(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 102111274 B
(45)授权公告日 2014.07.02

(21)申请号 201110050584.X
(22)申请日 2001.06.14
(30)优先权数据
09/605605 2000.06.28 US
(62)分案原申请数据
01811981.6 2001.06.14
(73)专利权人 英特尔公司
地址 美国加利福尼亚州
(72)发明人 C·埃利森 J·苏顿二世
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 柯广华 卢江
(51)Int.Cl.
H04L 9/32(2006.01)
(56)对比文件
US 5606617 A,1997.02.25,
US 4759064 A,1988.07.19,
审查员 苏宁

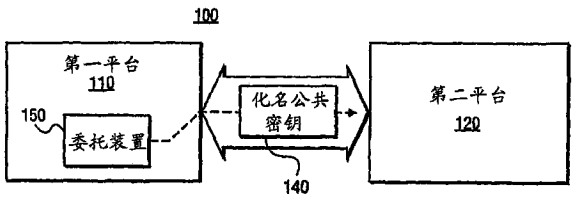
权利要求书2页 说明书5页 附图4页

(54)发明名称

用于建立可核查身份而又保密的平台和方法

(57)摘要

在一个实施方案中,一种利用化名来保护平台和其用户身份的方法被描述。该方法包括产生包括公共化名密钥的化名。该公共化名密钥被放置到证明模板中。对证明模板进行散列运算,以产生证明散列值,从平台上对其进行变换。随后,向该平台返回签署结果。该签署结果是该变换的证明散列值的数字签名。对该签署结果进行逆变换后,就恢复了该证明散列值的数字签名。该数字签名可以用于此后利用该化名通讯的数据完整性检查。



CN 102111274 B

1. 一种方法，包括：

在第一平台中产生一包含一公共化名密钥的化名，其中该化名可被产生、分配并删除，一第一密钥对驻留在一永久存储器中，第一密钥对包括第一平台的私用密钥和第一平台的公共密钥，所述公共化名密钥与第一平台的公共密钥分离；

将该公共化名密钥放入一数字证明模板中；

对该数字证明模板进行一散列运算，产生一证明散列值；

对该证明散列值进行一变换，用于从第一平台到第二平台的传送；

从第二平台接收一签署结果，该结果是用于变换的证明散列值的数字签名；和

在第一平台中对该签署结果进行一反变换，以恢复该证明散列值的一数字签名，

其中在接收数字签名之前，利用第一平台的所述私用密钥，数字签署一包括变换的证明散列值的证明请求，来产生一签署的证明请求；

与该签署的证明请求一起，获得一装置证明，即包括第一平台的所述公共密钥的数字证明链；以及

将签署的证明请求和装置证明加密并传送到第二平台。

2. 依照权利要求 1 的方法，其中产生化名的步骤包括产生公共化名密钥和一对应于该公共化名密钥的私用化名密钥，其中所述私用化名密钥与第一平台的公共密钥分离。

3. 依照权利要求 1 的方法，其中将该公共化名密钥放入一数字证明模板中的步骤包括将该公共化名密钥写入到数字证明模板的一字段中。

4. 依照权利要求 1 的方法，其中进行变换的步骤包括：

利用一伪随机数对证明散列值进行一逻辑运算，以产生一不同于证明散列值的值。

5. 依照权利要求 4 的方法，其中该伪随机数是一预定数值的由一伪随机值指定的相反次幂。

6. 依照权利要求 5 的方法，其中该伪随机值被存储在安全存储器中。

7. 依照权利要求 4 的方法，其中进行反变换的步骤包括利用伪随机数的倒数对签署结果进行一逻辑运算。

8. 依照权利要求 1 的方法，进一步包括：

存储该证明散列值的数字签名，用于此后在第一平台和第二平台之间的通讯。

9. 依照权利要求 1-8 中任何一项的方法，进一步包括：

在所述永久存储器中存储所述化名和数字签名。

10. 依照权利要求 9 的方法，进一步包括：

利用一数字发生器辅助产生所述化名。

11. 一种装置，包括：

用于在第一平台中产生一包含一公共化名密钥的化名的单元，其中该化名可被产生、分配并删除，一第一密钥对驻留在一永久存储器中，第一密钥对包括第一平台的私用密钥和第一平台的公共密钥，所述公共化名密钥与第一平台的公共密钥分离；

用于将该公共化名密钥放入一数字证明模板中的单元；

用于对该数字证明模板进行一散列运算、产生一证明散列值的单元；

用于对该证明散列值进行一变换、用于从第一平台到第二平台的传送的单元；

用于从第二平台接收一签署结果的单元，该结果是用于变换的证明散列值的数字签

名 ;和

用于在第一平台中对该签署结果进行一反变换、以恢复该证明散列值的一数字签名的单元,

其中所述装置还包括 :

用于在接收数字签名之前利用第一平台的所述私用密钥、数字签署一包括变换的证明散列值的证明请求、来产生一签署的证明请求的单元 ;

用于在接收数字签名之前与该签署的证明请求一起、获得一装置证明、即一包括一第一平台的所述公共密钥的数字证明链的单元 ;以及

用于在接收数字签名之前将签署的证明请求和装置证明加密并传送到一第二平台的单元。

12. 依照权利要求 11 的装置,其中用于产生化名的单元包括用于产生公共化名密钥和一对应于该公共化名密钥的私用化名密钥的单元,其中所述私用化名密钥与第一平台的公共密钥分离。

13. 依照权利要求 11 的装置,其中用于将该公共化名密钥放入一数字证明模板中的单元包括用于将该公共化名密钥写入到数字证明模板的一字段中的单元。

14. 依照权利要求 11 的装置,其中用于进行变换的单元包括 :

用于利用一伪随机数对证明散列值进行一逻辑运算、以产生一不同于证明散列值的值的单元。

15. 依照权利要求 14 的装置,其中该伪随机数是一预定数值的由一伪随机值指定的相反次幂。

16. 依照权利要求 15 的装置,其中该伪随机值被存储在安全存储器中。

17. 依照权利要求 14 的装置,其中用于进行反变换的单元包括用于利用伪随机数的倒数对签署结果进行一逻辑运算的单元。

18. 依照权利要求 11 的装置,进一步包括 :

用于存储该证明散列值的数字签名、用于此后在第一平台和第二平台之间的通讯的单元。

19. 依照权利要求 11-18 中任何一项的装置,进一步包括 :

用于在所述永久存储器中存储所述化名和数字签名的单元。

20. 如权利要求 19 所述的装置,进一步包括 :

用于利用一数字发生器辅助产生所述化名的单元。

用于建立可核查身份而又保密的平台和方法

技术领域

[0001] 本发明涉及的是数据安全领域。特别是，本发明涉及一种平台和方法，该平台和方法通过建立和使用化名来保护该平台的身份。

背景技术

[0002] 技术的发展，为超出传统贸易方式的应用提供了许多机会。电子商务(e-commerce)和企业对企业(B2B)的交易现在变得普及，以很快的速度触及全球市场。不幸的是，在诸如计算机的电子平台为用户提供方便有效的贸易、通讯和交易的方法同时，也容易受到肆无忌惮的攻击。这一弱点在很大程度上使内容提供者不愿意以一种下载的数字形式来提供其内容。

[0003] 当前，已经提出了各种机制来验证一个平台身份。这对于确定平台是否是一个“委托”装置（即该装置是否配置为防止在未授权的情况下以一种非加密的格式来拷贝数字内容）是特别有用的。一种验证方案包括使用一个分配给一个平台的唯一的序列号来识别该平台。另一独立于上述验证方案或与上述验证方案合作执行的验证方案包括采用一个永久密钥对。该永久密钥对包括(i)一个识别该平台的唯一公共密钥，和(ii)一个私用密钥，永久存储在该委托装置的存储器中。该私用密钥是秘密的，不向委托装置的外部提供。但是，这些验证方案有许多缺陷。

[0004] 例如，这些验证方案中的每一个仍受到数据收集攻击。“数据收集”涉及对一段时间内从一个平台发送的数据的采集和分析。这样，采用平台序列号和永久密钥用于识别目的近来已经导致对用户隐私的担忧。而且，对于上述两种机制，一个用户不能容易和可靠地基于每个用户的形式访问和使用平台身份。

发明内容

[0005] 按照本发明的实施例，提供一种方法，包括：在一平台中产生一包含一公共化名密钥的化名，其中该化名可被产生、分配并删除，一第一密钥对驻留在一永久存储器中；将该公共化名密钥放入一证明模板中；对该证明模板进行一散列运算，以产生一证明散列值；对该证明散列值进行一变换，用于从平台向外的传送；接收一签署结果，该签署结果是用于变换的证明散列值的数字签名；和对该签署结果进行一反变换，以恢复该证明散列值的一数字签名。

[0006] 优选地，产生化名的步骤包括产生公共化名密钥和一对应于该公共化名密钥的私用化名密钥。

[0007] 优选地，将该公共化名密钥放入一证明模板中的步骤包括将该公共化名密钥写入到证明模板的一字段中。

[0008] 优选地，进行变换的步骤包括：利用一伪随机数对证明散列值进行一逻辑运算，以产生一不同于证明散列值的值。

[0009] 优选地，该伪随机数是一预定值的由一伪随机值指定的反幂。

[0010] 优选地，该伪随机值被存储在安全存储器中。

[0011] 优选地，进行反变换的步骤包括利用伪随机数的倒数对签署结果进行一逻辑运算。

[0012] 优选地，在接收数字签名之前，该方法包括：利用第一平台的一私用密钥，数字签署一包括变换的证明散列值的证明请求，以产生一签署的证明请求。

[0013] 优选地，在接收数字签名之前，该方法进一步包括：与该签署的证明请求一起，获得一装置证明，即一包括一第一平台的一公共密钥的数字证明链。

[0014] 优选地，在接收数字签名之前，该方法进一步包括：将签署的证明请求和装置证明传送到一第二平台。

[0015] 优选地，该方法进一步包括：存储该证明散列值的数字签名，用于此后与一远处的平台进行通信。

[0016] 按照本发明的实施例，提供一种装置，包括：一处理单元；和一永久存储器，以包含一第一密钥对及至少一个化名，用于与远处装置通讯及确定包含该装置的平台是安全的。

[0017] 优选地，该装置进一步包括：一数字发生器，辅助产生该至少一个化名。

[0018] 按照本发明的实施例，提供一种平台，包括：一收发器；和一与该收发器通讯的装置，该装置包括一永久存储器，来存储一永久密钥对、至少一个在该装置内部产生的化名、和一数字证明链的散列值的数字签名，该数字证明链包含化名的一公共化名密钥，其中该化名可被产生、分配并删除。

[0019] 优选地，所述装置进一步包括：一处理单元，(i) 将公共化名密钥写入到一证明模板中，以便 (ii) 对该证明模板进行一散列运算，以产生一证明散列值；(iii) 对该证明散列值进行一变换。

[0020] 优选地，所述装置的处理单元利用永久密钥对的一私用密钥，进一步产生至少变换的证明散列值的一数字签名。

[0021] 优选地，装置的处理单元进一步附加具有该至少变换的证明散列值的数字签名的一装置证明。

[0022] 优选地，该装置证明是一数字证明链。

[0023] 按照本发明的实施例，提供一种使用一装置的永久存储器的方法，包括：在所述永久存储器中存储一第一密钥对。

[0024] 优选地，所述方法进一步包括：利用一数字发生器辅助产生至少一个化名。

附图说明

[0025] 根据下面对本发明的详细描述，可以清楚地了解本发明的特征和优点，其中：

[0026] 图 1 是利用本发明的系统的说明性实施方案的方框图。

[0027] 图 2 是图 1 中的第一平台中所采用的委托逻辑的说明性实施方案的方框图。

[0028] 图 3 是描述图 1 中的第一平台中产生的化名的分配和使用的说明性实施方案的流程图。

[0029] 图 4 和 5 是产生和验证化名的说明性实施方案的流程图。

具体实施方式

[0030] 本发明涉及一种平台和方法，用于通过产生和使用化名来保护平台的身份。此处，阐明了某些细节，以便对本发明的有一个透彻的理解。但是，显然，对于本领域的技术人员来讲，可以通过许多不同于所描述的实施方案来实施本发明。为了避免不必要地使本发明不明显，对于众所周知的电路和加密技术不做详述。

[0031] 在下面的描述中，利用术语来讨论本发明的某些特征。例如，“平台”包括处理信息的硬件和/或软件。平台的例子包括但不局限于或受限于下列任何情况：计算机（如台式机、膝上型电脑、手提式电脑、服务器、工作站等）；数据传输设备（如路由器、交换机、传真机等），无线设备（如蜂窝基站、电话手机等）；或者电视机顶盒。“软件”包括代码，当被执行时，实施某一功能。“信息”定义为数据、地址和/或控制的一个或多个位。

[0032] 关于加密功能，“加密运算”是为信息附加安全性所执行的运算。这些运算可能包括加密、解密、散列计算等等。在某些情况下，加密运算需要使用密钥，即位序列。对于不对称密钥加密术，将装置与包含公共密钥和私用密钥的唯一永久密钥对相关联。

[0033] 此外，不对称密钥加密术通常利用根证明。“根证明”是最初产生数字证明链时的公共密钥，并为随后所有的数字证明提供起始点。通常，“数字证明”包括用来验证信息发送者的信息。例如，根据 CCITTRecommendation X.509 :The Directory-Authentication Framework(1988)，数字证明可以包括关于被验证的，即利用认证机关的私用密钥进行加密的个人或团体的信息（如密钥）。“认证机关”的例子包括原始设备制造商 (OEM)、软件销售者、商贸协会、政府机构、银行或其它委托公司或个人。“数字证明链”包括如下所述的为认证而安排的两个或更多个数字证明的规则序列 (ordered sequence)，其中每个连续的证明代表先前证明的发出者。

[0034] “数字签名”包括利用其签署人的一个私用密钥签署的数字信息，以保证该数字信息在数字签署后没有被非法修改过。可以以其完整形式，或者以由单向散列运算产生的散列值来提供该数字信息。

[0035] “散列运算”是将信息单向变换为被称为“散列值”的固定长度的表示。通常，该散列值在尺寸上充分小于原始信息。在有些情况下，可以进行 1 ： 1 的原始信息变换。术语“单向”是指不易有反函数来恢复该固定长度的散列值的原始信息中任何可辨别的部分。散列函数的例子包括California Redwood City的RSA Data Security提供的MD5，或Secure Hash Algorithm(SHA-1)，如 1995 年出版的标题为“FederalInformation Processing Standards Publication”的 Secure HashStandard FIPS 180-1(1995 年 4 月 17 日）所述的那样。

[0036] 参考图 1，图中显示了利用本发明的系统 100 的说明性实施方案方框图。系统 100 包括第一平台 110 和第二平台 120。第一平台 110 是通过链路 130 与第二平台 120 进行通讯。“链路”被概括定义为一个或多个信息载运媒体（如电线、光纤、电缆、总线或无线信号技术）。当用户请求时，第一平台 110 产生并向第二平台 120 发送化名公共密钥 140（下面描述）。在响应中，当可适用时，第二平台负责确认该化名公共密钥 140 是在第一平台 110 中由委托装置 150 产生。

[0037] 现在参考图2，在一个实施方案中，委托装置150包括硬件和/或保护的软件。当采用访问控制方案来防止未授权的对软件的任何例程或子例程进行访问时，认为软件是“受

保护的”。更具体地讲，装置 150 是一个或多个防止其它逻辑的窜改和窃取的集成电路。可以将该集成电路放置在一个单一集成电路 (IC) 组件或多 IC 组件中。组件提供附加的窜改保护。当然，如果不需附加的保护，可以采用没有任何 IC 组件的装置 150。

[0038] 这里，装置 150 包括处理单元 200 和永久存储器 210（如非易失存储器、电池支持的随机存取存储器“RAM”等）。处理单元 200 是由内部处理信息的软件来控制的硬件。例如，处理单元 200 可以进行散列运算、进行逻辑运算（如乘法、除法等）、和 / 或通过使用数字签名算法进行数字签署信息来产生数字签名。永久存储器 210 包含在制造过程中编程的唯一的不对称密钥对 220。用于核实化名，不对称密钥对 220 包括公共密钥 (PUKP1)230 和私用密钥 (PRKP1)240。永久存储器 210 可以进一步包括第二平台 120 的公共密钥 250(PUKP2)，尽管如果可适用的话它可以被放置在装置 150 中的易失存储器（如 RAM、寄存器组等）中。

[0039] 在该实施方案中，装置 150 进一步包括数（字）发生器 260，如随机数发生器，或伪随机数发生器。数（字）发生器 260 负责产生比特流，至少部分地用于产生一个或多个化名。“化名”是另一密钥对形式的别名身份，该另一密钥对用来建立与另一个平台的受保护的通讯，并确认其平台包括委托装置 150。化名还支持询问 / 响应协议和许可绑定、保密和其它对特定平台的访问控制信息。但是，考虑数（字）发生器 260 也可从装置 150 的外部使用。在这种情况下，如果数（字）发生器 260 和装置 150 之间的通讯是受到保护的，则通过平台 110 可以实现更大的安全性。

[0040] 参考图 3，图中显示了说明化名的分配和使用的说明性实施方案的流程图。为了充分保护用户的机密，用户应当切实控制化名的产生、分配和删除。这样，响应用户明确应允，产生新的化名（程序块 300 和 310）。而且，为了访问用来识别现有化名的信息（如标记、公共密钥等），需要用户明确的应允（程序块 320 和 330）。可以通过向委托装置提供一个许可短语 (pass-phrase)（如包含文字和数字的字符串）、令牌和 / 或生物统计特征，来给出明确的用户应允。例如，在一个实施方案中，可以通过一个用户输入装置（如键盘、鼠标、小键盘、操纵杆、触摸垫、轨迹球等）来输入用户许可短语，并将其传送到委托装置。在另一个实施方案中，逻辑电路外部的存储器可以包含通过用户的许可短语的散列值加密的化名。这些化名中的任何一个都可以通过再次提供用户的许可短语来解密供使用。

[0041] 一旦产生了化名并配置用于与远程平台进行通讯，对于平台 / 平台的通讯，只要用户选择保持该化名，那么该化名就代表持久平台身份（程序块 340，350 和 360）。

[0042] 参考图 4 和 5，图中显示了产生和验证化名的说明性实施方案的流程图。开始，接收到用户的请求时，由装置结合一数（字）来产生化名（程序块 400）。个化名公共密钥 (PPUKP1) 被放置到数字证明模板中（程序块 405）。该数字证明模板可以内部地存储在第一平台中，或由第二平台根据第一平台的证明请求来提供。因此，该数字证明模板经过散列运算，产生证明散列值（程序块 410）。

[0043] 随后，该证明散列值经过一个类似于美国专利 No. 4,759,063 和 4,759,064 中所描述的变换，来创建一个“不可见的”证明散列值（程序块 415）。特别是，将该证明散列值乘以伪随机数（例如预定数的伪随机选择的幂）。该伪随机幂在第一平台中是保密的（如放置在图 2 中的永久存储器 210 中）。

[0044] 产生至少包括该变换的（或不可见的）证明散列值的证明请求（程序块 420）。利用第一平台的私用密钥 (PRKP1) 来数字签署该证明请求（程序块 425）。检索或产生装置证

明，即第一实施方案中包含第一平台的公共密钥 (PUKP1) 的数字证明链，伴随签署的证明请求（程序块 430）。在该实施方案中，装置证明的特征是具有包含 PUKP1 的高层证明和包括根证明的最低层证明。当然，该装置证明可以是包含 PUKP1 的单一数字证明。签署的证明请求和装置证明都利用第二平台的公共密钥 (PUKP2) 来加密，然后传送到第二平台（程序块 435 和 440）。

[0045] 在第二平台中，签署的证明请求和装置证明在利用第二平台的私用密钥 (PRKP2) 解密后被恢复（程序块 445）。可以利用负责签署装置证明的证明机关的公共密钥来获得第一平台的公共密钥 (PUKP1)（程序块 450）。如果第二平台可以恢复证明请求，则第二平台对装置证明进行验证回到根证明（程序块 455 和 460）。如果恢复了证明请求并验证了装置证明，则数字签署变换的（或不可见的）证明散列值，以产生“签署结果”（程序块 465）。否则，如果不能确定变换的（或不可见的）证明散列值，或不能验证装置证明，则向第一平台返回出错消息（程序块 470）。

[0046] 从第二平台接收到签署结果时，第一平台对该信号结果进行一个反变换。例如，在该说明性实施方案中，第一平台将签署结果除以伪随机数（例如预定数的伪随机数反幂）的倒数，来恢复证明散列值的数字签名（程序块 475 和 480）。该数字签名与一个或多个化名一同存储，用于以后与其它平台的通讯，来确定第一平台包括委托装置。

[0047] 虽然参照说明性的实施方案对本发明进行了描述，但该说明不要被限制性地进行解释。对说明性实施方案的各种修改以及本发明的其它实施方案，只要对本领域技术人员而言明显的，都被认为是在本发明的精神和范围内。

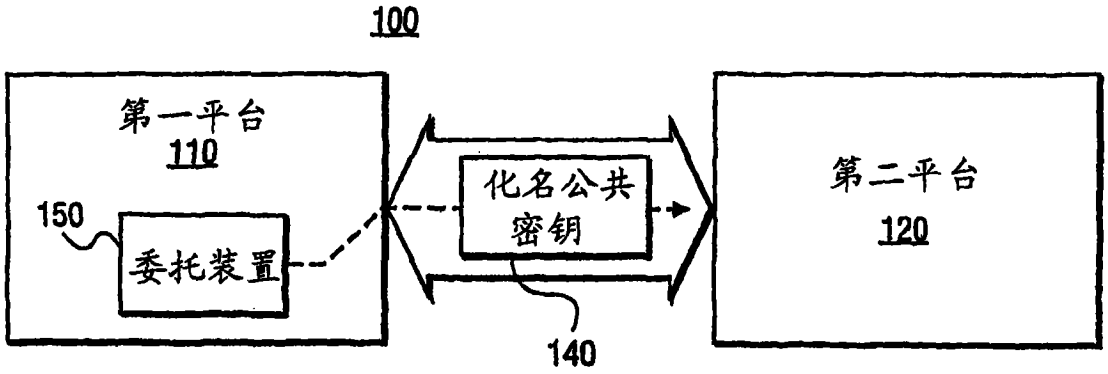

100
第一平台
110
150
委托装置
化名公共
密钥
140
第二平台
120

图 1

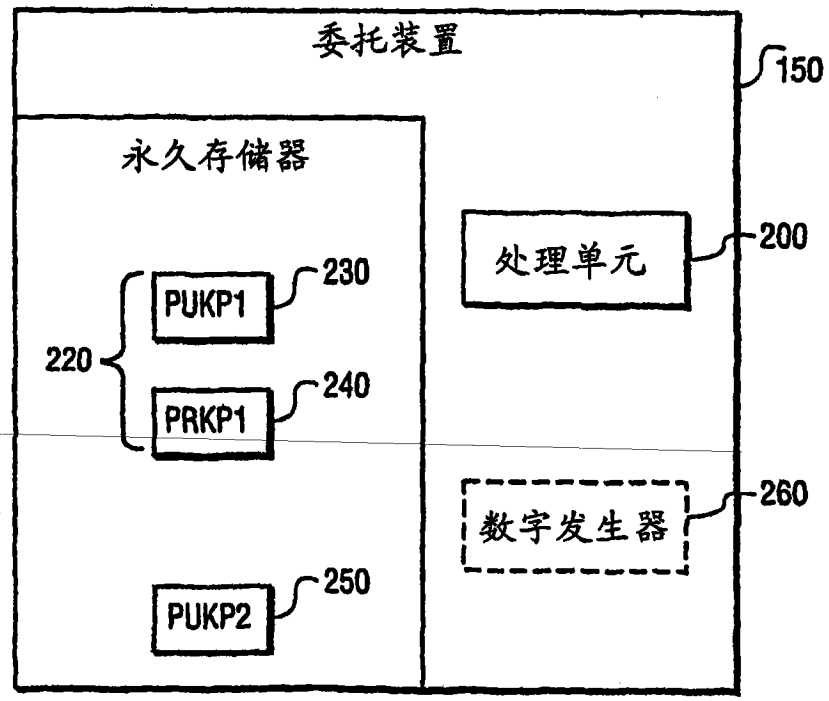

委托装置
150
永久存储器
处理单元
200
PUKP1
230
220
PRKP1
240
数字发生器
260
PUKP2
250

图 2

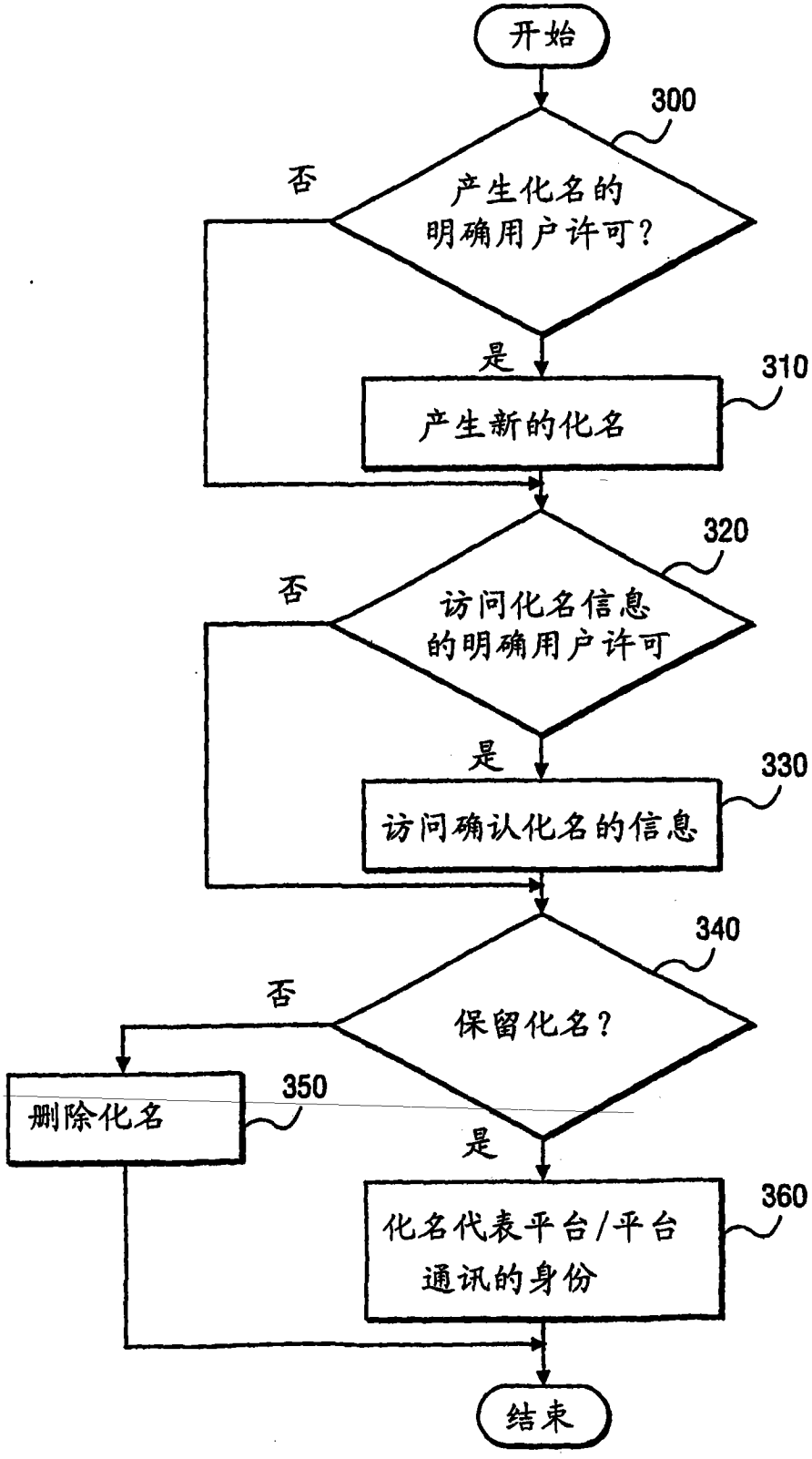

开始
300
产生化名的
明确用户许可？
否
是
310
产生新的化名
320
访问化名信息
的明确用户许可
否
是
330
访问确认化名的信息
340
保留化名？
否
是
350
删除化名
360
化名代表平台/平台
通讯的身份
结束

图 3

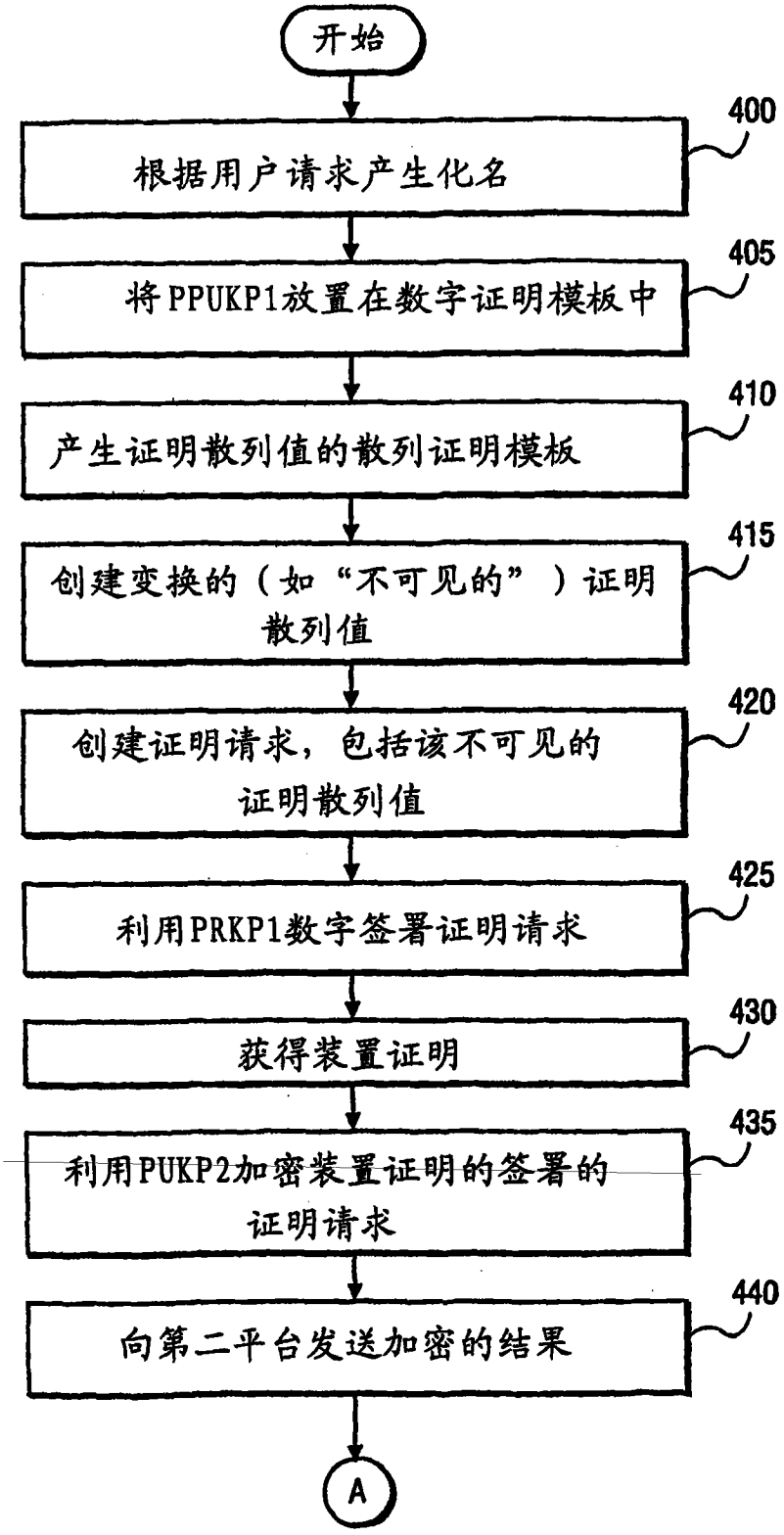

开始
400
根据用户请求产生化名
405
将PPUKP1放置在数字证明模板中
410
产生证明散列值的散列证明模板
415
创建变换的（如“不可见的”）证明散列值
420
创建证明请求，包括该不可见的证明散列值
425
利用PRKP1数字签署证明请求
430
获得装置证明
435
利用PUKP2加密装置证明的签署的证明请求
440
向第二平台发送加密的结果
A

图 4

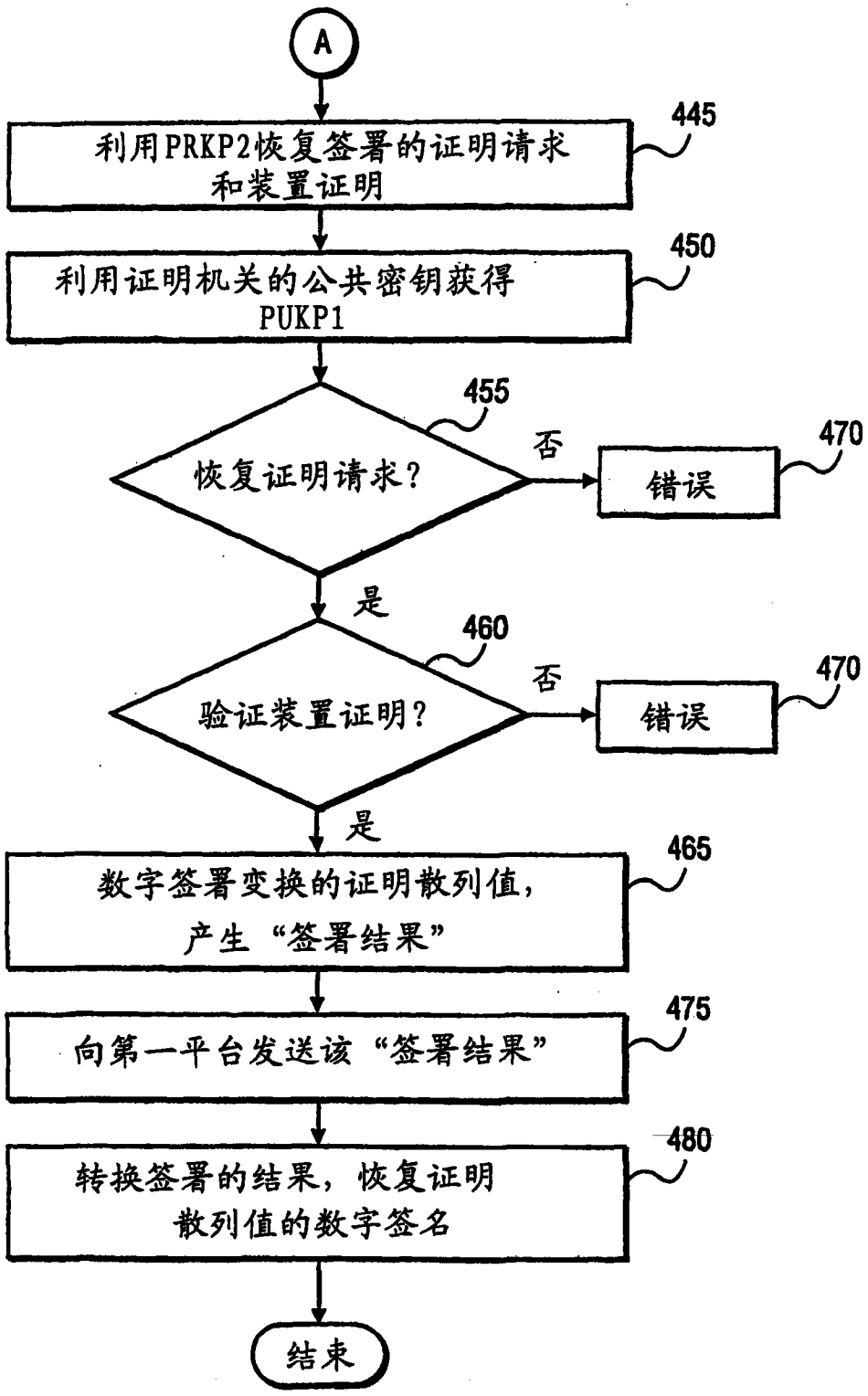

A
利用PRKP2恢复签署的证明请求和装置证明
445
利用证明机关的公共密钥获得PUKP1
450
恢复证明请求？
455
否
错误
470
是
验证装置证明？
460
否
错误
470
是
数字签署变换的证明散列值，产生“签署结果”
465
向第一平台发送该“签署结果”
475
转换签署的结果，恢复证明散列值的数字签名
480
结束

图 5