(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 109644137 A
(43)申请公布日 2019.04.16

(21)申请号 201780053315.4

(22)申请日 2017.07.18

(30)优先权数据
102016213104.4 2016.07.18 DE

(85)PCT国际申请进入国家阶段日
2019.02.28

(86)PCT国际申请的申请数据
PCT/EP2017/068161 2017.07.18

(87)PCT国际申请的公布数据
WO2018/015402 DE 2018.01.25

(71)申请人 比塔根图两合公司
地址 德国慕尼黑

(72)发明人 M.埃登施因克 M.森夫

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邸万奎

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

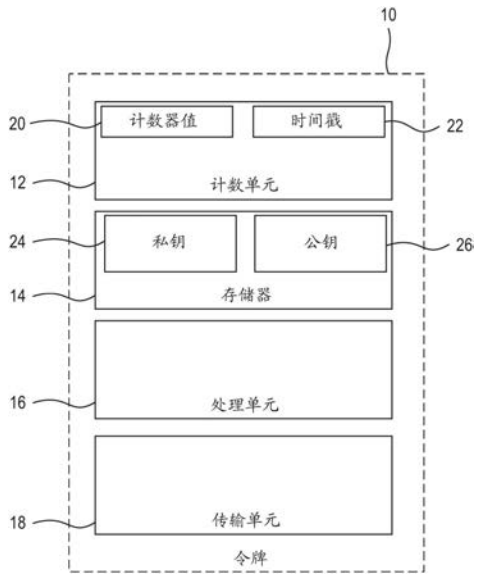
权利要求书2页 说明书11页 附图4页

(54)发明名称

具有签名消息的基于令牌的认证

(57)摘要

本发明涉及一种用于向计算机系统(70)认证用户的方法(50),该方法包括在令牌(10)中运行以下步骤:通过利用在令牌(10)中实施的计数单元(12)生成(52)计数器值(20、22),其中生成的计数器值(20、22)的至少一部分形成严格单调的序列;取决于生成的计数器值(20、22)生成(54)消息(30);通过利用用户的私钥(24)签名(56)生成的消息(30),其中私钥(24)存储在令牌(10)中,并且其中私钥(24)或其副本不向计算机系统(70)提供;以及将签名的消息传输(58)到计算机系统(70)。本发明还涉及用于向计算机系统(70)认证用户的令牌(10)以及在计算机系统(70)上运行的用于认证用户的方法(60)。根据本发明的令牌(10A、10B)可以以移动设备(80A、80B)中的软件或硬件实施。本发明还涉及包括指令的计算机程序产品,该指令当在处理器(72、82)上运行时,实施本发明方法的步骤。



CN 109644137 A

1.一种用于向计算机系统(70)认证用户的方法(50),所述方法包括在令牌(10)中执行的以下步骤:

通过利用在所述令牌(10)中实施的计数单元(12)生成(52)计数器值(20、22),其中生成的计数器值(20、22)的至少一部分形成严格单调的序列,

取决于生成的计数器值(20、22)生成(54)消息(30),

通过利用用户的私钥(24)签名(56)生成的消息(30),其中所述私钥(24)存储在所述令牌(10)中,并且其中所述私钥(24)或其副本不提供给计算机系统(70),以及

将签名的消息传输(58)到计算机系统(70)。

2.如权利要求1所述的方法(50),其中所述令牌(10)适于作为输入设备(人机接口设备)登录到计算机系统(70),并且

其中传输(58)签名的消息包括编码和传输作为输入数据,特别是作为键盘输入数据的签名的消息。

3.如权利要求1或2所述的方法(50),

其中,取决于所述令牌(10)的标识特征(36)进一步生成消息(30)。

4.如权利要求1或3中任一项所述的方法(50),

其中所述计数单元(12)包括时钟,并且其中所述计数器值(20、22)包括时间戳(22)。

5.如权利要求1或4中任一项所述的方法(50),

其中,所述签名的消息的传输(58)是经由通用串行总线(USB)、蓝牙或近场通信(NFC)。

6.一种用于向计算机系统(70)认证用户的令牌(10),包括:

计数单元(12),用于生成(52)计数器值(20、22),其中生成的计数器值(20、22)的至少一部分形成严格单调的序列,

存储器(14),用于存储与用户相关联的私钥(24),

处理单元(16)

用于取决于生成的计数器值(20、22)生成(54)消息(30)并且用于通过利用私钥(24)来签名(56)生成的消息(30),和

传输单元(18),用于将签名的消息传输到计算机系统(70),

其中所述令牌(10)适于执行如权利要求1至5中任一项所述的方法(50)。

7.如权利要求6所述的令牌(10),

其中所述令牌(10)包括用于启动认证过程(50)的第一控制元素。

8.如权利要求6或7所述的令牌(10),

其中所述存储器(14)包括与所述私钥(24)相关联的公钥(26)。

9.如权利要求8所述的令牌(10),

其中所述令牌(10)包括用于启动到计算机系统(70)的公钥(26)传输的第二控制元素。

10.一种用于认证用户的方法(60),所述方法包括在计算机系统(70)中执行的以下步骤:

从如权利要求6至9中任一项所述的令牌(10)接收(62)签名的消息,其中所述签名的消息取决于所述令牌(10)的计数器值(20、22),

借助于标识特征(36)将用户分配给(64)所述签名的消息,

通过利用用户的公钥(26)验证(66)所述签名的消息的签名,以及

将从消息(30)提取的计数器值(20、22)与用户的先前认证过程(60)的计数器值(20、22)进行比较(68)，

其中用户的连续认证过程的计数器值(20、22)的至少一部分形成严格单调的序列。

11.一种包括硬件实施的令牌(10A)的移动设备(80A)，其中所述硬件实施的令牌(10A)包括如权利要求6至9中任一项所述的令牌(10)。

12.一种包括软件实施的令牌(10B)的移动设备(80B)，其中所述软件实施的令牌(10B)包括指令，当所述指令在所述移动设备(80B)的处理器(82)上运行时，实施如权利要求1至5中任一项所述的方法(50)的步骤。

13.一种包括指令的计算机程序产品，当所述指令在处理器(72、82)上运行时，实施如权利要求1至5或权利要求10中任一项所述的方法(50、60)的步骤。

具有签名消息的基于令牌的认证

技术领域

[0001] 本发明一般涉及保护计算机系统的领域,更具体地,涉及向计算机系统认证用户。

背景技术

[0002] 授权用户访问计算机系统上的应用和数据需要验证用户的身份。只有在成功验证声明的身份之后,才允许访问应用和数据。

[0003] 验证用户的声称的身份的常见做法是查询静态密码。该过程具有用户必须进行容易出错且对用户来说烦人的密码输入的缺点。此外,静态密码查询具有通常需要记下安全密码并且密码能够由未经授权的人记录的缺点。另一方面,如果选择简单密码,则能够容易地猜测并因此例如借助于探测(“强力攻击”)来在足够短的时间段内确定。

[0004] US 2010/0049984A1公开了一种用于向服务器认证移动电话的用户的方法。移动电话包含在其中存储有用户标识的集成电路。用户标识和当前时间借助于签名密钥来签名并被传输到服务器。服务器使用相同的签名密钥来验证签名的有效性,因此充当用户和服务器的公共密钥。

[0005] 从JP 2012-138650A中已知一种用于基于时间的数据流的认证的方法。从数据流中生成由电子签名生成的哈希数据。

[0006] 从US 8,370,952B1中已知一种令牌,其中令牌的所有权通过由身份提供者执行的私钥加密来匿名化。具有相应公钥的服务提供者能够在不能解密的情况下得出有效身份。

[0007] WO 2007/122224A1公开了一种USB(Universal Serial Bus,通用串行总线)令牌,其作为输入设备(人机接口设备,HID)登录到计算机系统并且能够在按下按钮时发出击键(keystroke)。这允许输入设备借助于对称方法传输预定义的击键,诸如明文密码或对计算机系统加密。

[0008] 该USB令牌具有以下缺点:多个应用的单独集成需要使用相同的密码,或者如果USB令牌能够存储多个密码,则需要用户做出存储在USB令牌中的哪个密码将被传输到相应的应用的特定选择。

[0009] 另外,诸如密码的秘密(secret)的传输通常会带来安全风险。挑战-响应(challenge-response)方法通过不传输用于授权的秘密(共享秘密)而是通过向认证机构(authenticating body)提出挑战来减少关联的风险。基于待授权用户的响应,认证机构能够识别出他知道秘密。

[0010] 为了保护因此而传输的消息,能够使用公钥基础结构(Public Key Infrastructure,PKI)。公钥基础结构的每个用户被分配了公钥和私钥两者。该密钥对能够与由受信任的证书颁发机构颁发的证书相关联,该证书将相应的公钥和私钥绑定到关联的用户。

[0011] 为了确保安全性,必须确保用户的私钥保密,并且仅对分配了该密钥的授权用户可用以生成签名或解密消息。通常,智能卡或USB令牌用于存储私钥和公钥以及证书,并执行与私钥相关联的加密计算。

[0012] 使用这样的智能卡和USB令牌具有以下缺点:需要对应用的认证例程进行特定调整,因为代替与传统输入设备的通信,必须将消息发送到智能卡。智能卡对收到的消息进行签名,并将签名的消息发送给应用以便审核(review)。

发明内容

[0013] 本发明的一个目的是以一种一方面提供高级别的安全性、另一方面尽可能少的涉及现有应用中的调整工作的形式来实现用户认证。

[0014] 本发明基于如下概念:为了用户的安全认证,不需要用户和认证者之间的共享信息,这必须保密。以下对于本发明而言是必须的:(i)使用特定的设置来签名消息,(ii)以非对称加密方案来验证签名的有效性,以及(iii)基于消息的特定结构,在合理时间间隔内识别已经接收的消息的重复验证。

[0015] 本发明的优点在于认证方不需要秘密。认证需要的所有数据可能是公共知识。

[0016] 根据本发明的第一方面,提供了一种用于向计算机系统认证用户的方法,该方法包括在令牌中执行的以下步骤:

[0017] -通过利用在令牌中实施的计数单元生成计数器值,其中生成的计数器值的至少一部分形成严格单调的序列,

[0018] -取决于生成的计数器值生成消息,

[0019] -通过利用用户的私钥对生成的消息进行签名,其中私钥存储在令牌中,并且其中私钥或其副本未提供给计算机系统(70),以及

[0020] -将签名的消息传输到计算机系统。

[0021] 优选地,令牌被安排成使得不能从令牌外部的资源读取存储在令牌中的私钥。

[0022] 在本发明的优选实施例中,令牌被设置为作为输入设备(Human Interface Device,人机接口设备)登录到计算机系统。签名的消息的传输可以包括作为输入数据,特别是作为(例如借助于键盘扫描码的)键盘输入数据,来编码和传输签名的消息。

[0023] 能够取决于一个或多个附加计数器值生成消息。计数器值可以是数字计数器值,例如整数,其在再次轮询计数单元时递增。然而,也可以考虑其他类型的计数器值。因此,可以提供作为时间戳的例如包括日期的时间指示。可以根据传统日历(例如公历)对包含在时间指示中的日期进行编码。还可以提供日期的数字表示,例如从初始日期开始的秒数。

[0024] 在本发明的优选实施例中,计数单元包括时钟。计数器值可以包括时间戳。在这种情况下,例如,在消息中编码的计数器值能够基于时间戳,或者在消息中编码的计数器值还能够除了数值计数器值之外而存在。

[0025] 基本上,计数器值能够由任何内容表示,该任何内容能够作为随后针对先前生成的计数器值而生成的计数器值来通过计数单元的更新查询来标识。该规则必须至少适用于连续地生成的计数器值的足够大的部分。在这方面,生成的相同类型的计数器值的严格单调的部分适用。术语“部分”包括紧接在彼此之后生成的一定数量的计数器值,它们一起形成计数器值的一部分。要适用于至少一部分计数器值的严格单调的边界条件是由于在存储和处理期间计数器值的限制。在一定数量的生成的计数器值之后,计数器值将达到上限阈值,该上限阈值在计数器溢出之前发生。最迟在这种情况下,计数器将必须在下一次计数时使用与下限阈值相对应的计数器值继续。出于安全原因,计数器的宽度将相应地大。在优选

实施例中，计数器包括32位，并且因此能够区分大约40亿个计数器值。

[0026] 如果为了能够重用(reuse)具有特定计数器值的截获消息，潜在攻击者必须花费大量时间，则计数器的宽度被选择为足够大，因为在此期间发生了如此多的查询，截获的消息必须再次被视为后续消息。

[0027] 在本发明的优选实施例中，取决于令牌的标识特征进一步生成消息。标识特征允许接收计算机系统标识与令牌相关联的用户。需要该信息来标识验证接收的消息的签名所需的关联公钥。只要还能够另外确定关联的公钥，则签名的消息中的标识特征的传输不是强制性的。用户可以选择用户作为计算机系统上的认证过程的一部分，例如，通过经由键盘手动输入他的用户名(登录)。

[0028] 也能够取决于协议版本生成消息。从接收的消息中提取协议版本允许对生成的消息使用不同的格式，因为接收计算机系统能够取决于编码的协议版本来不同地处理消息。

[0029] 也能够取决于标志生成消息。标志能够用于指示在创建签名的消息时的问题。优选地，标志指示令牌中的电源故障。因此，标志指示令牌中的可选存在的实时时钟因为实时时钟已经被重置为起始值或者在电源故障期间被停止而不能生成正确的时间戳的状态。可替代地或另外地，标志可以发信号通知待处理的计数器溢出，使得接收计算机系统可以随后解释与低于上阈值的阈值相对应的计数器值。

[0030] 也能够取决于用户定义的前缀(prefix)生成消息。用户定义的前缀优选地用于分组令牌，例如用于标识公司的部门。用户定义的前缀还能够用于区分用户的不同令牌，例如区分用户的角色(私人令牌、商业令牌)。

[0031] 取决于所支持的消息的最大长度，可以在计算机系统上可用的消息中合并附加内容以供进一步处理。

[0032] 优选地，要签名的消息包括32个字节的最小长度，例如，该32个字节被编码为ASCII字符。如果要签名的消息短于最小长度，则能够根据定义的填充规则用填充字节填充。签名生成后，填充字节能够被再次移除。

[0033] 优选地，没有填充字节的要签名的消息具有23字节的长度，其借助于填充字节增加到32字节。如果在传输消息之前从签名的消息中移除填充字节，则必须使认证计算机系统知道填充规则，使得将未传输的填充字节添加回要认证的签名的消息，以用于签名的适当认证。填充字节可以是位于要签名的消息中的定义的位置的单ASCII字符。签名优选地包括64个字符，每个字符一个字节，并附加到消息中。签名的消息因此包括87个字节，其23个字节用于移除填充字节之后的消息并且其64个字节用于扩展到32个字节的消息的签名。

[0034] 在优选实施例中，根据Base64或类似格式对签名的消息进行编码，使得消息的长度以4/3的比率增加，例如，从87字节增加到116字节。在微软公司(Microsoft Corporation)的Windows系列操作系统中，输入密码的限制为127个字节。在这方面，将接收的消息读入密码输入字段是可能的。

[0035] 在一个实施例中，令牌包括用于检索安全特征的装置，诸如用于密码查询的键盘。取决于所请求的密码，在该实施例中也生成该消息。可替代地，密码与签名的消息一起传输。在优选实施例中，保留8个字节用于与签名的消息一起或在签名的消息中传输密码。

[0036] Base64编码的优点是，在传输Base64编码和签名的消息时，消息中没有特殊字符。Base64编码基于使用64个ASCII字符，包括26个小写和大写字母(a-z，A-Z)、数字0-9和

ASCII字符加(“+”)和斜杠(“/”)。在优选实施例中,使用具有ASCII字符逗号(“,”)和分号(“;”)的Base64衍生物代替加号(“+”)和斜线(“/”)。

[0037] 在本发明的优选实施例中,经由通用串行总线(Universal Serial Bus,USB)、蓝牙或近场通信(Near Field Communication,NFC)发送传输的和可选编码的消息。优选地,借助于在计算机系统上注册为人机接口设备并且例如被识别为USB或蓝牙键盘的令牌,将签名的和可选编码的消息作为模拟键盘输入发送到计算机系统。签名的和可选编码的消息的传输能够经由键盘扫描码完成。键盘扫描码表示键盘上的击键的编码,键盘扫描码在计算机系统中被分配了ASCII码。

[0038] 优选地,在相应的关联键盘扫描码的编码中传输Base64编码的消息的ASCII字符。应该注意,ASCII字符和键盘扫描码之间的分配取决于计算机系统的语言配置。虽然大量键盘扫描码独立于设置语言,然而,取决于当前键盘的给定语言,存在由不同键盘扫描码表示的单独ASCII字符。

[0039] 该行为的第一个示例是英语键盘上“z”键的键盘扫描码,其在德语键盘上被解释为“y”。第二个示例是英语键盘上“z”键的键盘扫描码,其在法语键盘上被解释为“w”。此外,法语键盘上的键“;”与德语键盘上的键“,”交换。在西里尔(Cyrillic)键盘上,几乎所有英语键盘扫描码都与具有不同ASCII码的特定西里尔字符相对应。在这方面,通过生成涉及语言差异的两个不同的先前商定的ASCII字符的键盘扫描码并检索由计算机系统生成的ASCII码来推断设置的语言配置是可能的。

[0040] 在优选实施例中,向签名的和可选编码的消息提供验证码。验证码包括适合于区分不同的语言配置的至少两个先前商定的ASCII字符的键盘扫描码。优选地,消息的验证码是前缀的。作为验证码,例如,从预定义的语言中选择的以下一对字符:在德语键盘上“y”和“,”能够用于区分,其与英语键盘上键“z”和“;”相对应。在一些实施例中,验证码被包括作为要签名的消息中的属性。

[0041] 在Base64编码的情况下,消息的可用“字母”由64个字符组成,其优选地由键盘扫描码表示。在一些实施例中,Base64编码的64个字符由字母表的26个字母(a-z)、数字0-9、shift键的键盘扫描码和逗号(“,”)的键盘扫描码表示。由于shift键影响字母和逗号字符,因此与shift键组合能够显示字符A-Z和分号(=德语键盘上的shift键加逗号)或“小于”字符(=英语键盘上的Shift键加逗号),使得能够显示总共64个字符。如果令牌和计算机系统使用相同的语言配置,则计算机系统能够通过应用从键盘扫描码到由标识的语言配置产生的ASCII字符的映射来将接收的消息的键盘扫描码转换为编码为ASCII字符的签名的消息。

[0042] 根据本发明的第二方面,提供了一种用于向计算机系统认证用户的令牌,该令牌包括:用于生成计数器值的计数单元,其中生成的计数器值的至少一部分形成严格单调的序列;用于存储与用户相关联的私钥的存储器;用于取决于生成的计数器值生成消息并且用于通过利用私钥对生成的消息进行签名的处理单元;和用于将签名的消息传输到计算机系统的传输单元,其中令牌适于执行根据本发明第一方面的方法。私钥不需要被计算机系统可访问以认证用户。

[0043] 令牌可以集成到专用硬件(“硬件令牌”)中,既可以作为独立的电子设备,又可以作为更全面的电子设备的一部分。

[0044] 以硬件实施的令牌的组件可以经由总线系统,例如通过I^2C总线,彼此通信。

[0045] 存储器可以包括存储用户的私钥的安全芯片。优选地，私钥通过在安全芯片上提供签名消息的功能而不离开安全芯片。安全芯片可以包括用于读取和存储私钥的接口。优选地，安全芯片具有用于生成私钥和关联的公钥的功能以及用于读取公钥的功能。

[0046] 计数单元可以包括用于计数的一个或多个组件，其中每个单独的组件可以是例如硬件计数器或实时时钟(Real-Time Clock，RTC)。

[0047] 在优选实施例中，硬件计数器根据请求提供已从先前请求递增的整数。如果硬件计数器达到上阈值，例如在计数器马上溢出之前，硬件计数器能够恢复到下阈值。达到上阈值或继续下阈值可以在消息中通信到计算机系统。可以向计算机系统通知计数器值的结构，并且因此知道当达到上阈值时，将跟随下阈值。

[0048] 优选地，实时时钟是独立于外部时间信号在令牌中操作的时钟。实时时钟能够进行温度补偿以提高准确度。实时时钟也能够是能够从GPS信号中提取时间的GPS接收器。实时时钟可以是诸如DCF77的无线电时钟接收器。实时时钟也可以是用于接收在认证过程中与令牌相关联的计算机系统的时间的单元。实时时钟还可以是用于通过因特网进行通信的单元，该时间是从一个或多个时间服务器获得的。

[0049] 处理单元可以包括用于计算的一个或多个组件，每个单独的组件是中央处理单元(Central Processing Unit，CPU)、微控制器(Microcontroller，MCU)、算术逻辑单元(Arithmetic Logic Unit，ALU)或并行逻辑单元(Parallel Logic Unit，PLU)。因此，处理单元的单独的组件可以负责对消息进行签名，并且一个或多个不同组件可以负责生成一个或多个计数器值。

[0050] 传输单元包括用于将消息传输到计算机系统的一个或多个组件，其中每个单独的组件可以被实施为通用串行总线(USB)、蓝牙或近场通信(NFC)接口。优选地，一旦令牌经由传输单元连接到计算机系统，令牌表示作为要被认证的计算机系统的键盘的功能。除了操作模式“键盘”之外，传输单元还能够具有其他操作模式，例如用于传输存储在令牌中的密钥。如果令牌传输单独的安全特征作为双因素认证的一部分，则该安全特征能够在传输单元的单独的操作模式中传输。

[0051] 术语传输单元不排除传输单元也能够接收数据，例如，用于向计算机系统确认成功接收的数据或用于令牌的配置的数据，例如上传密钥对或接收用于生成密钥对的指令。

[0052] 以硬件实施的令牌可以以具有令牌的组件之间的接口的若干组件实施。令牌优选地包括无线电接口，例如蓝牙和/或近场通信(NFC)。附加模块能够使用另一个接口，例如根据通用串行总线(USB)的接口，来扩展令牌。

[0053] 优选地，通用串行总线(USB)接口具有微控制器，一旦令牌经由USB接口连接到计算机系统，该微控制器就将令牌作为USB键盘登录到计算机系统。

[0054] 硬件实施的令牌可以具有内部电源，这对于仅具有一个或多个无线电接口以与计算机系统通信的令牌特别有利。内部电源可以甚至对于具有有线接口、允许外部电源的令牌也是有利的，尤其是如果令牌的实时时钟需要供应电源。内部电源可以是例如蓄电池、电池或太阳能电池。令牌可以具有到外部电源的接口。

[0055] 在以软件实施的令牌的情况下，像计数单元、存储器、处理单元和传输单元的所述组件能够由其上实施令牌软件的设备的相应组件代替。传输单元可以包括到操作系统的软件接口或设备的应用程序，以向安装有软件令牌的设备认证用户。

[0056] 在本发明的优选实施例中，令牌包括用于启动认证过程的第一控制元素。第一控制元素可以是由用户操作的按钮，以实现(effect)签名的消息的生成和传输。在设备注册为人机接口设备的情况下，令牌在计算机系统中像键盘，其在按下第一控制元素时生成表示签名的消息的模拟击键。

[0057] 在本发明的优选实施例中，存储器包含与私钥相关联的公钥。令牌中不需要公钥来生成签名的消息。然而，对于附加了令牌的任何计算机系统，公钥必须是可访问的，以认证用户。在这方面，有利的是将公钥存放在令牌中，使得能够根据请求将其导入计算机系统。

[0058] 在本发明的优选实施例中，令牌包括用于启动公钥到计算机系统的传输的第二控制元素。第二控制元素可以是按钮。公钥能够经由键盘扫描码传输。令牌另外地能够被设计为USB数据载体，在该USB数据载体上能够存放公钥以便传送到计算机系统。

[0059] 根据本发明的第三方面，提供了一种用于认证用户的方法，该方法包括在计算机系统中执行的以下步骤：

[0060] -从令牌接收签名的消息，该签名的消息取决于根据本发明的第二方面的令牌的计数器值，

[0061] -通过利用标识特征将用户分配给签名的消息，

[0062] -使用用户的公钥验证签名的消息的签名，以及

[0063] -将从消息中提取的计数器值与用户的先前认证过程中的计数器值进行比较，其中用户的连续认证过程的计数器值的至少一部分形成严格单调的序列。

[0064] 根据优选实施例，令牌作为人机接口设备连接到计算机系统。令牌可以将签名的消息作为在键盘扫描码中编码的模拟键盘输入来传输。优选地，接收的消息的前面有验证码，或者验证码被集成到签名的消息中。验证码包括适合于区分不同的语言配置的至少两个先前商定的ASCII字符的键盘扫描码。由于令牌和计算机系统之间存在关于要在验证码中提交的ASCII字符的协议，因此计算机系统能够确定哪种语言配置与接收的键盘扫描码相对应并将键盘扫描码分配给分别分配的ASCII字符。如果接收到的消息已经被令牌编码，则现在能够根据Base64解码。

[0065] 要验证签名，必须标识适当的公钥。为此目的，有必要将接收的消息分配给用户，以便从确定的用户确定关联的公钥。因此，用户和计算机系统不必共享诸如用户的私钥的秘密特征来认证用户。能够从签名的消息中的标识符确定用户。用户还能够由其他关联标识，例如，通过经由计算机系统上的键盘输入用户名(登录)，而密码输入由令牌启动。作为结果，并非绝对有必要在消息中集成标识特征。

[0066] 如果已经通过填充字节将要签名的消息扩展到最小长度并且在传输签名的消息之前已经移除了填充字节，则计算机系统在验证接收的消息的签名之前根据相应填充规则来补充未传输的填充字节。

[0067] 在一些实施例中，除了令牌的签名的消息之外，可以例如通过经由计算机系统的键盘或令牌输入密码来认证另一安全特征(双因素认证)。仅当输入的密码和令牌的签名的消息的验证是肯定的时，才允许访问计算机系统或计算机系统的应用。

[0068] 验证令牌涉及验证签名和验证消息中包含的计数器值的严格单调或消息中包含的计数器值。取决于安全性要求和使用用于用户认证的令牌的不同的计算机系统的同步

性,严格单调验证还可以包括验证验证的计数器值是表示最近验证的计数器值的增加而没有间隙。

[0069] 在其他实施例中,当前计数器值与最后验证的计数器值之间的间隙可以是允许的,特别是当在计算机系统不同步或者不足以经常同步最近认证的计数器值的多个计算机系统上使用用户认证令牌时。然而,在这种情况下,未经授权的人可以在第一计算机系统上篡改消息,以便将截获的消息导入尚未被通知第一计算机系统上的认证过程的第二计算机系统。为了防止令牌验证的不正确的肯定结果,能够在计算机系统之间进行验证的计数器值的同步。

[0070] 可选地或另外地,能够在消息中包括时间戳或类似属性,这确保了消息的短有效期。为此目的,能够使用消息中包含的时间戳,其允许仅在定义的时间段内使用接收的消息。

[0071] 如果签名的验证、(包括时间戳的)所有计数器值的验证都是肯定的,则用户的认证成功。这防止了截获的消息在其他非同步的计算机系统上成功播放(play)。

[0072] 根据本发明的认证过程能够在现有认证模块中以很少的调整工作来实施。

[0073] 例如,本发明的认证过程可以挂在LDAP认证模块的现有钩子(hook)上以根据本发明的第三方面来处理接收的密码数据。因此,根据本发明的认证过程能够在LDAP认证模块调用的动态库中实施。因此,从操作系统和应用程序的角度来看,仍然假设符合标准的LDAP认证。

[0074] 可以经由编程接口,例如经由Windows凭证管理API,将本发明的认证集成在Windows系列的操作系统中。根据本发明的认证的集成优选地经由开源软件pGina进行,该软件具有可扩展的插件架构并且使用Windows凭证管理API的编程接口。根据本发明的认证能够在LDAP服务器中实施,该LDAP服务器经由pGina连接到Windows凭证管理API。LDAP服务器优选地存储分配给用户的静态密码,该密码被传递到Windows凭证管理API以用于验证目的。可替代地,静态密码能够被存储在令牌中并被传输到计算机系统。Windows系列操作系统上需要静态密码,因为Windows使用用户的密码加密用户数据。

[0075] 在其上执行认证的计算机系统还可以包括与认证相关的其他电子设备。因此,计算机系统还可以包括用于访问控制和/或时间记录的终端以及电子门锁。

[0076] 计算机系统上的认证能够用于本地访问控制,例如在诸如Windows、Mac OS X、Linux和Unix的操作系统下。计算机系统上的认证能够用于目录登录,例如在Windows动态目录(Active Directory)、SMB和CIFS下。另外,对计算机系统的认证可以提供对应用程序、服务,web应用和VPN的访问控制。

[0077] 根据本发明的第四方面,提供了一种包括硬件实施的令牌的移动设备,该硬件实施的令牌包括根据本发明的第二方面的令牌。

[0078] 根据本发明的第五方面,提供了一种包括软件实施的令牌的移动设备,该软件实施的令牌具有指令,该指令当在移动设备的处理器上运行时,实施本发明的第一方面的方法的步骤。

[0079] 根据本发明的第六方面,提供了一种包括指令的计算机程序产品,该指令当在处理器上运行时,实施本发明的第一方面或第三方面的方法的步骤。

[0080] 本发明可以包括设置和维护程序,其将现有私钥和可选的关联公钥传送到令牌。

优选地，设置和维护程序具有用于生成由私钥和相应公钥组成的密钥对的功能、或者引起(prompt)用于生成密钥对的令牌的功能。设置和维护程序可以用于设置和/或读取令牌的实时时钟的时间，例如设置第一次的时间或设置电源故障后的时间，这导致了停顿或重置令牌的实时时钟。设置和维护程序可以具有用于设置和/或读取用户定义的前缀的功能。设置和维护程序可以包括用于设置和/或读取计数器值的功能。

附图说明

[0081] 通过以下结合附图的详细描述，本发明的其他特征、目的和优点将变得显而易见，其中：

[0082] 图1示出了根据本发明的实施例的令牌的示意图，

[0083] 图2示出了根据本发明的实施例的由令牌签名的消息的示意图，

[0084] 图3示出了根据本发明的实施例的用于向计算机系统认证用户的方法，

[0085] 图4示出了根据本发明的实施例的用于向计算机系统认证用户的方法，

[0086] 图5示出了根据本发明的实施例的具有硬件令牌的移动设备的示意图，和

[0087] 图6示出了根据本发明的实施例的具有软件令牌的移动设备的示意图。

具体实施方式

[0088] 本发明用于在计算机系统中认证用户。本发明优选地用于将用户登录到操作系统。本发明还能够被用于应用程序或Web应用中的认证，例如社交网络中的认证。本发明适合于验证分配给令牌的用户的身份。令牌可以集成到专用硬件(“硬件令牌”)中，既可以作为独立的电子设备，又可以作为更全面的电子设备的一部分。令牌还适用于以软件实施(“软件令牌”)，以在诸如计算机、平板计算机、智能电话、上网本、笔记本或膝上型计算机的移动便携式计算机访问计算机系统、特定应用程序或使用移动设备的数据时使用。软件令牌还能够用于安装有软件令牌的移动设备上的认证。作为硬件令牌的优选用途仅被视为可能的应用领域。

[0089] 在以下实施例中，本发明被实施为允许用户登录到计算机系统的操作系统的隔离硬件令牌。然而，实施例不限于此；以类似的方式，本发明的每个实施例及其公开的特征适用于应用的所有领域。

[0090] 在大多数情况下，单独地实施例仅突出了本发明的单独的特征。该说明是为了清楚和更好地理解本发明。独立于本发明的其他特征的本发明的那些特征可以根据需要任意组合。

[0091] 图1示出了令牌10的示意性结构，其包括计数单元12、存储器14、处理单元16和传输单元18。计数单元12用于生成一个或多个计数器值20、22。例如，数值计数器值20和/或时间戳22可以用作计数器值20、22。存储器14存储与令牌10的用户相关联的私钥24。私钥24不需要被计算机系统可访问以认证用户。存储器14还可以包括与私钥24相关联的公钥26。只有公钥26或其副本必须被计算机系统可访问以进行认证。处理单元16被配置成通过使计数单元12生成至少一个计数器值20、22来以生成消息30。至少一个生成的计数器值20、22用作使用至少一个生成的计数器值20、22生成消息30的基础。生成的计数器值20、22的特征在于，相对于先前生成的计数器值20、22计数器值20、22每次生成的新计数器值20、22能够被

标识为随后生成的计数器值。该条件必须至少适用于系列内具有最小数量的计数器值的系列的计数器值。对数值没有任何限制;任何内容可以作为计数器值20、22而提供,只要生成的内容与先前生成的内容相比较能够在足够大的定义的内容系列内被标识为随后生成的内容。在一些实施例中,术语"随后"可以被理解为紧随其后,而在其他实施例中,一定数量的计数器值20、22可以在当前生成的和先前的计数器值20、22之间。处理单元30还被配置成使用私钥24签名生成的消息30。在传输单元18将签名的和可选编码的消息传输到计算机系统70之前,可以根据传输路径和接收计算机系统的要求适当地编码签名的消息。计算机系统70接收签名的和可选编码的消息,以基于签名的消息认证用户。

[0092] 图2示出了根据本发明的实施例的要签名的消息30的结构。消息30可以优选地包括属于一个或多个字符编码的32个字符,例如,每个字符一个字节的ASCII。消息30根据一个或多个属性而生成,这些属性例如彼此相邻地布置并且可选地由分隔符彼此分离。示例消息30由以下六个属性组成:

[0093] 第一属性32表示消息30的协议版本,使得接收计算机系统70能够将消息30的结构与其他协议版本的消息30区分开。协议版本32能够例如以3个字节编码。

[0094] 第二属性34表示在生成消息时信号通知问题实例的标识,该问题实例诸如令牌中的电源故障,使得用于生成时间戳的令牌中的实时时钟已经停止或已经被重置为起始值。标志34可以例如以1字节编码。

[0095] 第三属性36表示令牌10的标识特征,使得令牌能够被分配给用户。令牌10的标识特征36能够例如以6个字节编码。

[0096] 第四属性38表示用户定义的前缀,例如,由公司的部门对令牌进行分组或者将多个令牌与用户相关联。例如,用户定义的前缀38可以以4个字节编码。

[0097] 第五属性40表示第一编码的计数器值。第一编码的计数器值40与由计数器12生成的计数器值20、22相对应,或者基于生成的计数器值20、22计算。第一编码的计数器值40可以是数字计数器值20,例如,以4字节编码。

[0098] 第六属性42表示第二编码的计数器值。第二编码的计数器值42与由计数器12生成的计数器值20、22相对应,或者基于生成的计数器值20、22计算。例如,第二编码的计数器值42可以是时间戳22并以5个字节编码。

[0099] 还可以基于六个属性中的一个或多个,例如,通过以任何顺序并置(juxtapose)六个属性中的一个或多个,来生成消息30。

[0100] 在优选实施例中,消息30中包括其他组件以确保要签名的消息的最小长度,诸如字符串"bitagent*"(不带引号)的ASCII代表,属性被插入先前生成的消息30的任何两个相邻字符之间。现在能够对生成的消息30进行签名。在已经生成签名之后,能够再次从消息中移除插入的附加组件,使得它们被包含在仅用于生成和稍后验证签名的消息中,而不在消息的传输期间包含。

[0101] 图3示出了用于向计算机系统70认证用户的方法50。该方法步骤在令牌10中执行。

[0102] 在第一方法步骤52中,在令牌10中实施的计数单元12生成至少一个计数器值20、22。生成的计数器值20、22的特征在于,相对于一个先前生成的计数器值20、22至少一个计数器值20、22每次生成的新计数器值20、22能够被标识为随后生成的计数器值。在这方面,生成的计数器值20、22的至少一部分形成严格单调的序列。

[0103] 在第二方法步骤54中，根据至少一个生成的计数器值20、22生成消息30。为此目的，能够将至少一个计数器值20、22变换为关联的编码的计数器值40、42。可以向消息30添加更多属性和固定组件。

[0104] 在第三方法步骤56中，使用分配给令牌10的用户的私钥24对生成的消息30进行签名。私钥24可以存储在令牌10中。可以取决于接收消息的计算机系统70和选择的传输路径来对签名的消息进行编码。

[0105] 在第四方法步骤58中，将签名的和可选编码的消息发送到计算机系统70以用于用户的认证。

[0106] 图4示出了用于向计算机系统70认证用户的方法60。

[0107] 在第一方法步骤62中，计算机系统70从用户的令牌10接收签名的和可选编码的消息。

[0108] 在第二方法步骤64中，计算机系统70确定能够向哪个用户分配签名的消息。为此目的，验证合适的标识特征36。标识特征36优选地被编码为接收的消息中的属性。标识特征36也能够经由其他输入通道提供，例如通过经由键盘的手动数据输入或者通过用户的选择。可以通过使用映射表从标识特征36中导出用户。

[0109] 在第三方法步骤66中，计算机系统70确定与标识的标识特征36相关联的用户的公钥26。在接收的消息已经使用与用户相关联的私钥24签名之后，计算机系统70能够使用确定的公钥26验证接收的消息的真实性。

[0110] 为了保护认证过程免于重复导入截获的签名的消息，在第四方法步骤68中验证包含在消息的至少一个计数器值20、22的严格单调。为此目的，从消息中提取包含在接收的消息的至少一个计数器值20、22，并与用户的在先认证过程60的分别分配的先前的计数器值20、22进行比较。在这种情况下，与先前的认证过程60相比较，一个或多个新接收的计数器值必须各自被标识为后续值。在一些示例性实施例中，验证接收的计数器值中的一个或多个计数器值随后紧随其后或者分别新接收的计数器值与关联的先前接收的计数器值之间的距离低于极限值。可替代地或另外地，还能够例如在消息中包含的时间戳22的基础上验证消息的有效期。

[0111] 令牌能够被设计为表示电子设备的硬件令牌。图5示出了移动设备80A，其中根据本发明的令牌被集成为硬件令牌10A。移动设备80A可以是为令牌的功能而专门设计的，并配备有用于与计算机系统通信的接口。移动设备还可以是移动计算机，例如平板计算机、上网本、笔记本或智能电话，可选地具有到第二或多个设备的接口。硬件令牌10A的定义并不排除它包括处理器，在该处理器上运行用于实现令牌的功能的指令，并且到目前为止硬件令牌的功能也由软件实现。作为硬件令牌的分类的决定性因素是软件在硬件令牌的封闭系统内运行。

[0112] 令牌还可以被实施为用于在电子设备的处理器上运行的软件令牌。图6示出了移动设备80B，其中根据本发明的令牌被集成为软件令牌10B。软件令牌10B可以在移动设备80B的操作系统中或者中间件中被集成为应用程序(“App”)。软件令牌包括在移动设备80B的至少一个处理器82上运行的指令。

[0113] 通过将用于运行令牌软件的资源与移动设备80B的剩余应用和服务共享来给出软件令牌10B到硬件令牌10A的软件的描绘，同时硬件令牌10A的软件专门在硬件令牌10A的与

移动设备80A的剩余资源隔离的资源上运行。

[0114] 附带地，本发明包括在示例性实施例中提到的用于硬件或软件令牌的实现所需的所有组件。在前面的示例性实施例中描述的令牌的各个组件之间的任务分配应被理解为示例。在令牌的组件之间还存在可想到的其他划分，其以等同的形式实现本发明的描述的特征。

[0115] 包含在实施例的以上描述中的细节不应被解释为限制本发明的范围，而是表示其一些实施例的示例。许多变体是可能的并且对技术人员而言是显而易见的。特别地，这涉及包括本说明书中公开的各个实施例的特征的组合的变型。因此，本发明的范围不应由所示实施例确定，而应由所附权利要求及其合法等同物确定。

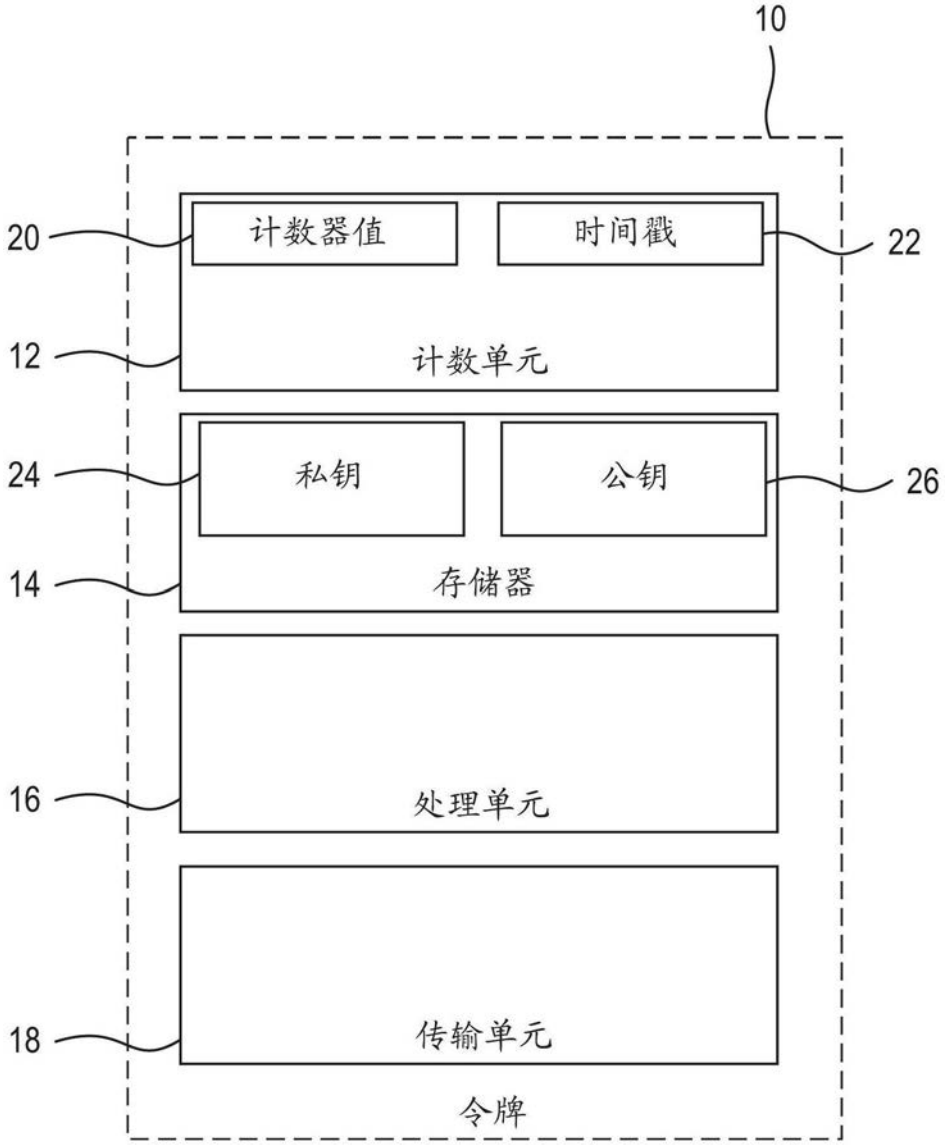

10
20
计数器值
时间戳
22
12
计数单元
24
私钥
公钥
26
14
存储器
16
处理单元
18
传输单元
令牌

图1

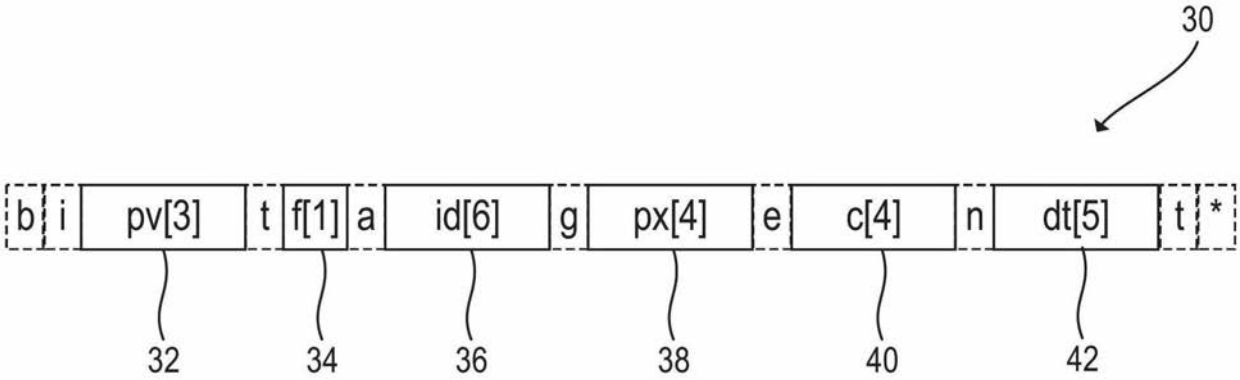

30
b
i
pv[3]
t
f[1]
a
id[6]
g
px[4]
e
c[4]
n
dt[5]
t
*
32
34
36
38
40
42

图2

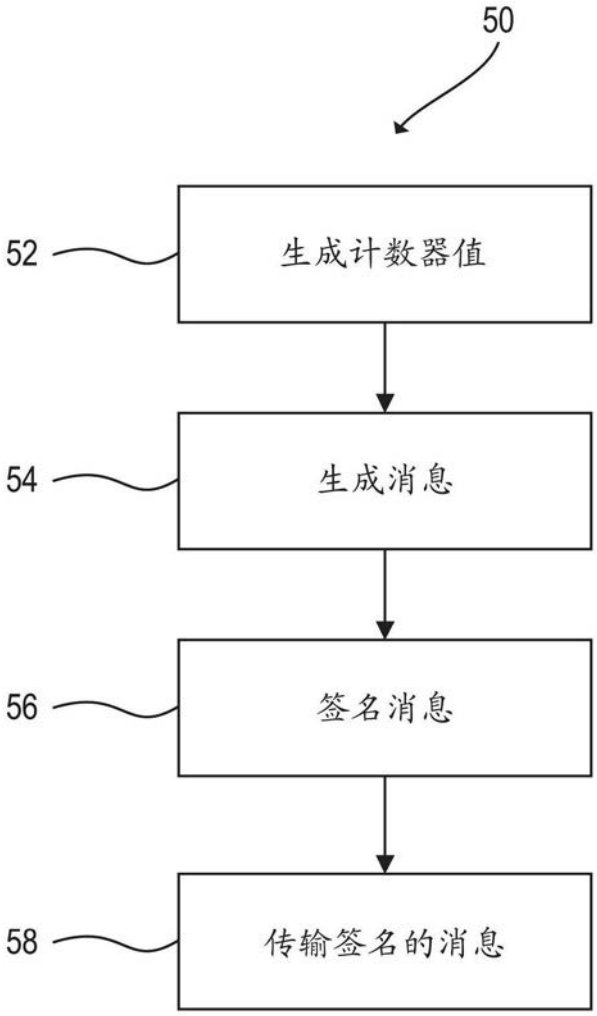


图3

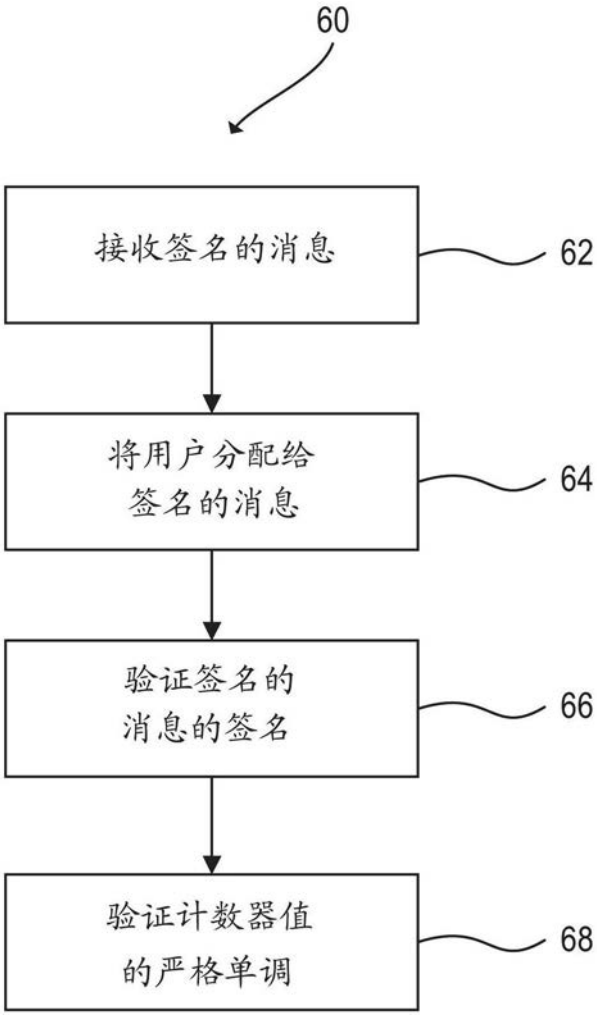

60
接收签名的消息
62
将用户分配给
签名的消息
64
验证签名的
消息的签名
66
验证计数器值
的严格单调
68

图4

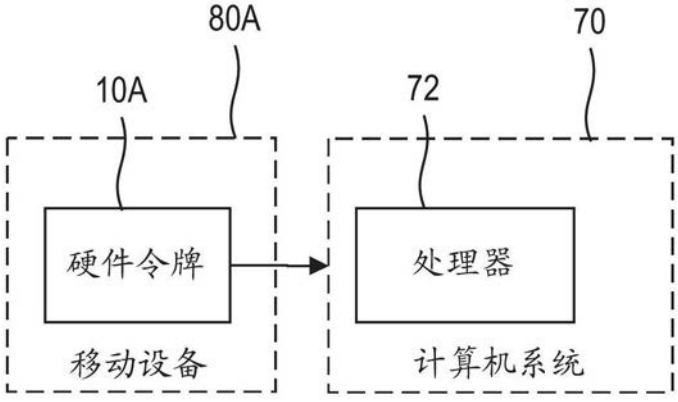

80A
70
10A
72
硬件令牌
处理器
移动设备
计算机系统

图5

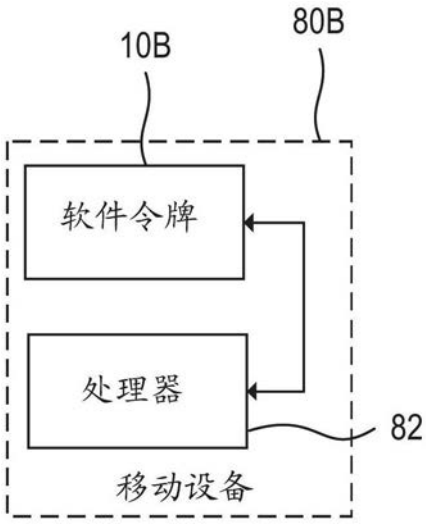


图6