



(12) 发明专利申请

(10) 申请公布号 CN 104798083 A

(43) 申请公布日 2015.07.22

(21) 申请号 201380057912.6

(74) 专利代理机构 北京康信知识产权代理有限公司 11240
代理人 梁丽超 陈鹏

(22) 申请日 2013.09.06

(51) Int. Cl.

(30) 优先权数据

G06F 21/72(2006.01)

1215951.3 2012.09.06 GB

G06F 21/34(2006.01)

1222090.1 2012.12.07 GB

(85) PCT国际申请进入国家阶段日

2015.05.05

(86) PCT国际申请的申请数据

PCT/GB2013/052347 2013.09.06

(87) PCT国际申请的公布数据

WO2014/037741 EN 2014.03.13

(71) 申请人 VISA 欧洲有限公司

地址 英国伦敦

(72) 发明人 鲍里斯·塔拉蒂内 马修·约翰逊

西蒙·彼得·拉斯特

安德鲁·沃伦·朗兹

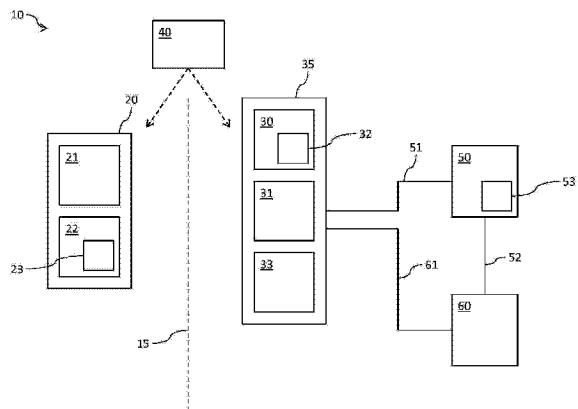
权利要求书4页 说明书14页 附图3页

(54) 发明名称

用于验证访问请求的方法和系统

(57) 摘要

用于在系统内验证访问数据的请求的系统和方法，系统包括：第一模块，访问第一受信任的时间指示器；第二模块，访问不受信任的时间指示器；以及计算装置，访问第二受信任的时间指示器。所述第一模块至少使用所述第一受信任的时间指示器生成密码。所述第二模块接收与访问数据的请求相关联的密码，并且至少使用不受信任的时间指示器验证所接收的密码。然后，所述第二模块促使将消息传输给所述计算装置，所述消息包括至少表示用于验证所接收的密码的不受信任的时间指示器的数据。然后，所述计算装置生成表示在不受信任的时间指示器与第二受信任的时间指示器之间的比较的数据，并且使用所生成的数据，来提供所述对数据的访问。



1. 一种用于验证对数据的访问的请求的系统,所述系统访问被配置为与第一受信任的时间指示器进行通信的计算装置,所述系统包括:

第一模块,访问第二受信任的时间指示器;以及

第二模块,访问不受信任的时间指示器,其中,

所述第一模块被设置为至少使用所述第二受信任的时间指示器生成密码;

所述第二模块被设置为:

接收与对数据的访问的所述请求相关联的密码,至少使用所述不受信任的时间指示器验证所接收的密码;并且

使消息被传输给所述计算装置,所述消息包括表示用于验证所接收的密码的所述不受信任的时间指示器的数据,并且

所述系统被设置为使所述计算装置生成表示在所述不受信任的时间指示器与所述第一受信任的时间指示器之间的比较的数据,其中,所生成的数据用于提供所述对数据的访问。

2. 根据权利要求 1 所述的系统,其中,所述系统被设置为使所述计算装置基于所生成的数据选择性地为系统提供所述对数据的访问。

3. 根据权利要求 1 或 2 所述的系统,其中,传输给所述计算装置的所述消息包括表示所述第二模块至少使用所述不受信任的时间指示器对所接收的密码的验证的数据。

4. 根据前述权利要求中任一项所述的系统,其中,所述第一模块和所述第二模块共享唯一地分配给其的密钥,所述第一模块被设置为使用所述密钥来生成所述密码,并且所述第二模块被设置为使用所述密钥来验证所接收的密码。

5. 根据权利要求 4 所述的系统,其中,所述密钥储存在所述第一模块的安全部件内。

6. 根据权利要求 4 或 5 所述的系统,其中,所述密钥储存在所述第二模块的安全部件内。

7. 根据前述权利要求中任一项所述的系统,其中,所述第一模块包括包含时钟的防损硬件,所述时钟被设置为提供所述第二受信任的时间指示器。

8. 根据前述权利要求中任一项所述的系统,其中,所述第二模块通信地连接至具有时钟的装置,所述时钟被设置为提供所述不受信任的时间指示器。

9. 根据前述权利要求中任一项所述的系统,其中,所述系统被设置为使所述计算装置将包括所生成的数据的消息发送给另一个计算装置,从而为所述系统提供所述对数据的访问,所述另一个计算装置被设置为在接收所生成的数据时提供所述对数据的访问。

10. 根据权利要求 2 到 8 中任一项所述的系统,其中,所请求的数据储存在所述计算装置处或者由所述计算装置生成,并且所述计算装置被设置为基于所生成的数据提供所述对数据的访问。

11. 根据前述权利要求中任一项所述的系统,其中,所述第一模块被设置为通过所述第一模块的接口接收由所述第二模块或所述计算装置生成的问询码,并且至少使用所述问询码,生成所述密码。

12. 根据前述权利要求中任一项所述的系统,其中,所述第一模块被设置为生成多个密码,所述多个密码中的至少一个密码与所述多个密码中的另一个密码不同,并且通过所述第一模块的接口将至少一个所生成的密码提供给用户。

13. 根据前述权利要求中任一项所述的系统,其中,所述第二模块和所述计算装置共享另一个密钥,以在其间的通信中使用。

14. 根据前述权利要求中任一项所述的系统,其中,所述第二模块被设置为储存所接收的密码,并且比较所接收的密码和任何先前储存的接收的密码,从而验证所接收的密码。

15. 根据权利要求 1 所述的系统,其中,所述第一模块和所述第二模块通信地断开,并且所述第二模块被设置为从所述计算装置中接收所生成的数据,并且使用所接收的数据来提供所述对数据的访问。

16. 根据权利要求 15 所述的系统,其中,从计算装置中接收的所述数据包括表示所述不受信任的时间指示器是否在所述第一受信任的时间指示器的预定范围内的数据。

17. 根据权利要求 15 或 16 所述的系统,其中,所请求的数据由所述第二模块保持,并且所述第二模块被配置为使用从所述计算装置中接收的所述数据,来确定是否提供对所请求的数据的访问。

18. 根据权利要求 15 到 17 中任一项所述的系统,其中,所述第二受信任的时间指示器是所述第一模块的时钟,并且所述第一受信任的时间指示器是与所述第一模块的时钟同步的时钟。

19. 根据权利要求 15 到 18 中任一项所述的系统,其中,所述计算装置和所述第二模块预先配置有加密密钥,用于签署在其间发送的数据,并且其中,所述第二模块被设置为签署传输给所述计算装置的所述消息,并且验证所述计算装置使用所述加密密钥签署从所述计算装置中接收的所述数据。

20. 根据权利要求 15 到 19 中任一项所述的系统,其中,所述第二模块被设置为储存所接收的密码,并且比较所接收的密码和任何先前储存的接收的密码,从而验证所接收的密码。

21. 一种由系统使用计算装置验证对数据的访问的请求的方法,所述计算装置被配置为与第一受信任的时间指示器进行通信,所述方法包括:

至少使用第二受信任的时间指示器在第一模块处生成密码;

接收与对数据的访问的请求相关联的密码;

至少使用不受信任的时间指示器在第二模块处验证所接收的密码;并且

使消息被传输给所述计算装置,所述消息包括表示用于验证所接收的密码的所述不受信任的时间指示器的数据;

其中,

所述系统使所述计算装置生成表示在所述不受信任的时间指示器与所述第一受信任的时间指示器之间的比较的数据,其中,所生成的数据用于提供所述对数据的访问,并且

其中,所述系统包括所述第一模块和所述第二模块。

22. 根据权利要求 21 所述的方法,其中,所述系统使所述计算装置基于所生成的数据选择性地为所述系统提供所述对数据的访问。

23. 根据权利要求 21 或 22 所述的方法,其中,传输给所述计算装置的所述消息包括表示所述第二模块至少使用所述不受信任的时间指示器对所接收的密码的验证的数据。

24. 根据权利要求 21 到 23 中任一项所述的方法,其中,所述第一模块和所述第二模块共享唯一地分配给其的密钥,所述密钥用于生成所述密码并且用于验证所接收的密码。

25. 根据权利要求 24 所述的方法, 其中, 所述密钥储存在所述第一模块的安全部件内。
26. 根据权利要求 24 或 25 所述的方法, 其中, 所述密钥储存在所述第二模块的安全部件内。
27. 根据权利要求 21 到 26 中任一项所述的方法, 所述方法包括从在所述第一模块的防损硬件内的时钟中检索所述第二受信任的时间指示器。
28. 根据权利要求 21 到 27 中任一项所述的方法, 所述方法包括从与所述第二模块通信地连接的时钟中接收所述不受信任的时间指示器。
29. 根据权利要求 21 到 28 中任一项所述的方法, 其中, 所述系统使所述计算装置将包括所生成的数据的消息发送给另一个计算装置, 从而为所述系统提供所述对数据的访问, 所述另一个计算装置被设置为在接收所生成的数据时提供所述对数据的访问。
30. 根据权利要求 21 到 28 中任一项所述的方法, 其中, 所请求的数据储存在所述计算装置处或者由所述计算装置生成, 并且所述计算装置被设置为基于所生成的数据提供所述对数据的访问。
31. 根据权利要求 21 到 30 中任一项所述的方法, 所述方法包括通过第一模块的接口接收由所述第二模块或所述计算装置生成的问询码, 并且至少使用所述问询码, 生成所述密码。
32. 根据权利要求 21 到 31 中任一项所述的方法, 所述方法包括生成多个密码, 所述多个密码中的至少一个密码与所述多个密码中的另一个密码不同, 并且通过所述第一模块的接口将至少一个所生成的密码提供给用户。
33. 根据权利要求 21 到 32 中任一项所述的方法, 其中, 所述第二模块和所述计算装置共享另一个密钥, 以在其间的通信中使用。
34. 根据权利要求 21 到 33 中任一项所述的方法, 其中, 所述方法包括在所述第二模块处储存所接收的密码, 并且比较所接收的密码和任何先前储存的所接收的密码, 从而验证所接收的密码。
35. 根据权利要求 1 所述的方法, 其中, 所述第一模块和所述第二模块通信地断开, 并且所述系统使所述计算装置将所生成的数据提供给所述第二模块, 所述方法包括由所述第二模块使用所述接收的生成的数据来提供所述对数据的访问。
36. 根据权利要求 35 所述的方法, 其中, 从所述计算装置中接收的所述数据包括表示所述不受信任的时间指示器是否在所述第一受信任的时间指示器的预定范围内的数据。
37. 根据权利要求 35 或 36 所述的方法, 其中, 所请求的数据由所述第二模块保持, 并且所述方法包括由所述第二模块使用从所述计算装置中接收的所述数据, 来确定是否提供对所请求的数据的访问。
38. 根据权利要求 35 到 37 中任一项所述的方法, 其中, 所述第二受信任的时间指示器是所述第一模块的时钟, 并且所述第一受信任的时间指示器是与所述第一模块的时钟同步的时钟。
39. 根据权利要求 35 到 38 中任一项所述的方法, 其中, 所述计算装置和所述第二模块预先配置有加密密钥, 用于签署在其间发送的数据, 并且其中, 所述方法包括签署传输给所述计算装置的所述消息, 并且验证所述计算装置使用所述加密密钥签署从所述计算装置中接收的所述数据。

40. 根据权利要求 35 到 39 中任一项所述的方法，其中，所述方法包括在所述第二模块处储存所接收的密码，并且比较所接收的密码和任何先前储存的接收的密码，从而验证所接收的密码。

用于验证访问请求的方法和系统

技术领域

[0001] 本发明涉及用于验证访问请求的方法和系统，并且尤其地，但不完全地适合于验证用于访问数据、服务或资产的请求。

背景技术

[0002] 访问机密或用户专用数据（或资产或服务）的需求越来越大。例如，提供对银行账户的访问并且允许从该账户中转账，应限于授权用户，例如，账户持有人。通常，在通过识别请求访问数据的人的凭证请求访问数据时，认证用户。数据的远程访问提出了特定的问题，这是因为请求数据、资产或服务的个人通常位于与对该请求做出响应的一方的位置不同的物理位置中。结果，为请求提供服务的一方非常难以知道做出请求的实体是否是 a) 其自称的一方，b) 是否有权使用该请求所起源的装置，并且 c) 是否占有该请求所起源的装置。

[0003] 通常，在个人与一方（例如，数据提供商）之间建立账户时，个人建立上述凭证，以由数据提供商用于识别和认证个人，以供将来的请求。这种凭证可以包括唯一地识别个人（例如，个人可识别信息（PII））和密钥（例如，密码）的信息，用于验证个人的身份。现在，也常见的做法是数据提供商要求个人登记自己，作为用于访问数据的装置的拥有人。在装置与装置拥有人之间登记的关联可以由数据提供商用作额外的验证因子。例如，在数据提供商代表特定的个人从特定的装置（该装置并非为个人登记的装置）中接收用于访问账户的请求的情况下，数据提供商可以确定相信为该账户登记的个人做出请求。

[0004] 希望代表与该数据提供商具有账户的另一个人访问数据提供商的数据的个人可以比较容易地通过从刑事影子网上市场购买凭证来获得其用户凭证（即，PII、用户 ID 和密码），然后，欺骗性地访问其他人的数据。此外，能够远程地访问和控制装置，从而代表那些装置的登记拥有人请求数据。通常，不能确定在物理上占有该装置的用户是否做出了请求或者使用另一个装置来远程控制做出了请求的装置的用户是否远程做出了请求。

[0005] 一次性密码（OTP）通常用于减少这些问题：认证服务器唯一地将 OTP 生成密钥分配给装置的登记拥有人，OTP 生成密钥用于生成和验证 OTP。认证服务器通常持有几百或几千 OTP 生成密钥，每个密钥唯一地分配给一个不同的人或者为一个不同的人登记。在由登记拥有人通过其分配的 OTP 生成密钥占有时，认证服务器配置 OTP 令牌。例如，每当登记用户请求一个新密码时，这些 OTP 令牌可以使用 OTP 生成密钥来生成一个不同的密码，或者再如，可以使用 OTP 生成密钥来通过固定的时间间隔生成新密码。OTP 令牌可以另外使用当前世界的指示来生成 OTP，以防止在稍后的时间储存和重放 OTP。

[0006] 为了通过装置访问用户限制的数据，用户将由 OTP 令牌生成的 OTP 以及唯一地识别装置的拥有的凭证提供给数据提供商。通常，然后，数据提供商识别装置的拥有人并且将所接收的 OTP 传递给认证服务器。认证服务器查看与所识别的个人相关联的 OTP 生成密钥，并且使用该密钥以及（如果需要的话）当前时间来确定所接收的 OTP 是否与由 OTP 令牌生成的 OTP 对应，该装置的拥有人在当前时间或者至少在当前时间的预定周期内保持该 OTP 令牌。然后，认证服务器向数据提供商指示所接收的 OTP 是否有效。如果将正确的 OTP

发送给数据提供商,那么可以确定该装置的用户占有 OTP 令牌。然而,认证服务器容易妥协,从而促进到其他实体的未授权分布,并且允许(非法)访问分布的 OTP 生成密钥的任何人代表与该密钥相关联的个人访问数据。

发明内容

[0007] 根据本发明的第一方面,提供了一种用于验证访问数据的请求的系统,所述系统访问被配置为与第一受信任的时间指示器进行通信的计算装置,所述系统包括:第一模块,访问第二受信任的时间指示器;以及第二模块,访问不受信任的时间指示器,其中,所述第一模块被设置为至少使用所述第二受信任的时间指示器生成密码;所述第二模块被设置为:接收与访问数据的请求相关联的密码,至少使用不受信任的时间指示器验证所接收的密码;并且促使将消息传输给所述计算装置,所述消息包括表示用于验证所接收的密码的不受信任的时间指示器的数据,并且所述系统被设置为促使计算装置生成表示在不受信任的时间指示器与第一受信任的时间指示器之间的比较的数据,其中,所生成的数据用于提供所述对数据的访问。

[0008] 在某些情况下,第二模块可以不访问受信任的时间指示器(不与外部元件进行通信)。因此,修改不受信任的时间,可以打开系统,以受到攻击。通过使用不受信任的时间指示器来验证密码,然后,促使将消息传输给计算装置,其中,比较不受信任的时间和受信任的时间,避免攻击的可能性。而且,由于仅仅需要从第二模块中发送一条消息给计算装置或系统,所以减少了用于验证的信令量。

[0009] 在一个实施方式中,所述系统被设置为促使计算装置基于所生成的数据选择性地为系统提供所述对数据的访问。在这个实施方式中,计算装置促进访问所请求的数据。

[0010] 有利地,传输给计算装置的消息可以包括表示第二模块至少使用不受信任的时间指示器对所接收的密码的验证的数据。

[0011] 在一个设置中,所述第一模块和所述第二模块共享唯一地分配给其的密钥,所述第一模块被设置为使用密钥来生成密码,并且所述第二模块被设置为使用密钥来验证所接收的密码。共享的密钥可以储存在第一模块的安全部件内。或者/此外,所述密钥可以储存在第二模块的安全部件内。在其他实施方式中,第一和第二模块不共享用于生成和验证密码的密钥。

[0012] 在一个设置中,所述第一模块包括包含时钟的防损硬件,所述时钟被设置为提供第二受信任的时间指示器。

[0013] 在一些设置中,所述第二模块可以通信地连接至具有时钟的装置,所述时钟被设置为提供不受信任的时间指示器。

[0014] 有利地,在一个设置中,所述系统可以被设置为促使计算装置将包括所生成的数据的消息发送给另一个计算装置,从而为系统提供所述对数据的访问,并且所述另一个计算装置可以被设置为在接收所生成的数据时提供所述对数据的访问。

[0015] 或者,在所请求的数据储存在计算装置处或者由计算装置生成的一个设置中,所述系统可以被设置为促使计算装置基于所生成的数据提供所述对数据的访问。

[0016] 在一些设置中,所述第一模块可以被设置为通过第一模块的接口接收由第二模块或计算装置生成的问询码(challenge code),并且至少使用所述问询码,生成密码。

[0017] 在一些设置中,所述第一模块可以被设置为生成多个密码,所述多个密码中的至少一个密码与所述多密码中的另一个密码不同,并且通过第一模块的接口将至少一个生成的密码提供给用户。

[0018] 有利地,所述第二模块和所述计算装置可以共享另一个密钥,以在其间的通信中使用。

[0019] 在一个设置中,所述第二模块可以被设置为储存所接收的密码,并且比较所接收的密码和任何先前储存的所接收的密码,从而验证所接收的密码。

[0020] 在本发明的一个替换的实施方式中,第二模块可以被设置为从计算装置中接收所生成的数据,并且使用所接收的数据来提供所述对数据的访问。这个实施方式可以与计算装置被设置为基于所生成的数据为系统提供所述对数据的访问的实施方式形成对比,这是因为,在这个实施方式中,第二模块(而非计算装置)促进访问所请求的数据。

[0021] 在一些设置中,所述第一模块和所述第二模块可以通信地断开。这具有不能通过第二模块远程地访问由第一模块生成的密码的优点。因此,为了使用户能够正确地将由第一模块生成的密码输入第二模块内,用户必须占有第一模块。在这种设置中,因此,可以确定用户是否占有第一模块。例如,这可以有利于确定第一模块的用户是否是个人用户。

[0022] 在一些设置中,从计算装置中接收的所述数据包括表示不受信任的时间指示器是否在第一受信任的时间指示器的预定范围内的数据。

[0023] 在一些设置中,所请求的数据可以由第二模块保持,并且所述第二模块可以被配置为使用从计算装置中接收的所述数据,来确定是否提供对所请求的数据的访问。

[0024] 所述第二受信任的时间指示器可以是第一模块的时钟,并且第一受信任的时间指示器可以是与第一模块的时钟同步的时钟。

[0025] 有利地,所述计算装置和所述第二模块可以预先配置有加密密钥,用于签署在其间发送的数据,并且所述第二模块可以被设置为签署传输给计算装置的所述消息,并且验证所述计算装置使用所述加密密钥签署从计算装置中接收的所述数据。

[0026] 在一些设置中,所述第二模块可以被设置为储存所接收的密码,并且比较所接收的密码和任何先前储存的接收的密码,从而验证所接收的密码。

[0027] 根据本发明的第二方面,提供了一种由系统使用计算装置验证访问数据的请求的方法,所述计算装置被配置为与第一受信任的时间指示器进行通信,所述方法包括:至少使用第二受信任的时间指示器在第一模块处生成密码;接收与访问数据的请求相关联的密码;至少使用不受信任的时间指示器在第二模块处验证所接收的密码;并且促使将消息传输给所述计算装置,所述消息包括表示用于验证所接收的密码的不受信任的时间指示器的数据;其中,所述系统促使计算装置生成表示在不受信任的时间指示器与第一受信任的时间指示器之间的比较的数据,其中,所生成的数据用于提供所述对数据的访问,并且其中,所述系统包括第一模块和第二模块。

[0028] 通过参照附图进行的仅仅通过实例提供的本发明的优选实施方式的以下描述,本发明的进一步特征和优点显而易见。

附图说明

[0029] 图1示出了根据本发明的一个实施方式的系统的方框图;

[0030] 图 2 示意性示出了根据本发明的一个实施方式的方法；以及

[0031] 图 3 示意性示出了根据本发明的进一步实施方式的方法。

具体实施方式

[0032] 本发明的实施方式涉及确定是否能够访问所请求的数据、资产或服务。图 1 示出了根据本发明的一个实施方式的系统 10 的方框图。系统 10 包括第一模块 20 和第二模块 30。第一模块 20 被设置为生成密码，并且第二模块 30 被设置为从系统 10 的用户中接收密码并且验证所解释的密码。由虚线 15 表示，在图 1 中所示的实施方式中，第一模块 20 从第二模块 30 中通信地断开。换言之，系统 10 被构造和配置为使在这两个模块 20 和 30 之间没有任何通信的方式（除了通过个人用户以外）。在一个特定的实施方式中，在物理上彼此断开的模块 20 和 30 防止在这两个模块 20 和 30 之间的通信。然而，要理解的是，这两个模块 20 和 30 可以在物理上连接（即，整合），同时通信地断开，例如，如果这连个模块不共享任何共同的电路或系统接口或者包括彼此交换信息的任何其他方式。

[0033] 在一个替换的实施方式中，第一和第二模块 20、30 可以通信地断开。

[0034] 第一模块 20 包括可以作为用户接口的接口 21。接口 21 可以至少包括一个输入和 / 或输出。例如，装置的用户接口的输入可以是按钮、键盘、数字键盘、鼠标、触摸屏、麦克风或允许用户为装置提供输入的任何其他元件。例如，装置的用户接口的输出可以是屏幕、扬声器、盲文编码器、或者能够将信息从装置中输出给接口 21 的用户的任何其他元件。

[0035] 第一模块 20 还可以包括安全部件 22。如下面更详细地所述，在一些实施方式中，安全部件 22 可以储存分配给第一和第二模块的密钥。安全部件 22 还可以包括能够提供受信任的时间指示器（在后文中也称为“第二受信任的时间指示器”）的时钟 23。安全部件 22 可以防干扰；即，安全部件 22 可以被配置为使第二受信任的时间指示器不能改变，因此，信任第二受信任的时间指示器。同样，防干扰表示不能读取所储存的密钥，因此，使用该密钥，无需与第一模块 20 合作。

[0036] 第二模块 30 显示为装置 35 的一部分。装置 35 可以包括接口 31，该接口可以是用户接口，可以包括上面根据接口 21 描述的任何或所有特征。此外，该装置包括能够提供时间指示的时钟。第二模块 30 能够与接口 31 和装置的时钟 33 进行通信，并且同样能够与用户进行通信，尤其以便接收由用户提供的密码，并且能够从时钟 33 中访问时间指示。

[0037] 第二模块 30 本身可以包含安全部件 32。与安全部件 22 一样，在一些实施方式中，安全部件 32 可以储存分配给第一和第二模块的密钥。在一些实施方式中，第二模块和 / 或安全部件 32 可以从装置 35 中去除。由于装置 35 的时钟 33 不是安全部件 32 的一部分，所以由时钟 33 提供的时间指示器不受信任，这是因为该指示器可以由用户或其他当事人（例如，远程对手）改变。

[0038] 第二模块通信地连接至至少一个另一个计算装置或系统，例如，一个或两个计算装置 50 和 60。这种计算装置可以是通过网络连接至装置 35 的服务器。或者，计算装置可以是（例如）通过连接装置 51 和 61 与装置 35 连接的其他形式的计算机，例如，台式计算机。计算装置可以是分布式系统，即，云计算系统或相似的系统。计算装置 50 和 60 可以通过连接装置 52 连接。如下面更详细地所述，计算装置 50 还包括能够提供第一受信任的时间指示器的时钟 53。第二模块 30 可以与计算装置 50 成对。例如，在将加密密钥分配给第

二模块 30 和计算装置 50 以用于在其间进行安全通信的配置工艺期间,第二模块 30 可以与计算装置 50 成对。

[0039] 如上所述,在本实施方式中,第一和第二模块通信地断开。因此,在使用期间,第一模块 20 的接口 21 被配置为给用户提供所生成的密码,显示为方框 40,并且第二模块 30 可进入的接口 31 被配置为从用户 40 中接收密码。

[0040] 在一些实施方式中,第一模块 20 和第二模块 30 可以是单独装置,这些装置可以共同被配置为确定访问数据的请求是否可能源自在物理上占有第二模块 30 的用户。作为一个实例,可以共同制造和销售这两个模块 20 和 30,并且这两个模块由特定的用户占有。在一个实例中,装置 35 可以是通信装置,例如,移动电话或银行读卡器。同样,第二模块可以是 SIM 卡或者能够插入装置 35 内的银行卡。在替换的实施方式中,第一和第二模块 20 和 30 可以是单个装置的元件。

[0041] 第二模块 30 可以通过装置 35 的接口 31 在占有第二模块 30 的用户的控制下进行操作。然而,第二模块 30 还可以在具有与第二模块 30 的通信链路的远程实体的控制下进行操作。在本实施方式中,由于第一模块 20 与第二模块 30 通信地断开,如下面更详细地所述,所以不能通过第二模块 30 的接口 31 或者由远程通信链路控制。

[0042] 装置 35 可以储存与特定的人相关联的机密数据。作为一个特定的实例,第二模块 30 可以储存用户限制的加密密钥,用于将数据解密。此外 / 或者,第二模块 30 可以提供或促进对第三方(例如)在一个或两个计算装置 50 和 60 上在外部储存的机密数据的访问。在后一种情况下,如果确定将数据提供给一个特定的人,即,在物理上占有第一和第二模块 20 和 30 的人(换言之,该数据可以是用户限制的数据),那么第三方可以仅仅允许访问数据。在第三方同意通过特定的装置访问用户限制的数据之前,第三方可以要求装置的拥有人登记在装置与拥有人之间的关联。在这种情况下,然后,第三方可以仅仅将旨在由特定的人接收的数据发送给与这个人相关联的装置。在进一步的实施方式中,如果通过第二模块 30 接收这样做的指导,那么第三方可以采取行动,例如,访问机密信息和 / 或支付数据,并且将其发送给第四方。例如,计算装置 50 可以将机密信息发送给计算装置 60。同样,在本实例中,第二模块 30 可以与特定的人具有登记的关联性,因此,第二模块 30 可以用于确定这个特定的人(即,账户持有人)做出请求。

[0043] 在第二模块 30 包括通信模块时,要理解的是,未授权的个人可以与第二模块 30 进行连接并且远程控制第二模块 30,以将请求发送给第三方。如果第二模块 30 可以确定占有第二模块 30 的用户或者远离第二模块 30 的用户是否做出访问数据的请求,那么可以采取合适的反应行动,例如,在确定远程用户做出请求时,禁止进一步使用第二模块 30。

[0044] 现在,要解释的是,实施方式提供了执行这种确定的方式。第一模块 20 包括电路和 / 或软件,其被构造和配置为基于时钟 23 的受信任的时间指示器(即,上述第二受信任的时间指示器)生成密码。这个电路和 / 或软件可以至少部分包含在安全部件 23 内。

[0045] 如上所述,在一个实施方式中,第一和第二模块 20、30 可以配置有共享的密钥,用于生成和验证密码。在这个实施方式中,第一模块 20 可以被设置为还基于共享的密钥,生成密码。在一个实施方式中,该密钥可以唯一地分配给第一和第二模块 20、30。

[0046] 分配给第一和第二模块 20、30 的密钥可以是 OTP 生成密钥,因此,由第一模块 20 生成的密钥是一次性密码(OTP)。在这个实施方式中,由第一模块 20 生成的后续密码与先

前生成的密码不同，并且每个生成的密钥仅仅对于一个认证企图有效。在一个特定的设置中，所生成的 OTP 与时间相关，并且对于预定的时间段有效。在一个替换的设置中，第一模块 20 可以使用 OTP 生成密钥根据预先生成的密码和第二受信任的时间指示器生成密码。

[0047] 根据由第一模块 20 的时钟 23 提供的第二受信任的时间指示器和 OTP 生成密钥（即，密钥），由第一模块 20 生成 OTP。OTP 可以是 OTP 生成密钥和当前时间的密码函数。在第一模块 20 和第二模块 30 是单个装置的复合部件的情况下，另外，可以根据与该装置唯一地相关联的装置 ID，生成 OTP。这种装置 ID 可以（例如）是 CPU ID 的哈希函数、该装置的 GPU ID 的哈希函数或其组合。在这种情况下，OTP 可以是 OTP 生成密钥、装置 ID 以及第二受信任的时间指示器的密码函数。第二受信任的时间指示器的值在本文中称为“生成时间” T_g ，并且要理解的是，相对于第一模块 20 的时钟 23 进行测量。在这种情况下，如果用于生成时间 T_g 的预定周期内，那么特定的生成的 OTP 可以仅仅用于验证访问数据的请求。在这种情况下，如果时间 T_{RU} 在位于用于在第一模块 20 处生成密码的生成时间 T_g 之前或之后的预定时间段内，那么可以验证所生成的 OTP，在此处，由于在这两个时间指示器之间具有时间漂移，所以 T_{RU} 可以位于 T_g 之前。

[0048] 要理解的是，尽管具有这个名称，可以重新使用 OTP 的可能性还是低，但是有限。然而，先前生成的密码在稍后的时间有效的可能性与随机密码运行的可能性有效地相同，同样，为了本文档的目的，假设在模块的使用期期间，规定的密码仅仅一次有效，因此，该密码是 OTP。此外，如果 OTP 在有效的预定时间段内使用两次，那么拒绝 OTP，这防止了重新使用密码。

[0049] 第二模块 30 还包括电路和 / 或软件，其被构造和配置为基于时钟 33 的不受信任的时间指示器（并且如果这样配置第二模块 30，那么还可选地基于共享的密钥）确定在由时钟 33 的不受信任的时间指示器表示的时间，从第二模块 30 的用户 40 中接收的密钥是否与第一模块 20 生成的密码匹配。而且，至少一部分电路和 / 或软件可以包含在安全部件 32 内。

[0050] 在图 1 中所示的特定实施方式中，密钥唯一地分配给第一和第二模块 20 和 30。换言之，密钥可以与仅仅与第一和第二模块 20 和 30 相关联。然而，这并非基本要求。在实施方式中，第一和第二模块 20 和 30 的安全部件 22 和 32 防损，即，用于生成储存在安全部件 22 和 32 内的密码的密钥和算法不能改变。

[0051] 如上所述，使用合适的算法和时间指示，生成由第一装置 20 生成的密码，因此，该密码是 OTP。时间指示（即，上述第二受信任的时间指示器）可以是（例如）整数，其中，正数通过预定的频率（例如，每隔 30 秒或每隔一分钟）增大。整数可以具有与在过去的已知时间点对应的零值，并且可以设置为在装置的使用期，使整数不翻滚，即，不达到储存整数的寄存器的最大值，从而返回零。这确保了第二受信任的时间指示器具有决不重复的唯一值，因此，使用第二受信任的指示器生成的任何密码不重复。尽管有前述规定，但是显然可以代替使用任何其他受信任的时间指示器。包含在安全部件 23 内的时钟可以生成第二受信任的时间指示器。

[0052] 图 2 示意性示出了根据本发明的一个实施方式的一个示例性方法。在这种方法中，用户 40 做出访问数据的请求，由箭头 74 表示。访问数据的请求可以是（例如）访问限制的网页的请求、访问机密信息的请求或者访问数据的请求，用于能够访问服务。可以在装

置 35 上做出请求,因此,通过第二模块 30,用户可以对任一个计算装置 50 和 60 做出请求。通常,用户 40 希望访问的数据可以是储存在系统 10 的任何元件上或者由该元件生成的数据,或者可以是储存在位于系统 10 的外面的实体(例如,外部数据库或服务器)处或者由该实体生成的数据。第二模块 30 的用户 35 希望访问的数据可以是(例如)在位于系统 10 的外面的服务器上托管的限制的网页,并且在这种情况下,将数据发送给第二模块 30 的服务器可以允许访问网页。下面更详细地解释包含在由第二模块 30 发送的数据内的信息。

[0053] 响应于在步骤 74 中访问数据的请求,在步骤 76 中,第二模块 30 提示用户 40 输入由第一模块 20 生成的密码。然后,在步骤 78 中,例如,通过按压第一模块的接口 21 的按钮,或者另外向第一模块 20 指示需要密码,用户可以促使第一模块 20 生成密码。

[0054] 在步骤 80 中,第一模块 20 使用唯一地分配给第一和第二模块 20 和 30 的密钥以及由时钟 33 提供的第二受信任的时间指示,来生成然后在步骤 82 中提供给用户 40 的密码。例如,所生成的密码可以是一系列数字、一系列字母、字母组合、数字以及其他字符或图像,并且可以(例如)在接口 21 的屏幕上呈现给用户 40。

[0055] 或者,第一模块 20 可以通过固定的时间间隔生成密码(根据共享的密钥以及第二受信任的时间指示器),并且可以在第一模块 20 的接口 21 上自动呈现最近生成的密码。在这种情况下,由于第一模块 20 呈现密码,无需请求,所以不需要步骤 78。

[0056] 在任一种情况下,然后,在步骤 84 中,用户 40 可以将由第一模块 20 生成密码提供给第二模块 30。用户将密码输入装置 35 的接口 31 内,可以这样做,通过该接口,将密码提供给第二模块 30。在步骤 86 中,然后,第二模块 30 使用唯一地分配给第一和第二模块 20 和 30 的密钥以及装置 35 的时钟 33 的不受信任的时间指示器,来验证从用户 40 中接收的密码是否与由第一模块 20 生成的密码相同。

[0057] 要理解的是,在由第一模块 20 生成的密码输入第二模块 30 内时,必须预先从第一模块 20 中检索密码。在该实施方式中,第一模块 20 从第二模块 30 中通信地断开时,用户 40 非常可能是占有或者至少访问第一模块 20 以及第二模块 30 的人,因此,能够从第一模块 20 中检索密码,并且将该密码手动提供给第二模块 30。

[0058] 如上所述,第一模块 20 和第二模块 30 均可以包括各个安全部件 22 和 32,密钥储存在其内。密码可以唯一地分配给第一和第二模块 20 和 30,并且储存在安全部件 22 和 32 内。换言之,唯一地分配给第一和第二模块 20 和 30 的密钥储存在用户(例如,用户 40)以及同样地可以同意访问第一和第二模块 20 和 30 的任何其他方不能访问的部分第一和第二模块 20 和 30 内。

[0059] 在这种情况下,在制造时,可以将密钥提供给第一和第二模块 20 和 30 的安全部件 22 和 32。在一个实施方式中,安全部件 22 和 32 单独地制造到模块 20 和 30 的其他元件中,因此,位于系统 10 外面的任何实体不能知道在模块 20 和 30 之间的关联以及储存在安全部件 22 和 32 上的密钥。在安全部件 22 和 32 内储存密钥,防止访问模块 20 和 30 的任何用户找出密钥,从而能够解决需要输入第二模块 30 内的密码,以便访问所请求的数据。还防止任何用户修改生成密码的算法,因此,这可以促使第一模块 20 或第二模块 30 生成虚假反应。例如,在第二模块上的算法可以改变,以接受有效的任何输入。

[0060] 本发明的一个特定优点由用于生成和验证密码的密钥唯一地分配给第一和第二模块 20 和 30 这一事实引起。更具体而言,由于在密钥与使用密钥验证密码的模块 30 之

间具有一对一映射，并且在密钥与使用密钥生成密码的模块 30 之间也具有一对一映射，然后，如果密钥被盗用，那么模块 20 和 30 仅仅需要重新配置有新密钥（再次唯一地分配给模块 20 和 30）。例如，这可以通过使用在其上储存了新密钥的新安全部件代替模块 20 和 30 的安全部件 22 和 32 来实现。或者，在模块是较低成本的物品的情况下，例如，电话 SIM（第二模块 30）和相关的密码生成器模块（第一模块 20），可以更换这两个模块。

[0061] 这可以与在背景部分中描述的已知 OTP 系统形成对比，其中，规定的 OTP 密钥唯一地与特定的用户（而非一对模块 20 和 30）相关联。在这个已知的系统中，在 OTP 密钥与使用 OTP 密钥生成密码的装置之间可以具一对多关系。在这种情况下，如果 OTP 密钥被盗用，那么可以通过使用 OTP 密钥的任何装置，代表该用户访问数据。由于 OTP 密钥通常储存在多个 OTP 令牌上并且还尺寸在认证服务器上，所以建立新的 OTP 密钥可以对认证服务器造成相当沉重的负担，这是因为认证服务需要将新的 OTP 生成密钥重新分配给这个用户并且使一组新的 OTP 令牌配置有新的 OTP 生成密钥。

[0062] 在从第二模块 30 接收密码的时间开始的预定时间内的时间，第二模块 30 使用时钟 33 的不受信任的时间指示器以及 OTP 生成密钥（即，共享的密钥）来确定该密码是否与由第一模块 20 生成的密码相同。第二模块 30 接收密码的不受信任的时间指示器的值在本文中称为“不受信任的接收时间” T_{RU} 。

[0063] 第二模块 30 用于验证所接收的密码的方法取决于第一模块 20 用于生成密码的方法。已经了解很多这种方法，并且具体方法被视为在本发明的范围之外。

[0064] 如果在接收时间 T_{RU} 的预定周期内的时间 T_g ，第二模块 30 确定所接收的密码与由第一模块 20 / 本由第一模块生成的 OTP 匹配，那么第二模块 30 验证所接收的密码。

[0065] 然而，这个密码可以由第一模块 20 在更早的时间生成，并且给第二模块 30 重放。如果损害装置 35，并且因此，可以拦截通过接口 31 输入的密码，那么可能发生这种情况。如上所述，密码是使用时间指示生成的一次性密码 (OTP)。因此，在由第一模块 20 生成与由第二模块 30 接收的密码之间的时间延迟对于 OTP 通常足够长，以便不再有效。

[0066] 然而，第二模块 30 仅仅访问不受信任的时间指示器。这通常是因为时间指示器由装置 35 的时钟 33 提供。同样，例如，通过远程访问装置来篡改装置 35，或者通过用户偏好来简单地设置时钟 33，可以相当合法地调整时钟。这表示不受信任的时间指示器可以调整为与由第一模块 20 生成密码的时间对应，因此，与和由对手更早拦截的密码对应的时间对应。这反过来可以促使第二模块错误地确定重放的密码有效。

[0067] 第二模块 30 可以仅仅访问不受信任的时间，这是因为为第二模块 32 或其安全部件 32 提供安全的以及因此受信任的时间不切实际。例如，在安全部件是 SIM 或银行卡的情况下，可以从第二模块 30 中去除功率，同样，在该模块上运行的任何时钟可以耽误时间。这使第二模块 30 依靠如上所述不受信任的装置 35 的时钟 33。

[0068] 同样，一旦第二模块 30 使用不受信任的时间指示器 T_{RU} 验证了所接收的密码，第二模块 30 就在步骤 88 中将消息发送给计算装置 50。该消息包含表示用于验证所接收的密码的时间指示器（即，不受信任的时间戳 T_{RU} ）的数据。该消息还可以包含表示由第二模块 30 接收的密码（使用不受信任的时间）的验证的数据。

[0069] 如上所述，计算装置 50 访问第一受信任的时间指示器，例如，通过时钟 53。这个时钟 53 可以与第一模块 20 的时钟 23 同步。在此处，同步表示计算装置 50 能够访问在第一模

块 20 用于生成密码的时间 T_c 的预定范围（允许在时钟之间漂移）内的时间指示器 (T'_{c_0})。而且，通过共享用于签署并且从而认证在其间发送的消息的加密密钥，可以在计算装置 50 与第二模块 30 之间建立信任，下面更详细地进行讨论。

[0070] 在接收包含不受信任的时间指示器的消息时，计算装置 50 比较在所接收的消息内指示的不受信任的时间指示器和由计算装置 50 的时钟 53 确定的第一受信任的时间指示器 T'_{c_0} 。如果确定不受信任的时间 T_{RU} 在第一受信任的时间 T'_{c_0} 的预定范围内，并且消息表示由第二模块 30 接收的密码有效，那么计算装置 50 确定信任用户 40 访问第一和第二模块 20 和 30。因此，计算装置 50 可以生成表示这个比较的数据，并且使用所生成的数据提供最初在步骤 74 中请求的数据访问。

[0071] 这是因为如果第二模块 30 使用时间戳 T_{RU} 积极地验证所接收的密码，那么用户 40 必须在接近 T_{RU} 的信任时间 T_c 提供由第一模块 20 生成的密码。然后，由此断定，如果 T_{RU} 接近由计算装置 50 确定的信任时间 T'_{c_0} ，那么 T_c 必须也接近当前时间，因此，可以确定在接近由 T'_{c_0} 表示的当前时间（即，在当前时间的预定范围内）的某个时间 T_c ，用户 40 必须提供由第一模块 20 / 本由第一模块生成的密码。因此，用户 40 可能目前占有或者至少访问第一模块 20。由于没有将由第一模块 20 生成的密码自动传输给第二模块 30 的方式，所以占有第二模块 30 的个人也非常可能占有第一模块 20，从而可以将由第一模块 20 生成的密码手动传输给第二模块 30。

[0072] 有利地，如果计算装置 50 确定不受信任的时间戳 T_{RU} 不在受信任的时间 T'_{c_0} 的预定范围内，并且因此从与第一模块 20 的时钟不同步的时间源中获得，那么计算装置 50 可以拒绝访问数据。

[0073] 因此，如步骤 92 所示，计算装置 50 可以与系统的其他部件进行通信，以实现访问数据，从而使用由以上比较生成的数据。例如，计算装置 50 可以将消息发送给表示时间 T_R 是否在预定的时间范围内的第二模块 30。如果时间 T_R 在预定的时间范围内，那么第二模块 30 可以允许访问所请求的数据。或者，如果时间 T_R 在预定的时间范围之外，那么第二模块可以拒绝访问所请求的数据。

[0074] 用户 40 可以请求访问由计算装置 50 在外面保持的数据。在这种情况下，计算装置 50 可以通过将所请求的数据发送给第二模块 30 或通过拒绝访问来做出响应。

[0075] 或者，在进一步的实例中，计算装置 50 可以允许计算装置 60 访问储存在计算装置 50 或第二模块 30 中的任一个或这两个上的数据。在更进一步的实例中，成功的验证可以用于允许计算装置 50 和 / 或第二模块 30 在计算装置 60 上访问数据。

[0076] 在以上实例中，第二模块 30 可以储存预先接收的 OTP 并且可以使预先接收的任何 OTP 无效。对于第二模块 30 同时由远程对手以及占有第一和第二模块 20 和 30 的用户（即，本地用户 40）访问。假设远程用户试图通过复制本地用户 40 预先输入第二模块 30 内的 OTP 来访问数据，第二模块 30 拒绝复制 OTP，作为复制品。在一个设置中，第二模块 30 可以储存有限数量的预先接收的 OTP，以便能够拒绝复制品。所储存的复制品的数量可以使如果复制第二模块 30 不再储存的特定 OTP，那么第三方 100 可能拒绝这个 OTP，这是因为这与在当前时间的预定范围之外的时间戳相关联。

[0077] 包含由第二模块 30 用于验证所接收的密码的不受信任的时间戳 T_{RU} 的消息可以由第二模块 30 签署（例如，使用与第二模块 30 和计算装置 50 相关联的加密密钥），从而允许

计算装置 50 验证消息的来源。这表示如果远程用户试图改变包含不受信任的时间的由第二模块 30 发送的消息,那么计算装置 50 认识到改变了消息,这是因为该消息不包含第二模块的正确的签署,并且拒绝访问相关联的请求的数据。同样,重放的消息(即,由重新发送给计算装置 50 的第二模块 30 预先发送的消息)包含在过去不受信任的时间指示器 T_{RU} ,因此,拒绝这些消息。

[0078] 而且,如果计算装置 50 被配置为将消息发送给第二模块 30,表示所接收的时间戳是否有效,那么也可以签署该消息。这允许第二模块 30 识别由除了计算装置 50 以外的一方发送给第二模块 30 的消息,这些消息可能不受信任。

[0079] 以上内容可以与第二模块 30 从第三方检索时间戳的系统形成对比。在这种系统中,远程用户可能可以观察由占有第一和第二模块 20 和 30 的用户 40 输入的 OTP,并且还可以观察从第三方中接收的时间戳。在稍后的某个时间,这个远程用户可以为第二模块 30 提供所观察的时间戳和所观察的 OTP。在这种情况下,第二模块 30 可以验证远程用户的密码。然而,在根据以上实施方式配置的系统中,第二模块 30 将用于验证密码的时间戳发送给计算装置 50,计算装置 50 能够确定任何时间戳过时并且相应地拒绝访问所请求的数据。

[0080] 根据以上实施方式配置的系统具有以下优点:第二模块能够在验证所提供的密码时,采用第一步骤,无需访问远程时间戳。这加快了验证的时间,这是因为总体上需要为该系统传输仅仅一条消息(步骤 88),以完成验证。通过对比,将受信任的时间戳提供给第二模块 30 的系统需要至少两条消息、受信任的时间的请求以及响应。

[0081] 图 3 示意性示出了用于在可以是计算装置 50 的银行服务提供商与第二模块 30 之间共享临时加密密钥的一个示例性方法,作为提供数据访问的方式。在该实例中,银行服务提供商 50 具有与另一个服务提供商共享的临时加密密钥,该服务提供商可以与计算装置 60 相关联。与服务提供商 60 共享的加密密钥和与第二模块 30 共享的加密密钥共同用于认证和/或加密/解密在第二模块 30 与服务提供商 60 之间发送的消息,下面更详细地进行讨论。

[0082] 第二模块 30 和银行服务提供商 50 已经具有预先分配的加密密钥,用于加密和认证在其间发送的消息,如上所述。而且,银行服务提供商 50 可以储存在第二模块 30 与特定的银行账户持有人之间的关联。

[0083] 如上所述,第二模块 30 没有与第一模块 20 的时钟同步的时钟。然而,银行服务提供商 50 具有与第一模块 20 的时钟同步的时钟(例如,这两个时钟都可以根据世界时间运行,或者银行服务提供商 50 能够在第一模块 20 上获得时间戳)。

[0084] 在这个特定的实例中,用户 40 在步骤 96 中通过第二模块 30 和装置 35 从银行服务提供商 50 中请求临时加密密钥。在请求访问临时加密密钥时,用户 40 可以将信息提供给识别特定的银行账户持有人的第二模块 30 和/或装置 35,用户 40 想要获得关于该信息的临时加密密钥。

[0085] 在接收临时加密密钥的请求(即,数据的请求)时,第二模块 30 将消息(步骤 98)发送给银行服务提供商 50,表示用户 40 做出了访问临时加密密钥的请求,并且表示模块 20 和 30 可用于生成和验证密码。该消息(在步骤 98 中发送)通知银行服务提供商 50 能够确定访问临时加密密钥的请求(在步骤 98 中)是否源自于在物理上占有第一和第二模块 20 和 30 的用户。

[0086] 因此,如步骤 74' 所示,银行服务提供商 50 可以请求第二模块提供提供了正确密码的指示。在该实施方式中,该方法总体上如上所述参照步骤 76 到 88 进行,从第一模块中请求密码并且由第二模块验证该密码。

[0087] 然而,此外,问询码可以用于提供进一步的安全性。在步骤 74' 中,问询码可以由第二模块 30 生成或者可以由第二模块 30 从银行服务提供商 50 中接收。在步骤 76 中,将问询码提供给用户 40,并且在步骤 78 中,用户 40 将问询码提供给第一模块 20。在步骤 80 中,在生成密码 80 时,并且随后,在步骤 86 中,在第二模块验证密码时,第一模块 20 使用问询码。

[0088] 在一个额外步骤(未引用)中,可以请求用户 40 输入预先设置在银行服务提供商 50 与银行账户持有人(即,用户 40)之间的凭证(例如,用户名和 PIN 或密码)。这具有以下优点:银行服务提供商 50 能够验证第二模块 30 的用户 40 是否是识别的银行账户持有人或者用户是否是一个不同的人(例如,这个人可以偷窃模块 20 和 30)。

[0089] 如上所述,在步骤 86 中,第二模块 30 基于可用于第二模块 30 的不受信任的时间指示,并且如果合适的话,基于可以提供的任何问询码,确定从用户 40 中接收的密码是否有效,随后,在步骤 88 中,第二模块 30 发送提供用于验证这个接收的 OTP 的不受信任的时间指示的消息。该消息可以另外包含表示发现所接收的 OTP 有效并且正确的问询码用于生成密码的数据。例如,通过使用在第二模块 30 与计算装置 50 之间共享的加密密钥,可以加密和/或签署该响应。该响应还包含由用户 40 提供的任何用户名、密码等。

[0090] 另一方面,如果第二模块 30 未成功地验证所接收的密码,那么第二模块 30 可以将签署消息发送给银行服务提供商 50,表示发现所接收的 OTP 无效。

[0091] 如果在步骤 88 中发送的消息表示所接收的 OTP 有效,那么银行服务提供商 50 可以比较在步骤 88 中发送的不受信任的时间戳中表示的时间和第一受信任的时间指示器。这个步骤可以包括任何其他形式的认证,例如,如上所述,验证用户名和密码。如果银行服务提供商 50 确定不受信任的时间(在步骤 88 中提供)在预定的时间间隔内,并且如果需要的话,确定任何其他认证凭证(即,用户名和密码)有效,那么银行服务提供商 50 可以将(在步骤 100 中)锁清秋的临时加密密钥发送给第二模块 30,然后,在该模块中储存。

[0092] 在一个替换的实例中,银行服务提供商 50 并不生成和分布临时加密密钥,临时加密密钥可以由服务提供商 60 生成并且发送给银行服务提供商 50,然后,确定是否与在临时加密密钥由银行服务提供商 50 生成的情况下一样,与第二模块 30 共享该加密密钥。或者,临时加密密钥可以由第二模块 30 生成,并且可以(例如)在消息 88 中发送给银行服务提供商 50。在这个设置中,银行服务提供商 50 可以与服务提供商 60 共享临时加密密钥。

[0093] 如上所述,由于由特定的银行账户持有人拥有,所以第二模块 30 登记有银行服务提供商 50。银行服务提供商 50 与第二模块 30 和服务提供商 60 共享临时加密密钥。服务提供商 60 可以已经知道银行账户持有人是第二模块 30 的登记持有人,并且在这种情况下,在与服务提供商 60 共享临时加密密钥时,确定与那些加密密钥相关联的银行账户持有人是服务提供商 60。或者,如果服务提供商 60 还不知道银行账户持有人,那么在共享相关联的临时加密密钥时,银行服务提供商 50 可以给服务提供商 60 提供信息,用于识别服务并且将服务提供给这个银行账户持有人。

[0094] 在本实例中,用户 40 可以请求(步骤 102)访问进一步的服务提供商 60,用于从银

行账户持有人的账户中进行支付或者划拨资金。

[0095] 在一些实施方式中，无需用户输入，第二模块 30、计算装置 50 或计算装置 60 中的任一个也可以生成访问数据的请求，而非从用户 40 中在第二模块 30、计算装置 50 或计算装置 60 中的任一个处接收访问数据的请求。例如，操作计算装置 50 的第三方可以希望确定第二模块 30 的用户 40 是否在物理上占有第二模块 30，从而计算装置 50 将表示其的消息发送给第二模块 30。在接收这个消息时，第二模块 30 提示第二模块 30 的用户 40 将由第一模块 20 生成的密码输入第二模块 30 内，并且该方法如上所述进行。

[0096] 本发明的实施方式可以与一种系统相比较，在该系统中，第二模块 30 不知道由第一模块 20 用于生成密码的密钥，但是在认证服务器（例如，计算装置 50）与第一模块 20 之间共享该密钥。虽然在这种实施方式，无论是受信任还是不受信任，第二模块 30 都不需要访问时间指示，但是该系统可以丧失在第一与第二模块之间唯一地共享密钥的安全性，这是因为然后在第一模块 20 与计算装置 50 之间共享该密钥。实际上，如果入侵计算装置 50，那么可以暴露很多密钥，与以上系统相反，其中，通过入侵的第一或第二模块，可以暴露仅一个密钥。

[0097] 如上所述，第一和第二模块 20 和 30 可以是相同装置的复合部件，并且可以在该装置内彼此通信地断开。在这些实施方式中，用户 40 能够从第一模块 20 中检索密码并且将该密码输入第二模块 30 内的唯一（实际上可能的）方法是用户 40 是否占有第一模块 20。因此，由此断定，在这种情况下，用户 40 非常可能占有该装置，并且因此，是个人用户。因此，如果第二模块 30 验证从用户 40 中接收的密码，那么第二模块 30 可以确信无疑地确定访问数据的请求源自占有该装置的人（并且因此不是远程实体）。能够访问所请求的数据，可以包括允许访问在该装置上保持的限制的数据，或者在第三方（例如，计算装置 50）保持所请求的数据的情况下，可以包括将数据发送给第三方，用于能够访问所请求的数据。

[0098] 要理解的是，如上所述，用户 40 可以不是单个自然人，同样，第一用户可以给第二用户提供密码，接口 31 从第二用户中接收密码。

[0099] 如上所述，第一模块 20 的接口 21 和装置 35 的接口 31 可以是用户接口。然而，在一些实施方式中，接口可以提供连接至合适的用户接口的输入 / 输出接口。可以这样做，以能够分布第一模块 30 或装置 35，以便可以在物理上分离用户接口，通过这些用户接口，提供密码。

[0100] 以上实施方式要理解为本发明的说明性实例。设想本发明的进一步实施方式。例如，第二模块 30 可以用于允许访问由多个第三方（例如，计算装置 50 和 60）以及未显示的其他系统保持或提供的数据、资产或服务。要理解的是，虽然在上面描述的很多实施方式中，第一和第二模块描述为通信地连接，但是这个特征并非本发明的基本特征，并且在其他实施方式中，第一和第二模块 20 和 30 可能通信地连接。同样，虽然有利，但是第一和第二模块 20 和 30 不需要共享密钥，用于生成和验证密码。要理解的是，相对于任何一个实施方式描述的任何特征可以单独地或者与所描述的其他特征相结合地使用，并且还可以与任何其他实施方式的一个或多个特征或者任何其他实施方式的任何组合相结合地使用。而且，在不背离在所附权利要求中限定的本发明的范围的情况下，还可以使用上面未描述的等同物和修改。

[0101] 以下编号条款陈述了本发明的优选实施方式：

[0102] 1. 一种用于验证访问数据的请求的系统,所述系统访问被配置为与第一受信任的时间指示器进行通信的计算装置,所述系统包括:

[0103] 第一模块,访问第二受信任的时间指示器;以及

[0104] 第二模块,访问不受信任的时间指示器,其中,

[0105] 所述第一模块被设置为至少使用所述第二受信任的时间指示器生成密码;

[0106] 所述第二模块被设置为:

[0107] 接收与访问数据的请求相关联的密码,至少使用不受信任的时间指示器验证所接收的密码;并且

[0108] 促使将消息传输给所述计算装置,所述消息包括表示用于验证所接收的密码的不受信任的时间指示器的数据;并且

[0109] 所述系统被设置为促使计算装置:

[0110] 生成表示在不受信任的时间指示器与第一受信任的时间指示器之间的比较的数据,并且

[0111] 基于所生成的数据选择性地为系统提供所述对数据的访问。

[0112] 2. 根据条款 1 所述的系统,其中,传输给计算装置的消息包括表示第二模块至少使用不受信任的时间指示器对所接收的密码的验证的数据。

[0113] 3. 根据条款 1 或 2 所述的系统,其中,所述第一模块和所述第二模块共享唯一地分配给其的密钥,所述第一模块被设置为使用密钥来生成密码,并且所述第二模块被设置为使用密钥来验证所接收的密码。

[0114] 4. 根据条款 3 所述的系统,其中,所述密钥储存在第一模块的安全部件内。

[0115] 5. 根据条款 1 到 4 中任一项所述的系统,其中,所述密钥储存在第二模块的安全部件内。

[0116] 6. 根据条款 1 到 5 中任一项所述的系统,其中,所述第一模块包括包含时钟的防损硬件,所述时钟被设置为提供第二受信任的时间指示器。

[0117] 7. 根据条款 1 到 6 中任一项所述的系统,其中,所述第二模块通信地连接至具有时钟的装置,所述时钟被设置为提供不受信任的时间指示器。

[0118] 8. 根据条款 1 到 7 中任一项所述的系统,其中,所述计算装置被设置为将包括所生成的数据的消息发送给另一个计算装置,从而为系统提供所述对数据的访问,所述另一个计算装置被设置为在接收所生成的数据时提供所述对数据的访问。

[0119] 9. 根据条款 1 到 7 中任一项所述的系统,其中,所请求的数据储存在计算装置处或者由计算装置生成,并且所述计算装置被设置为基于所生成的数据提供所述对数据的访问。

[0120] 10. 根据条款 1 到 9 中任一项所述的系统,其中,所述第一模块被设置为通过第一模块的接口接收由第二模块或计算装置生成的问询码,并且至少使用所述问询码,生成密码。

[0121] 11. 根据条款 1 到 10 中任一项所述的系统,其中,所述第一模块被设置为生成多个密码,所述多个密码中的至少一个密码与所述多密码中的另一个密码不同,并且通过第一模块的接口将至少一个生成的密码提供给用户。

[0122] 12. 根据条款 1 到 11 中任一项所述的系统,其中,所述第二模块和所述计算装置共

享另一个密钥,以在其间的通信中使用。

[0123] 13. 根据条款 1 到 12 中任一项所述的系统,其中,所述第二模块被设置为储存所接收的密码,并且比较所接收的密码和任何先前储存的所接收的密码,从而验证所接收的密码。

[0124] 14. 一种用于验证访问数据的请求的系统,所述系统包括:

[0125] 第一模块,访问第二受信任的时间指示器;以及

[0126] 第二模块,访问不受信任的时间指示器,其中,

[0127] 所述第一模块被设置为至少使用所述第二受信任的时间指示器生成密码;

[0128] 所述第二模块被设置为:

[0129] 接收与访问数据的请求相关联的密码,

[0130] 至少使用不受信任的时间指示器验证所接收的密码,并且

[0131] 促使将消息传输给所述计算装置,所述消息包括表示用于验证所接收的密码的不受信任的时间指示器的数据;并且

[0132] 从计算装置中接收表示在不受信任的时间指示器与进一步受信任的时间指示器之间的比较的数据,并且

[0133] 使用所接收的数据来提供所述对数据的访问,

[0134] 其中,所述第一模块和第二模块通信地断开。

[0135] 15. 根据条款 14 所述的系统,其中,从计算装置中接收的所述数据包括表示不受信任的时间指示器是否在第一受信任的时间指示器的预定范围内的数据。

[0136] 16. 根据条款 14 或 15 所述的系统,其中,所请求的数据由第二模块保持,并且所述第二模块被配置为使用从计算装置中接收的所述数据,来确定是否提供对所请求的数据的访问。

[0137] 17. 根据条款 14 到 16 中任一项所述的系统,其中,所述第一模块访问的所述受信任的时间指示器是第一模块的时钟,并且所述计算装置访问的进一步受信任的时间指示器是与第一模块的时钟同步的时钟。

[0138] 18. 根据条款 14 到 17 中任一项所述的系统,其中,所述计算装置和所述第二模块预先配置有加密密钥,用于签署在其间发送的数据,并且其中,所述第二模块被设置为签署传输给计算装置的所述消息,并且验证所述计算装置使用所述加密密钥签署从计算装置中接收的所述数据。

[0139] 19. 根据条款 14 到 18 中任一项所述的系统,其中,所述第二模块被设置为储存所接收的密码,并且比较所接收的密码和任何先前储存的接收的密码,从而验证所接收的密码。

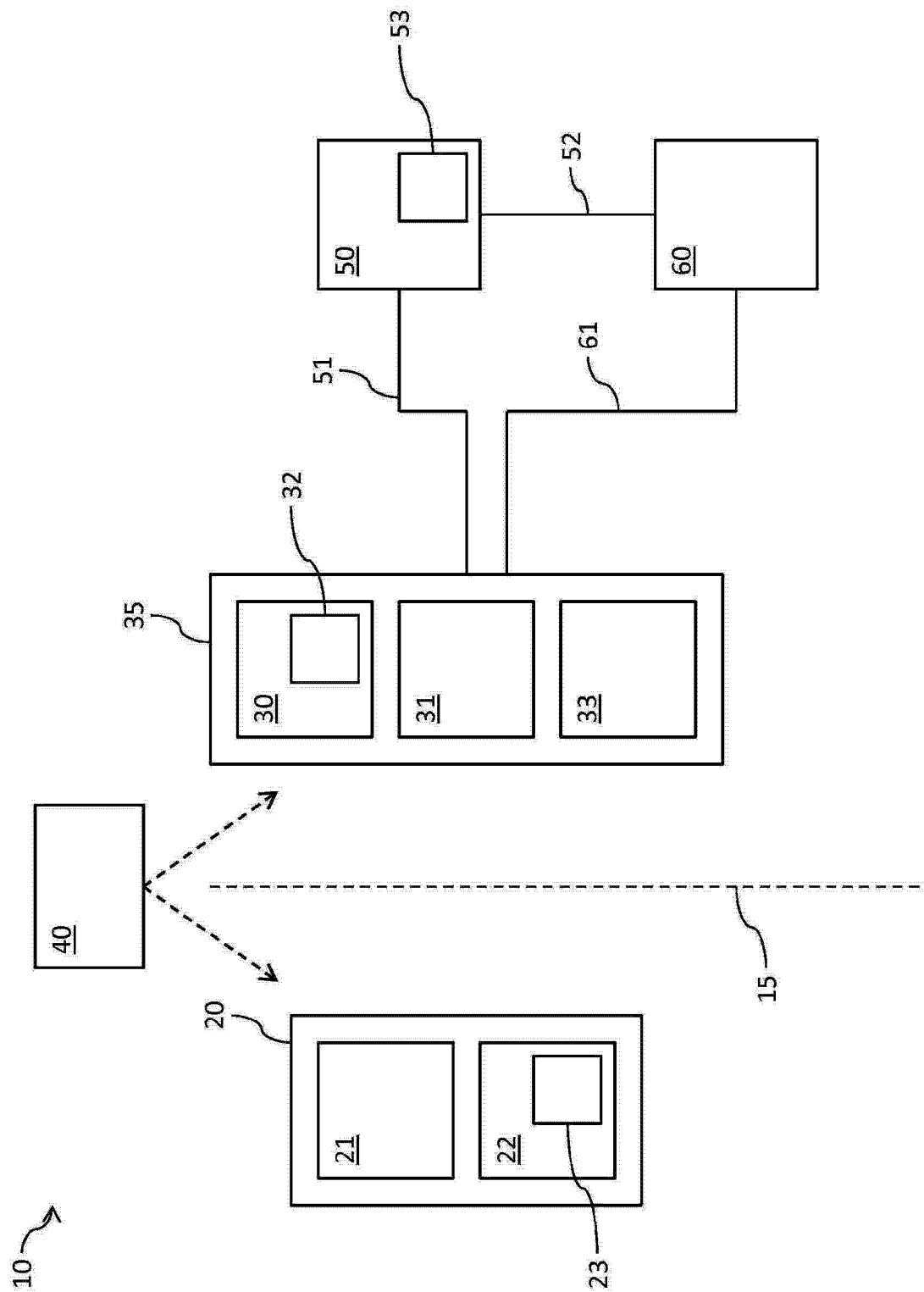


图 1

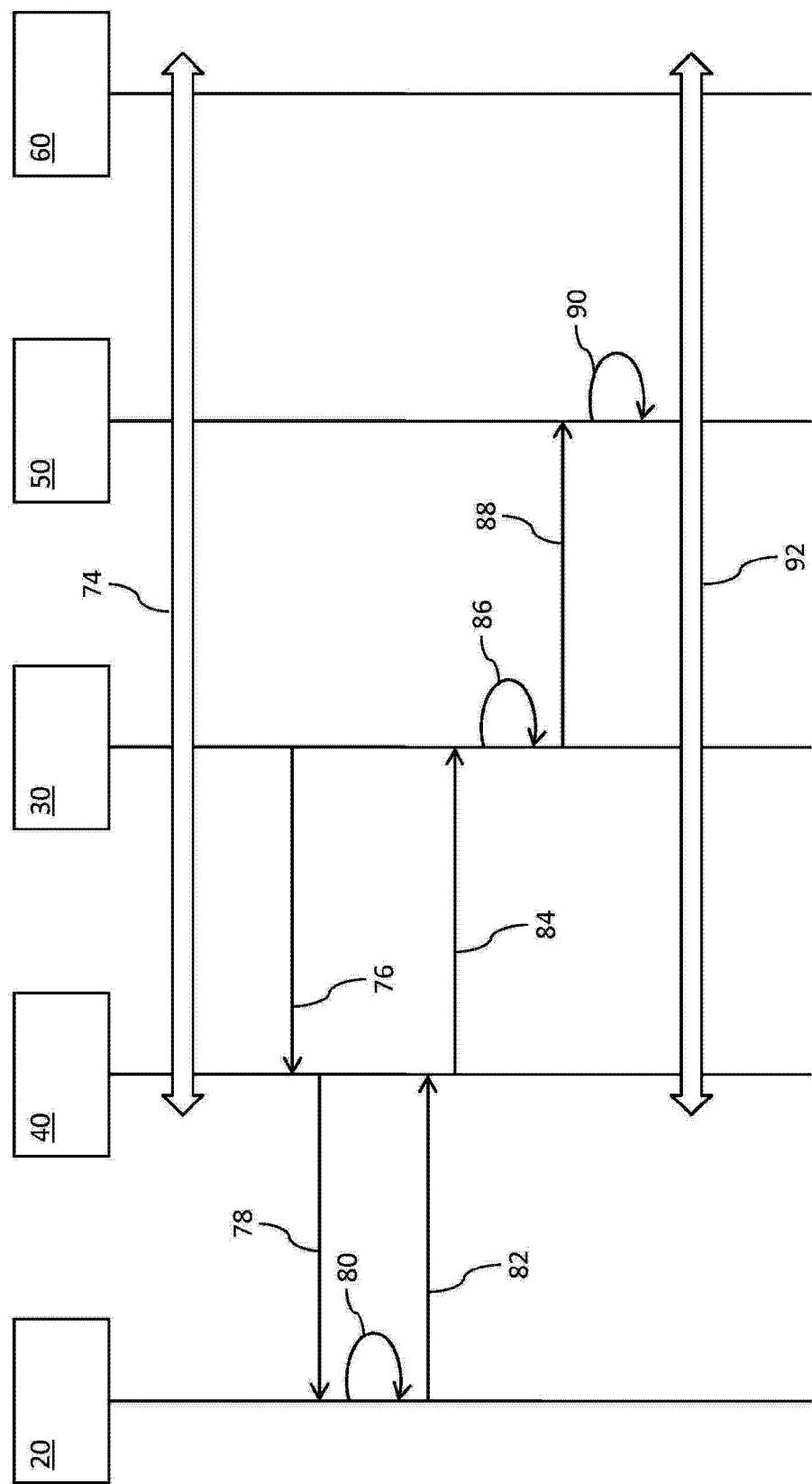


图 2

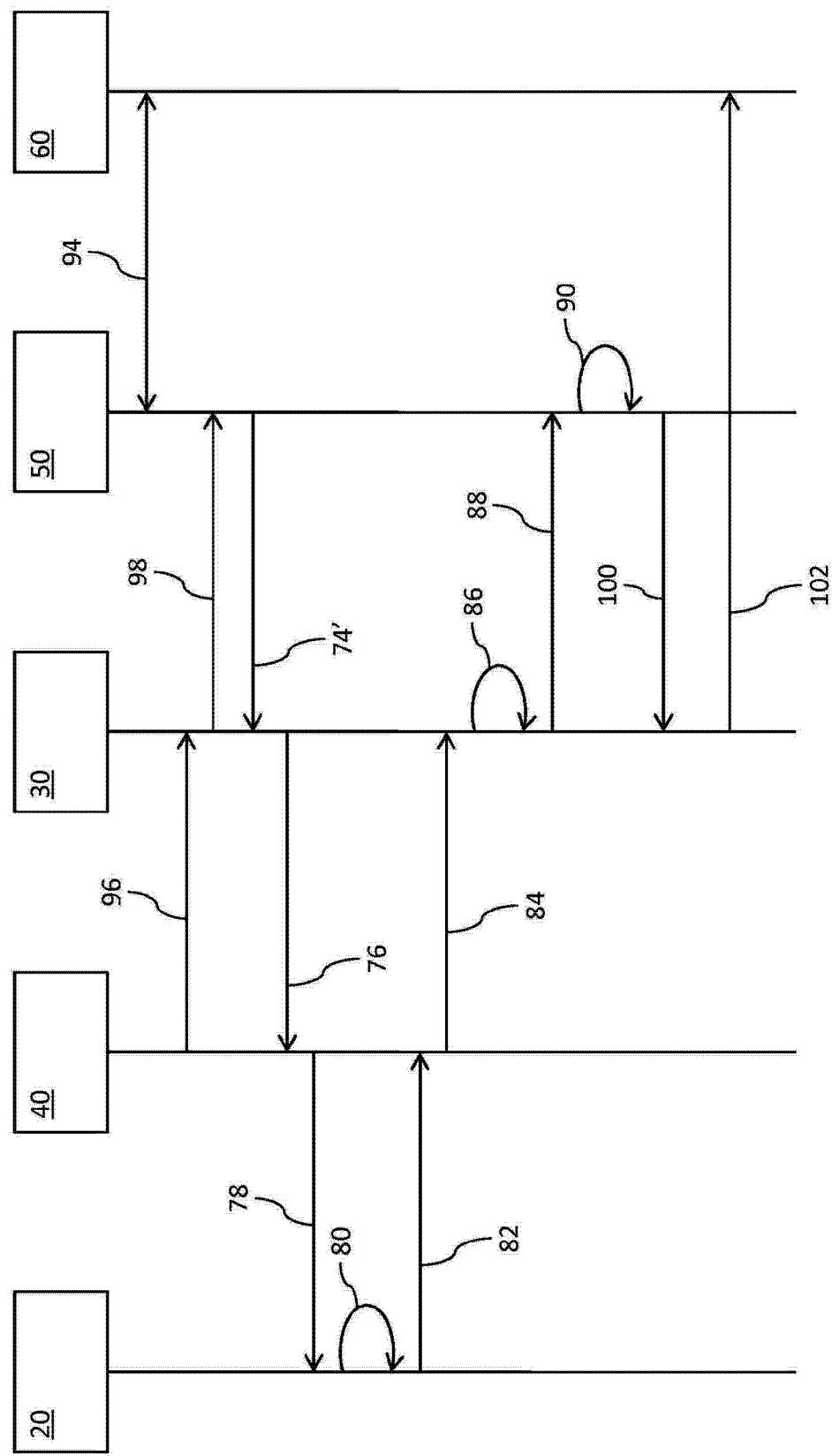


图 3