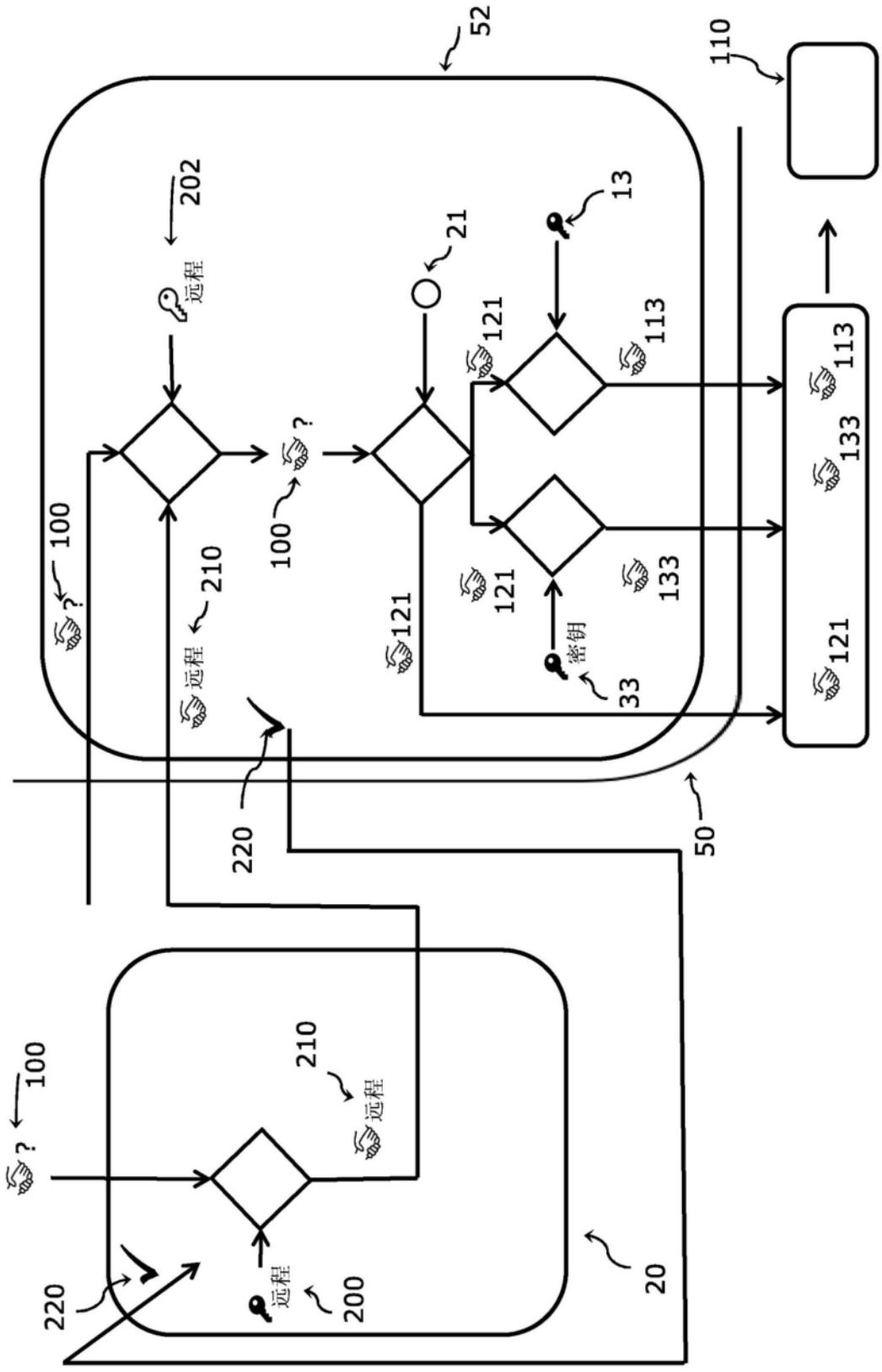

52
110
202
远程
13
21
121
113
100
?
210
远程
100
?
121
113
133
121
133
121
密钥
33
121
220
50
100
?
210
远程
远程
200
220
20

图10