(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 106063182 B
(45)授权公告日 2019.11.19

(21)申请号 201480074422.1

(22)申请日 2014.12.18

(65)同一申请的已公布的文献号
申请公布号 CN 106063182 A

(43)申请公布日 2016.10.26

(30)优先权数据
61/922,128 2013.12.31 US

(85)PCT国际申请进入国家阶段日
2016.07.28

(86)PCT国际申请的申请数据
PCT/US2014/071068 2014.12.18

(87)PCT国际申请的公布数据
WO2015/102918 EN 2015.07.09

(73)专利权人 威斯科数据安全国际有限公司
地址 瑞士格拉特布吕格

(72)发明人 迪尔克·马里恩

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 唐京桥 陈炜

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
US 2008263363 A1,2008.10.23,

审查员 王怡轩

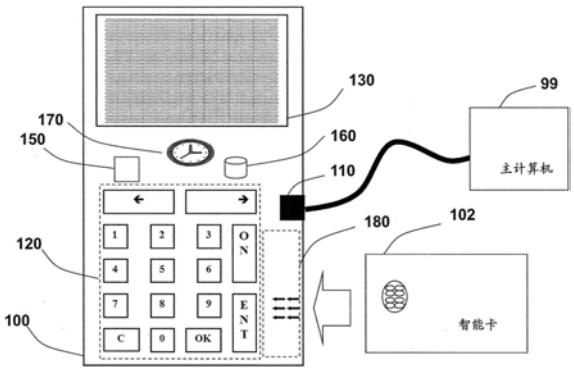
权利要求书4页 说明书15页 附图3页

(54)发明名称

电子签名方法、系统及设备

(57)摘要

公开了用于生成数字签名的方法、设备和系统。设备可以将其本身作为大容量存储装置提供至主计算机，以通过用于交换文件的标准大容量存储装置访问机构来提供加密处理结果。



CN 106063182 B

1.一种用于生成数字签名的设备,包括:

通信接口,用于在本地将所述设备连接至主计算机;以及

数据处理部件,其适于提供通过将加密密钥与第一输入数据进行加密组合而生成的加密处理结果;

其中,

当所述设备通过所述通信接口连接至所述主计算机时,所述设备适于将其本身作为大容量存储装置提供至所述主计算机,所述主计算机上的应用可以通过用于交换文件的标准大容量存储访问机构来访问所述大容量存储装置;

所述通信接口还适于从所述主计算机接收输入文件,其中,所述主计算机通过以下来经由所述通信接口将所述输入文件发送给所述设备:通过所述标准大容量存储访问机构的用于保存文件的机构,将所述输入文件保存至由所述设备提供的大容量存储装置;

所述设备还适于在所述输入文件的至少一些内容上生成数字签名,其中,所述数字签名被包括在将所述加密密钥与所述第一输入数据进行加密组合的结果中,并且所述第一输入数据基于表示所述输入文件的至少一些内容的值;以及

所述通信接口还适于经由所述通信接口将输出文件返回至所述主计算机,其中,所述输出文件包括所述加密处理结果,并且所述主计算机通过以下来获得所述输出文件:通过所述标准大容量存储访问机构的用于读取文件的机构,经由所述通信接口从所述设备读取所述输出文件。

2.根据权利要求1所述的设备,其中,所述通信接口包括通用串行总线(USB)接口,并且其中,当所述设备连接至所述主计算机时,所述设备还适于将其本身作为USB大容量存储装置类的USB装置提供至所述主计算机。

3.根据权利要求1或2所述的设备,还包括:

存储器部件,其适于存储所述加密密钥;

其中,所述数据处理部件适于利用所述加密密钥来执行加密计算;

其中,将所述加密密钥与所述第一输入数据进行加密组合包括:所述数据处理部件执行所述加密计算。

4.根据权利要求1所述的设备,还包括:

第二通信接口,用于与外部可移除密钥存储装置进行命令和响应的接收和交换,所述密钥存储装置包括密钥存储装置存储器部件和密钥存储装置数据处理部件,所述密钥存储装置存储器部件适于存储所述加密密钥,所述密钥存储装置数据处理部件适于利用所述加密密钥来执行加密计算;

其中,将所述加密密钥与所述第一输入数据进行加密组合包括:所述密钥存储装置数据处理部件利用所述加密密钥来执行所述加密计算。

5.根据权利要求4所述的设备,其中,所述第二通信接口包括国际标准化组织(ISO)7816可兼容智能卡接口,并且所述命令和响应包括智能卡命令和响应,并且其中,所述密钥存储装置包括智能卡。

6.根据权利要求1所述的设备,进一步包括:用户输入接口,用于所述设备的用户指示许可,其中,所述设备适于通过所述用户输入接口来获取所述用户的许可,并且其中,以下中的至少一个是以在所述设备上获得所述许可为条件的:将所述加密密钥与所述第一输入

数据进行加密组合;或者返回包括所述加密组合的结果的至少一个输出文件。

7.根据权利要求1所述的设备,其中,所述加密密钥包括与应用共享的对称密钥,并且其中,将所述加密密钥与所述第一输入数据进行加密组合包括:对所述第一输入数据执行利用所述对称密钥而参数化的对称加密算法。

8.根据权利要求1所述的设备,其中,所述加密密钥包括非对称公钥私钥对的私有密钥,并且其中,将所述加密密钥与所述第一输入数据进行加密组合包括:对所述第一输入数据执行利用所述私有密钥而参数化的非对称加密算法。

9.根据权利要求8所述的设备,还适于向所述主计算机提供公钥文件,所述公钥文件包括所述公钥私钥对的公钥,并且其中,所述主计算机通过以下来获得所述公钥文件:通过所述用于读取文件的机构,经由所述通信接口从所述设备读取所述公钥文件。

10.根据权利要求8或9所述的设备,还适于向所述主计算机提供证书文件,所述证书文件包括与所述公钥私钥对相关联的一个或更多个证书,并且其中,所述主计算机通过以下来获得所述证书文件:通过所述用于读取文件的机构,经由所述通信接口从所述设备读取所述证书文件。

11.根据权利要求10所述的设备,其中,所述输入文件的至少一些内容包括整个输入文件。

12.根据权利要求10所述的设备,还包括用于向所述设备的用户提供输出的用户输出接口以及用于从所述用户获取输入的用户输入接口;所述设备还适于:

识别所述输入文件的多个可能文件类型格式中的至少一个的格式;

读取所述输入文件的至少一些内容;

通过所述用户输出接口向所述用户提供至少一些内容;以及

通过所述用户输入接口从所述用户获取由所述用户对提供至所述用户的至少一些内容作出的许可或拒绝中的至少一个;

其中,将所述加密密钥与所述第一输入数据进行加密组合或者返回包括所述加密组合的结果的至少一个输出文件是以在所述设备上获得所述许可为条件的。

13.根据权利要求1所述的设备,还包括用户输入接口,用于所述设备的用户向所述设备提供PIN值或口令值中的至少一个;所述设备还适于通过所述用户输入接口从所述用户获得所述PIN值或所述口令值中的所述至少一个,并且验证所述PIN值或所述口令值中的所述至少一个是否正确;其中,将所述加密密钥与所述第一输入数据进行加密组合或者返回包括所述加密组合的结果的至少一个输出文件是以由用户提供的所述PIN值或所述口令值中的至少一个是正确的为条件的。

14.根据权利要求13所述的设备,还适于存储参考值,其中,对所获得的PIN值或所获得的口令值中的至少一个的验证包括:所述设备将所获得的PIN值或所获得的口令值中的至少一个与所述参考值进行比较。

15.根据权利要求13或14所述的设备,还包括第二通信接口,所述第二通信接口用于与外部可移除装置进行命令和响应的接收和交换,其中,对所获得的PIN值或所获得的口令值中的至少一个的验证包括:

所述设备经由所述第二通信接口向所述外部可移除装置传送PIN代表值或口令代表值中的至少一个,所述PIN代表值或口令代表值表示用于所述外部可移除装置进行验证的所

获得的PIN值或所获得的口令值中的至少一个;以及

所述设备经由所述第二通信接口从所述外部可移除装置接收由所述外部可移除装置对所述代表值进行验证的结果。

16.根据权利要求1所述的设备,还包括生物特征传感器,所述生物特征传感器用于获取所述设备的用户的生物特征测量;所述设备还适于通过所述生物特征传感器从所述用户获得所述生物特征测量,并且验证所述生物特征测量是否正确;其中,以下中的至少一个是以所获得的生物特征测量是正确的为条件的:将所述加密密钥与所述第一输入数据进行加密组合;或者返回包括所述加密组合的结果的至少一个输出文件。

17.根据权利要求16所述的设备,还适于存储生物特征参考数据,其中,对所获得的生物特征测量的验证包括:所述设备将所获得的生物特征测量与所述生物特征参考数据进行比较。

18.根据权利要求16或17所述的设备,还包括第二通信接口,所述第二通信接口用于与外部可移除装置进行命令和响应的接收和交换,其中,对所获得的生物特征测量的验证包括:

所述设备经由所述第二通信接口向所述外部可移除设备传送所述生物特征测量,以用于所述外部可移除设备进行验证;以及

所述设备经由所述第二通信接口从所述外部可移除装置接收由所述外部可移除装置对所述生物特征测量进行验证的结果。

19.一种供设备使用的用于在电子输入文件上生成数字签名的方法,所述设备包括用于在本地将所述设备连接至主计算机的通信接口,

其中,所述设备适于:

当所述设备连接至所述主计算机时,将所述设备本身作为大容量存储装置提供至所述主计算机,所述主计算机上的应用可以通过用于读取和保存文件的标准大容量存储访问机构来访问所述大容量存储装置;

经由所述通信接口从所述主计算机接收所述输入文件;

通过向所述输入文件应用数字签名算法来在所述输入文件上生成所述数字签名,所述数字签名算法通过签名密钥被参数化;

经由所述通信接口将输出文件返回至所述主计算机,其中,所述输出文件包括所述输入文件上的所述数字签名;

所述方法包括以下步骤:

在所述主计算机处生成与所述设备的连接;

通过以下来在所述主计算机处经由所述通信接口将所述输入文件发送至所述设备:通过使用所述标准大容量存储访问机构的用于保存文件的方法,将所述输入文件保存至由所述设备提供的大容量存储装置;

通过以下来在所述主计算机处经由所述通信接口从所述设备获得输出文件:通过使用所述标准大容量存储访问机构的用于读取文件的方法读取所述输出文件;

从所述输出文件检索所述数字签名。

20.根据权利要求19所述的方法,其中,所述通信接口包括通用串行总线(USB)接口,并且其中,当所述设备连接至所述主计算机时,所述设备还适于将其本身作为所述USB大容量

存储装置类的USB装置提供至所述主计算机。

21.一种用于在电子输入文件上生成数字签名的系统,包括:

主计算机,所述主计算机包括:

数据处理部件,用于运行软件应用,

连接机构,用于将至少一个外围装置可移除地连接至所述主计算机,

所述主计算机适于:

支持大容量存储装置中的一个种类;

如果当通过所述连接机构要与所述主计算机连接的设备被连接至所述主计算机时所述设备通告其本身属于所述种类的大容量存储装置,则将所述设备识别为属于所述种类;

支持标准大容量存储装置访问机构以将文件读取和保存至大容量存储装置,所述大容量存储装置通过所述连接机构被连接至所述主计算机,并且被所述主计算机识别为属于所述种类的大容量存储装置;

向所述软件应用提供所述标准大容量存储访问机构的用于将文件读取至所述大容量存储装置的第一方法以及所述标准大容量存储访问机构的用于将文件保存至所述大容量存储装置的第二方法;

所述系统还包括:

签名设备,其包括通信接口,所述通信接口用于通过所述连接机构将所述签名设备在本地连接至所述主计算机,其中,所述签名设备适于:

当所述签名设备被连接至所述主计算机时,将所述签名设备本身作为属于所述种类的大容量存储装置提供至所述主计算机;

经由所述通信接口从所述主计算机接收所述输入文件;

通过向所述输入文件应用数字签名算法来在所述输入文件上生成所述数字签名,所述数字签名算法通过签名密钥被参数化;

经由所述通信接口将输出文件返回至所述主计算机,其中,所述输出文件包括所述输入文件上的数字签名;以及

其中:

所述签名设备通过所述通信接口和所述连接机构被连接至所述主计算机;以及

所述主计算机运行签名应用,所述签名应用适于:

通过以下来经由所述通信接口将所述输入文件发送至所述签名设备:通过使用所述标准大容量存储访问机构的用于保存文件的所述第二方法将所述输入文件保存至所述设备;

通过以下来在所述主计算机处经由所述通信接口从所述签名设备获得所述输出文件:通过使用所述标准大容量存储访问机构的所述第一方法读取所述输出文件。

22.根据权利要求21所述的系统,其中,所述通信接口包括通用串行总线(USB)接口,并且其中,当所述设备连接至所述主计算机时,所述设备还适于将其本身作为USB大容量存储装置类的USB装置提供至所述主计算机。

电子签名方法、系统及设备

[0001] 相关申请的交叉引用

[0002] 本申请要求于2013年12月31日提交的序列号为61/922,128的题为“Electronic Signing Methods,Systems,and Apparatus”的美国临时申请的优先权,该申请的全部公开内容通过引用并入本文中。

技术领域

[0003] 本发明涉及对计算机和应用的远程访问以及通过计算机网络的远程交易进行保护。更具体地,本发明涉及用于生成电子签名的方法和设备。

背景技术

[0004] 随着对计算机系统和应用的远程访问日渐普及,通过公共网络如因特网远程访问的交易的数目和种类显著增加。这种普及强调了对安全性的需要;具体地:如何确保正在远程访问应用的人是他们所声称的人,如何确保正在远程进行的交易是由合法的个体发起的,如何确保在应用服务器处接收交易数据之前该交易处理数据不被更改,以及如何保证个体一旦从事交易则不能否认。

[0005] 过去,应用提供者曾依赖静态口令来提供针对远程应用的安全性。近年来,显而易见,静态口令是不够的,并且需要更先进的安全性技术。

[0006] 一种解决方案是数字签名数据,例如使用非对称数字签名算法的电子文件(例如电子文档),该非对称数字签名算法利用公钥私钥对中的私钥来进行参数化。这可以例如使用公钥构架(PKI)而发生。在公钥构架中,将公钥私钥对与每个用户相关联。该密钥对与(由受信任的认证机构颁发的)证书相关联,该证书将所述公钥私钥对绑定到特定用户。通过使用非对称加密,该公钥私钥对可以用于:验证用户;对交易、文件、电子邮件进行签名(以便防止否认);建立加密的通信渠道;以及对已经由发送者使用收件人的公钥而加密的消息或文件进行解密。

[0007] 在许多情况下,用户使用通用计算装置(例如个人计算机)与应用进行交互。在与应用进行交互的某些时候,可能会要求用户利用与该用户相关联的私钥对电子文件进行电子签名。

[0008] 为了安全起见,用户的私钥通常存储在适于安全地存储用户的私钥的独立密钥存储装置上。在大多数情况下,密钥存储装置还适于使用所存储的私钥根据非对称加密算法来进行加密计算。这样的密钥存储装置的示例包括PKI智能卡和PKI USB(通用串行总线)令牌。通常,用户的通用计算机使用智能卡阅读器与智能卡进行交互。在大多数情况下,这些智能卡阅读器必须通过USB接口连接至通用计算机。PKI USB令牌经常将USB智能卡阅读器和PKI智能卡的功能结合在单个加密狗类装置中。

[0009] 在大多数情况下,应用通过标准加密API(应用编程接口)例如MS-CAPI(微软加密API)或PKCS#11(公钥加密标准11)与向应用提供高级别加密服务(例如对电子文件进行签名或解密)的加密库对接,并且加密库将高级别应用请求转化为呈一系列命令-响应,所述

应用将一系列命令-响应与持有用户相关联的私钥的用户的智能卡进行交换。

[0010] 然而，该解决方案存在许多问题。为了使解决方案起作用，用户所使用的PC必须具有这样的加密库，但很多PC(个人计算机)在默认情况下不具有这种的加密库，这意味着用户必须安装加密库。此外，在实践中，智能卡与加密库之间的接口未被标准化，这意味着用户必须安装与用户的特定智能卡兼容的特定加密库。此外，虽然大多数PC都支持USB，但他们在默认情况下往往不支持USB智能卡阅读器，所以用户还必须安装与用户所用的智能卡阅读器兼容的用于智能卡阅读器的USB驱动器。安装要求的这种组合在实际中往往对于许多用户来说首先开始太复杂，或者引起安装失败，从而使得系统不可靠或者甚至不能正常工作。

[0011] 所需要的是一种以下解决方案：利用用户的私钥对电子文件进行签名而不要求用户在用户的通用计算设备上安装特定的硬件和软件。

发明内容

[0012] 本发明基于本发明人的见解，即尽管许多计算机在默认情况下不支持USB智能卡阅读器，但他们几乎无一例外地支持USB大容量存储装置。

[0013] 本发明的一个方面提供了一种设备，该设备包括通信接口和数据处理部件，该通信接口用于在本地将所述设备连接至主计算机，该数据处理部件适于提供由通过将加密密钥(cryptographic secret key)与第一输入数据进行加密组合而生成的加密处理结果；其中，所述设备可以适于：当所述设备通过通信接口被连接至主计算机时，将其本身作为大容量存储装置提供至主计算机，主计算机上的应用可以通过用于交换文件的标准大容量存储访问机构访问大容量存储装置；以及通信接口可以适于：经由通信接口将输出文件返回至主计算机，其中所述输出文件可以包括加密处理结果，并且所述主计算机可以通过以下来获得所述输出文件：通过标准大容量存储访问机构的用于读取文件的机构，经由通信接口从所述设备读取所述输出文件。

[0014] 在一些实施方式中，所述通信接口可以包括USB接口，并且当所述设备被连接至主计算机计算机时，所述设备还可以适于将其本身作为USB大容量存储装置类的USB装置提供至主计算机。

[0015] 在一些实施方式中，所述设备可以是前述实施方式中的任一实施方式所述的设备，所述设备还包括存储器部件和数据处理部件，该存储器部件适于存储所述加密密钥，该数据处理部件适于利用所述加密密钥执行加密计算；其中，对所述加密密钥与所述第一输入数据进行所述加密组合可以包括：所述数据处理部件执行所述加密计算。

[0016] 在一些实施方式中，所述设备可以是前述实施方式中的任一实施方式所述的设备，所述设备还包括：第二通信接口，用于与外部可移除密钥存储装置进行命令和响应的接收和交换，所述密钥存储装置包括密钥存储装置存储器部件和密钥存储装置数据处理部件，该密钥存储装置存储器部件适于存储所述加密密钥，该密钥存储装置数据处理部件适于利用所述加密密钥来执行加密计算；其中，对所述加密密钥与所述第一输入数据进行所述加密组合可以包括：所述密钥存储装置数据处理部件利用所述加密密钥来执行所述加密计算。

[0017] 在一些实施方式中，所述第二通信接口可以包括智能卡接口，其可以是与ISO/IEC

(国际标准化组织/国际电工委员会)7816组的标准(特别是ISO/IEC 7816-2和ISO/IEC 7816-3)兼容,并且所述命令和响应可以包括智能卡命令和响应,例如智能卡APDU(应用协议数据单元),并且所述密钥存储装置可以是能够执行非对称加密的智能卡例如PKI(公钥构架)智能卡。在一些实施方式中,第二通信接口可以包括可从外部访问的智能卡插槽,以用于接收ISO/IEC 7810ID-1格式的智能卡,并且密钥存储装置可以是ISO/IEC 7810ID-1格式的ISO/IEC 7816可兼容智能卡。在一些实施方式中,智能卡可以与ISO/IEC 7816-15标准相兼容。

[0018] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设备,所述设备还包括:用户输入接口,用于所述设备的用户指示许可,其中,所述设备可以适于通过用户输入接口获取用户的许可,并且其中,以下中的至少一个可以为在所述设备上获得许可的条件:将密钥与第一数据进行加密组合;或者返回包括加密组合结果的至少一个输出文件。

[0019] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设备,其中,所述加密密钥可以包括与应用共享的对称密钥,并且其中,加密密钥与第一输入数据的加密组合可以包括:对第一输入数据执行对称加密算法,其中对称加密算法利用对称密钥被参数化。在一些实施方式中,对称加密算法可以包括对称加密或者解密算法,例如AES(高级加密标准)。在一些实施方式中,对称加密算法可以包括加密散列算法,例如HMAC(Hash-based Message Authentication Code,基于散列的消息认证码)。

[0020] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设备,其中,所述加密密钥包括非对称公钥私钥对的私有密钥(secret private key),并且其中,加密密钥与第一输入数据的加密组合包括:对第一输入数据执行非对称加密算法,例如RSA(Rivest-Shamir-Adleman),该非对称加密算法利用私有密钥被参数化。

[0021] 在一些实施方式中,所述设备还可以适于使得公钥文件可用于主计算机,该公钥文件包括公钥私钥对的公钥,并且其中,该主计算机通过用于读取文件的机构经由通信接口从设备读取公钥文件来获得公钥文件。在一些实施方式中,公钥文件可以与输出文件是相同的。在其他实施方式中,公钥文件可以是除了输出文件之外的另外的文件。在一些实施方式中,公钥文件包括采用标准化格式例如根据PKCS#1的公钥。

[0022] 在一些实施方式中,所述设备还可以适于使得证书文件可用于主计算机,该证书文件包括与公钥私钥对相关联的一个或更多个证书,并且其中,该主计算机通过以下来获得证书文件:通过用于读取文件的机构,经由通信接口从设备读取证书文件。可以由认证机构生成证书。在一些实施方式中,证书文件可以包括证书链。在一些实施方式中,所述设备可以具有一个以上的证书文件以及一个以上的证书。在一些实施方式中,证书文件可以与输出文件或公钥文件是相同的。在其他实施方式中,证书文件可以是与输出文件和公钥文件不同的另外的文件。在一些实施方式中,证书文件可以包括例如在X.509标准中所描述的标准化格式的证书。

[0023] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设备,该设备还适于生成一次性口令,其中,所述一次性口令被包括在加密密钥与第一输入数据的加密组合的结果中,并且其中,所述第一输入数据包括动态变量。

[0024] 在一些实施方式中,所述设备还可以包括时钟,并且所述动态变量可以基于由所

述时钟提供的时间值。

[0025] 在一些实施方式中,所述设备还可以适于:存储第二变量;根据所存储的第二变量来确定动态变量的值;并且当第二变量的值已用于所述组合时,更新并存储第二变量的值。在一些实施方式中,所述设备还可以包括存储部件,并且还可以适于:将第二变量存储在存储部件中;根据所存储的第二变量来确定动态变量的值;当第二变量的值已用于所述组合例如用于生成一次性口令时,更新第二变量的值并且将第二变量的值存储在存储部件中。在一些实施方式中,所述第二变量可以包括计数器,并且更新所述第二变量可以包括:使所述计数器的值单调增加(或递增)或单调递减(或递减)。例如,在一些实施方式中,动态变量可以是计数器,所述设备可以将该计数器存储在其存储器中,并且每当所述设备生成一次性口令时,该计数器可以递增(或递减)一。

[0026] 在一些实施方式中,所述设备可以适于:在所述设备已收到来自主计算机的要读取包括一次性口令的输出文件的请求之后,生成一次性口令(OTP),并且可以在生成一次性口令之后生成包括所生成的一次性口令的输出文件,并将所生成的输出文件返回至主计算机。在其他实施方式中,所述设备可以适于:将一次性口令的当前值存储在永久性存储器中,并且当接收到第二变量即从主计算机接收到要读取包括一次性口令的输出文件的请求时,所述设备可以生成包括所存储的一次性口令的输出文件,并且将具有所存储的一次性口令的该输出文件返回至主计算机,并且随后可以(在返回所述输出文件之后)生成一次性口令的新值,并且在从主计算机接收到要读取输出文件的请求之前将一次性口令的存储值更新为新生成的值。换句话说,在一些实施方式中,所述设备可以在接收要读取包括所述一次性口令的输出文件的请求与返回包括该一次性口令的输出文件之间生成所述一次性口令,而在其他实施方式中,所述设备可以在返回包括一次性口令的先前值的输出文件之后以及在接收到要读取包括新生成的一次性口令的输出文件的请求之前生成新的一次性口令值。

[0027] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设备,所述设备还适于:在输入文件的至少一些内容上生成数字签名,其中所述通信接口还可以适于从主计算机接收所述输入文件,其中所述主计算机可以通过以下来经由通信接口将输入文件发送至所述设备:通过标准大容量存储访问机构的用于保存文件的机构将输入文件保存至由所述设备所提供的大容量存储装置,所述第一输入数据可以基于表示输入文件的至少一些内容的值;以及所述数字签名可以被包括在加密密钥与第一输入数据的加密组合的结果中。在一些实施方式中,所述输入文件的所述至少一些内容包括整个输入文件。即,在一些实施方式中,所述设备可以适于在整个输入文件上生成签名。在一些实施方式中,数字签名可以是MAC(消息认证码),MAC可以由所述设备利用对称加密算法来生成。在一些实施方式中,所述加密密钥可以包括公钥私钥对的私钥,并且加密密钥与第一输入数据的加密组合可以包括:所述设备生成输入文件的至少一些内容的散列;并且通过利用私钥而参数化的非对称加密算法来处理该散列。在一些实施方式中,所述私钥可以存储在外部可移除密钥存储装置上,并且所述设备可以将涉及私钥的加密操作(例如通过利用私钥而参数化的非对称加密算法对所述散列的处理)委托给外部可移除密钥存储装置。

[0028] 在一些实施方式中,所述设备可以包括用于向所述设备的用户提供输出的用户输出接口以及用于获取来自用户的输入的用户输入接口。所述设备还可以适用于:识别所述

输入文件的多个可能的文件类型格式中的至少一个的格式;读取所述输入文件的至少一些内容;通过用户输出接口将所述至少一些内容提供至用户;并且通过用户输入接口从用户获取由用户对提供至用户的至少一些内容作出的许可或拒绝;其中,以下中的至少一个可以为在所述设备上获得许可的条件:将密钥与第一数据进行加密组合;或者返回包括加密组合结果的至少一个输出文件。所述用户输出接口可以例如包括显示器,例如LCD(液晶显示器)。用户输入接口可以例如包括键盘,该键盘可以例如包括用于指示许可的OK(确定)按钮以及用于指示拒绝的Cancel(取消)按钮。在一些实施方式中,输入文件可以包括例如可表示交易的数据,并且所述设备可以将这些数据提供至用户以供许可。如果用户许可所提供的数据,则所述设备可以接着在这些数据上生成签名。如果用户拒绝所提供的数据,则所述设备可以拒绝生成有效签名。在一些实施方式中,输入文件可以包括呈文本形式的待签名的数据,并且将该文本提供至用户。例如,在一些实施方式中,输入文件可以包括ASCII(美国信息交换标准代码)文本。

[0029] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设备,所述设备还适于:对输入文件的至少一些内容进行加密或解密,其中所述通信接口还可以适于从主计算机接收所述输入文件,其中所述主计算机可以通过以下来经由通信接口将输入文件发送至所述设备:通过标准大容量存储访问机构的用于保存文件的机构将输入文件保存至由所述设备所提供的大容量存储装置;所述第一输入数据可以包括所述至少一些内容;并且加密密钥与第一输入数据的加密组合可以包括利用加密或解密算法对第一输入数据进行加密或解密,其中可以利用加密密钥将加密或解密算法参数化。在一些实施方式中,加密或解密算法可以包括对称加密或解密算法例如AES。在一些实施方式中,所述输入文件的至少一些内容包括整个输入文件。在一些实施方式中,所述设备可以适于对整个输入文件进行加密或解密。

[0030] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设备,所述设备还包括用户输入接口,用于所述设备的用户向所述设备提供PIN和/或口令值;所述设备还可以适于:通过用户输入接口从用户获得PIN和/或口令值,并且验证PIN和/或口令是否正确;其中,所述将密钥与第一数据进行加密组合或者所述返回包括加密组合结果的至少一个输出文件可以以由用户提供的PIN和/或口令值是正确的为条件。在一些实施方式中,所述设备可以适于验证由用户输入的PIN和/或口令,并且所述设备可以适于仅继续进行密钥与第一数据的加密组合(例如,生成OTP或者生成签名或者对数据进行解密或加密),并且如果PIN和/或口令是正确的,则返回结果。在一些实施方式中,所述设备还可以适于存储参考值,其中,对所获得的PIN和/或口令值的验证可以包括:所述设备将所获得的PIN和/或口令值与参考值进行比较。

[0031] 在一些实施方式中,所述设备可以将对PIN和/或口令的验证委托给外部可移除密钥存储装置。在一些实施方式中,所述设备还可以包括第二通信接口,用于与外部可移除装置进行命令和响应的接收和交换,其中对所获得的PIN和/或口令值的验证可以包括:所述设备经由第二通信接口向外部可移除装置传送PIN和/或口令代表值,所述PIN和/或口令代表值表示用于外部可移除装置进行验证的所获得的PIN和/或口令值;并且所述设备经由第二通信接口从外部可移除装置接收由外部可移除装置对代表值进行验证的结果。

[0032] 在一些实施方式中,所述设备可以是前述实施方式中的任一实施方式所述的设

备,所述设备还包括生物特征传感器,用于获取所述设备的用户的生物特征测量;所述设备还可以适于通过生物特征传感器从用户获得所述生物特征测量,并且验证所述生物特征测量是否正确;其中,以下中的至少一个可以以所获得的生物特征测量是正确的为条件:所述将密钥与第一数据进行加密组合或所述返回包括加密组合结果的至少一个输出文件。在一些实施方式中,所述生物特征传感器可以包括例如指纹传感器,并且生物特征测量可以包括用户的指纹数据。在一些实施方式中,所述设备可以适于验证用户的生物特征测量,并且所述设备可以适于仅继续对密钥与第一数据进行加密组合(例如,生成OTP或者生成签名或者对数据进行解密或加密),并且如果生物特征测量被所述设备接受,则返回结果。在一些实施方式中,所述设备还可以适于存储生物特征参考数据,其中,对所获得的生物特征测量的所述验证可以包括:将所获得的生物特征测量与生物特征参考数据进行比较。

[0033] 在一些实施方式中,所述设备可以将对生物特征测量的验证委托给外部可移除密钥存储装置。在一些实施方式中,所述设备还可以包括第二通信接口,用于与外部可移除装置进行命令和响应的接收和交换,其中对所获得的生物特征测量的所述验证包括:所述设备经由第二通信接口向外部可移除装置传送生物特征测量,以供外部可移除装置进行验证;并且所述设备经由第二通信接口从外部可移除装置接收由外部可移除装置对生物特征测量进行验证的结果。

[0034] 本发明的另一方面提供了一种在电子输入文件上生成数字签名的方法。在一些实施方式中,所述方法可以供前述实施方式中的任一实施方式所述的设备使用。在一些实施方式中,所述方法可以供下述设备使用,所述设备可以包括用于在本地将所述设备连接至主计算机的通信接口,并且所述设备可以适于:当所述设备被连接至主计算机时,将其本身作为大容量存储装置提供至主计算机,主计算机上的应用可以通过用于读取和保存文件的标准大容量存储访问机构来访问大容量存储装置;经由通信接口从主计算机接收所述输入文件;通过向输入文件应用数字签名算法来在输入文件上生成数字签名,其中所述数字签名算法通过签名密钥(secret signature key)被参数化;经由通信接口将输出文件返回至主计算机,其中,所述输出文件包括输入文件上的数字签名。在一些实施方式中,所述方法可以包括以下步骤:使得所述设备在主计算机处进行连接;通过使用一种用于将文件保存至标准大容量存储访问机构的方法将输入文件保存至由所述设备所提供的大容量存储装置来在主计算机处经由通信接口将输入文件发送至所述设备;通过使用一种用于读取标准大容量存储访问机构的文件的方法读取所述输出文件,来在主计算机处经由通信接口从所述设备获得所述输出文件;从输出文件中检索数字签名。

[0035] 在一些实施方式中,所述通信接口包括USB接口,并且其中,所述设备还适于在所述设备连接至主计算机时,将其本身作为USB大容量存储装置类的USB装置提供至主计算机。

[0036] 本发明的又一方面提供了一种用于在电子输入文件中生成数字签名的系统。在一些实施方式中,所述系统可以包括前述实施方式中的任一实施方式所述的设备。在一些实施方式中,所述系统可以包括适于执行前述任一方法的一些或所有步骤的一个或更多个部件。在一些实施方式中,所述系统可以包括:主计算机,该主计算机包括数据处理部件和连接机构,该数据处理部件用于运行软件应用,该连接机构用于将至少一个外部外围装置可拆卸地连接至主计算机,其中,所述主计算机可以适于:支持一类大容量存储装置;如果当

所述设备被连接至主计算机时所述设备将自己通告为属于所述种类的大容量存储装置，则将通过连接机构被连接至主计算机的装置识别为属于所述种类；支持标准大容量存储访问机构以将文件读取和保存至大容量存储装置，所述大容量存储装置经由连接机构连接至主计算机并且被主计算机识别为属于所述类别的大容量存储装置；向软件应用提供标准大容量存储装置访问机构的用于将文件读取到大容量存储装置的第一方法以及标准大容量存储访问机构的用于将文件保存至大容量存储装置的第二方法；所述系统还可以包括：签名设备，所述签名设备包括用于通过连接机构将签名设备在本地连接至主计算机的通信接口，其中所述签名设备可以适于：当签名设备连接至主计算机时，将其本身作为属于所述类别的大容量存储装置提供至主计算机；经由通信接口从主计算机接收所述输入文件；通过将数字签名算法应用于输入文件来在输入文件上生成数字签名，其中通过签名密钥将数字签名算法参数化；经由通信接口将输出文件返回至主计算机，其中所述输出文件包括输入文件上的数字签名；并且其中，所述签名设备通过通信接口和连接机构被连接至主计算机；并且所述主计算机运行签名应用，所述签名应用适于：通过使用标准大容量存储访问机构的用于保存文件的第二方法将输入文件保存至所述设备，来经由通信接口将输入文件发送至签名设备；并且通过使用标准大容量存储访问机构的第一方法读取所述输出文件，来在主计算机处经由通信接口从签名设备获得输出文件。

[0037] 在一些实施方式中，所述连接机构可以包括主连接器或端口(例如USB端口)，其用于将至少一个外围装置可拆卸地连接至主计算机和驱动软件(其针对主连接器)。在一些实施方式中，所述签名设备的通信接口可以包括外围装置连接器，该外围装置连接器可以匹配主连接器或端口。

[0038] 在一些实施方式中，所述通信接口可以包括USB接口，并且所述签名设备还可以适于：当所述签名设备连接至主计算机时，将其本身作为USB大容量存储装置类的USB装置提供至主计算机。

[0039] 在一些实施方式中，所述主计算机可以例如包括笔记本电脑或PC(个人计算机)。在一些实施方式中，在主计算机上运行的应用可以包括客户端应用，该客户端应用使得主计算机的用户能够进行远程访问以及/或者与基于可远程访问计算机的应用进行交互。例如，在一些实施方式中，在主计算机上运行的应用可以包括web浏览器，用户可以与在远程web服务器上运行的基于web的应用进行交互，其中远程web服务器可以经由计算机网络例如因特网被连接至主计算机。该应用可以将待签名的一些数据(例如合同)汇编到输入文件中并且将输入文件提供至用户。用户可以将他或她的签名设备连接至主计算机(例如，在主计算机的USB端口上)，并且签名设备可以将其本身作为大容量存储装置(例如USB大容量存储装置)提供至主计算机。用户可以例如在称为“待签名文件”的目录中下载文件，并且将具有待签名数据的输入文件保存至签名设备(其作为大容量存储装置出现在主计算机上)。签名设备可以通过创建其中包括签名的输出文件来对输入文件进行签名和用信号通知该签名已准备好用于检索，所述签名可以具有与输入文件相同的名称或者可以具有固定名称(例如‘signature_file’)，或者可以是输入文件名称的更改版本，并且可以使得该输出文件在例如称为“签名”的目录中的特定位置处可用，并且用户可以指引浏览器来将该输出文件读取并上传至应用。在一些实施方式中，输入文件可以是文本文件，并且签名设备在对所述输入文件的内容进行签名之前可以在签名设备的显示器上将在输入文件中包括的文本

提供至用户。用户可以查看所提供的文本，并且通过按压在签名设备的键盘上的OK(或Cancel)按钮来许可(或拒绝)所提供的文本。在用户已许可所提供的文本之后，签名设备可以接着对该输入文件进行签名。

[0040] 在另一示例中，用户可以使用客户端应用与需要用户来认证的应用进行交互。客户端应用可以通过读取其中包括一次性口令的输出文件来获得一次性口令(其可以具有固定的名称和位置，例如“凭证/一次性口令”)，其中，该设备可以在接收到要读取所述输出文件的请求时立即生成一次性口令。然后，应用可以从输出文件中检索一次性口令。在一些实施方式中，所述设备可以生成一次性口令或者通过使用非对称数字签名算法来对文件进行签名，其中可以通过与用户相关联的公钥私钥对的私钥将非对称数字签名算法参数化。在一些实施方式中，应用可以通过读取其他特定文件来获得与私钥对应的公钥和/或公钥的证书(用于验证签名或一次性口令)，其中其他特定文件可能包括公钥和/或证书(如“凭证/公钥”或“凭证/证书”)。在其他实施方式中，可以将公钥和/或证书作为签名或一次性口令编码到同一输出文件中。

[0041] 在一些实施方式中，根据本发明的方面的设备包括或者包括签名装置，该签名装置具有用于在本地将所述装置连接至主计算机的第一通信接口，该主计算机可以包括通用计算装置，例如PC(个人计算机)或者笔记本电脑。在一些实施方式中，通信接口可以包括USB接口。在一些实施方式中，签名装置将其本身作为USB大容量存储装置类的装置通告所连接的主计算机。

[0042] 在一些实施方式中，签名装置可以适于：从签名装置通过其USB接口所连接的主计算机接收输入文件，其中主计算机可以通过经由用于将文件保存至USB大容量存储装置类的装置的标准接口以将输入文件保存至签名装置所提供至主计算机的大容量存储装置来将输入文件递送至签名装置。然后，签名装置可以使用与用户相关联的公钥私钥对的私钥来对所接收的输入文件进行加密处理。签名装置可以将输入文件的加密处理结果(例如，签名或经解密的文件或一次性口令)存储在输出文件中。主计算机上的应用可以通过以下来获得结果：通过用于从USB大容量存储装置类的装置读取文件的标准接口，从签名装置提供至主计算机的大容量存储装置读取所述输出文件。

[0043] 在一些实施方式中，签名装置可以安全地存储与用户相关联的签名密钥，并且可以适于使用所存储的用于对文件进行签名或解密的签名密钥根据加密算法来执行加密计算。在一些实施方式中，签名密钥可以包括与用户相关联的公钥私钥对的私钥，并且加密算法可以包括非对称加密算法，例如RSA(Rivest-Shamir-Adleman)算法或椭圆曲线算法。

[0044] 用于智能卡的接口装置。

[0045] 在一些实施方式中，签名装置可以包括用于与外部可移除密钥存储装置进行通信的第二通信接口，该外部可移除密钥存储装置适于存储与用户相关联的私钥，并且使用所存储的私钥根据非对称加密算法来执行加密计算。在一些实施方式中，签名装置可以将涉及私钥(例如用于对文件进行签名或解密或者用于生成OTP)的加密计算中的至少一些加密计算委托给密钥存储装置。在一些实施方式中，第二通信接口可以包括智能卡接口，并且密钥存储装置可以包括智能卡。在一些实施方式中，智能卡可以是ISO 7816可兼容的智能卡，并且第二通信接口可以是ISO 7816可兼容的。在一些实施方式中，智能卡可以是具有PKI功能的智能卡。

[0046] 加密库、智能卡阅读器和/或智能卡驱动器的仿真。

[0047] 在一些实施方式中，签名装置可以用于模拟加密库、USB智能卡阅读器和USB智能卡驱动器中的一个或更多个(包括所有三种的组合)，从而不再需要将所述这些的一个或更多个提供或安装在用户的主计算机上。

[0048] 例如，在一些实施方式中，寻求在电子文件例如电子文档上获得签名的应用可以如下继续进行，其中利用与用户相关联的私钥生成签名，并且将其安全地存储在例如用户的智能卡上。代替与标准加密的API例如PKCS#11或MS-CAPI进行对接以获得通过与用户相关联并存储在用户的智能卡上的私钥来签名的电子文档，所述应用可以使用标准接口将待签名的文件传送至签名装置，以将包括电子文档的文件保存至USB大容量存储装置类的装置。然后，签名装置可以进行通过使用现有智能卡命令与智能卡针对生成签名进行交互来在电子文档上生成签名。例如，签名装置可以通过用于将文件保存至签名装置的标准USB大容量存储装置类接口从主计算机上的应用接收具有待签名的电子文档的输入文件。然后，签名装置可以(例如使用散列算法，例如SHA-1)生成所接收的电子文档的消息摘要，并且使用普通现有的智能卡命令来将所生成的消息摘要递送至智能卡，以指示智能卡在消息摘要上生成签名并且从智能卡接收所生成的签名。然后，签名装置可以将所接收的签名保存在输出文件中，并且所述应用可以通过以下来检索包括签名的该输出文件：通过用于从签名装置读取文件的标准USB大容量存储装置类接口，从签名装置读取所述输出文件。

[0049] 对电子文件进行签名。

[0050] 在一些实施方式中，签名装置可以用于按以下方式对电子文件进行签名。所述应用可以通过使用用于将文件保存至签名装置的标准USB大容量存储装置类接口来将待签名的文件(其还可以被称为输入文件)传送至签名装置。当接收到所述输入文件时，签名装置可以使用与用户相关联的私钥在所接收的输入文件上生成签名。当签名装置已生成签名时，签名装置可以使得能够读取包括所生成的签名的输出文件。所述应用可以如将在下面更详细地描述的那样通过使用用于从签名装置读取文件的标准USB大容量存储装置类接口读取该签名文件或输出文件来获得签名。

[0051] 在一些实施方式中，输出文件采用标准签名格式。在一些实施方式中，输出文件包括待签名的原始文件的数据以及实际签名二者。在一些实施方式中，输出文件的格式可以通过输入文件的格式来确定。在一些实施方式中，签名装置可以在输入文件被接收时立即处理待签名的输入文件，并且可以不存储整个输入。例如，在一些实施方式中，签名装置可以立即在输入文件上生成消息摘要，并且当输入文件的原始内容已经被用于生成消息摘要时可以丢弃输入文件的原始内容，并且可以使用消息摘要来生成签名。

[0052] 对电子文件进行解密。

[0053] 在一些实施方式中，签名装置可以用于利用与用户相关联的私钥对应的公钥来对已加密的电子文件进行解密。所述应用可以通过使用用于将文件保存至签名装置的标准USB大容量存储装置类接口来将待解密的文件(其还可以被称为输入文件)传送至签名装置。当接收到所述输入文件时，签名装置可以使用与用户相关联的私钥对所接收的输入文件进行解密。当签名装置已经将输入文件解密时，签名装置可以使得能够读取包括解密文件的输出文件。所述应用可以如将在下面更详细地描述的那样通过使用用于从签名装置读取文件的标准USB大容量存储装置类接口以读取该解密文件或输出文件来获得签名。

[0054] 生成一次性口令。

[0055] 在一些实施方式中,签名装置可以用于生成一次性口令,其中,用户的私钥用于对动态变量进行签名,其中动态变量的值是签名装置和将验证一次性口令(OTP)的实体二者已知的(或使得知晓)。在一些实施方式中,一次性口令可以包括动态变量上的签名。在一些实施方式中,通过签名装置生成以及/或者保持动态变量。例如,在一些实施方式中,签名装置可以包括用于生成时间值的时钟,签名装置可以使用该时间值来确定用于生成基于时间的OTP的动态变量的值。在其他实施方式中,签名装置可以将基于某些事件而更新的事件相关值存储和保持在存储器中,并且签名装置可以使用该事件相关值来确定用于生成基于事件的OTP的动态变量的值。例如,在一些实施方式中,签名装置可以每当签名装置生成一次性口令时更新该事件相关值。在一些实施方式中,事件相关值可以是计数器,并且更新事件相关值可以包括递增计数器。在一些实施方式中,更新事件相关值可以包括:签名装置用新值替换事件相关值的当前值,其中该签名装置可以根据事件相关值的当前值来计算所述新值。在一些实施方式中,签名装置可以例如通过将散列函数应用于事件相关值的当前值来计算事件相关值的新值。

[0056] 当签名装置已生成一次性口令时,签名装置可以使得能够读取包括该一次性口令的输出文件。所述应用可以如将在下面更详细地描述的那样通过使用用于从签名装置读取文件的标准USB大容量存储装置类接口以读取该签名文件或输出文件来获得签名。在一些实施方式中,可以通过经由标准USB大容量存储装置类接口的要读取具有一次性口令的文件的读取请求来提示由签名装置生成一次性口令。在一些实施方式中(例如在基于时间的OTP的情况下),签名装置可以在接收到来自主计算机的要读取一次性口令输出文件的请求时,立即计算一次性口令,用新生成的OTP更新一次性口令输出文件的内容,并且将所更新的OTP输出文件返回至主计算机。在一些实施方式中(例如在基于事件的OTP的情况下),签名装置可以计算新的一次性口令,并且在主计算机读取OTP输出文件之后用新计算的OTP值更新OTP输出文件的内容。

[0057] 在一些实施方式中,除了一次性口令的值之外,OTP输出文件还可以包括由签名装置用于计算OTP的动态变量的值。

[0058] 在一些实施方式中,OTP输出文件可以包括采用人类可读格式的OTP的值。在一些实施方式中,OTP输出文件可以例如是文本文件,并且OTP可以例如以ASCII格式被编码。在一些实施方式中,用户可以利用例如主计算机上的文件管理器应用来打开包括一次性口令的输出文件,复制包括OTP的输出文件中的文本,并且将所复制的OTP粘贴到应用中。

[0059] 接收输入文件。

[0060] 在一些实施方式中,签名装置适于:对通过用于将文件保存至签名装置的标准USB大容量存储装置类接口接收的任何文件进行签名或解密。在一些实施方式中,签名装置可以适于对其文件名称与特定格式符合的任何文件进行签名或解密。例如,在一些实施方式中,签名装置可以适于对通过用于将文件保存至签名装置的标准USB大容量存储装置类接口接收到的具有特定文件名称(例如“input_file_to_be_signed”)的任何文件进行签名,以及/或者类似地对具有另一特定文件名(例如“input_file_to_be_decrypted”)的任何文件进行解密。在一些实施方式中,签名装置可以适于对通过用于将文件保存至签名装置的标准USB大容量存储装置类接口接收到的具有特定文件路径或正被保存至特定位置(例如,

目录“input_files_to_be_signed”)的任何文件进行签名,以及/或者类似地对在另一特定位置(例如,目录“input_files_to_be_decrypted”)接收到的任何文件进行解密。

[0061] 将输出文件提供给主计算机。

[0062] 在一些实施方式中,(如果适用的话,即如果执行涉及输入文件的操作)可以由签名装置将输出文件保存在由标准USB大容量存储装置类接口使用的名称和位置下,以便正式保存所述输入文件。也就是说,不是(如USB大容量存储装置类接口所指示的)将输入文件本身保存在给定名称下和指定位置处,而是签名装置可以将输出文件保存在该名称下和该位置处。例如,这可以在对文件进行签名或解密的情况下适用。在一些实施方式中,签名装置可以将输出文件提供在固定位置处(例如在具有固定路径的目录例如“signature_files”中),并且输出文件的名称可以例如是与已签名或已解密的输入文件的名称相同的名称。在一些实施方式中,当生成新的输出文件时,最近生成的输出文件被自动删除或者覆盖。在一些实施方式中,签名装置可以将输出文件提供在固定位置处(例如在具有固定路径的目录例如“output_files”中)以及在固定名称(例如“one_time_password”)下。

[0063] 在一些实施方式中,签名装置可以适于执行多种类型的口令操作,例如在输入文件的内容中的至少一些上生成签名,生成一次性口令或者对输入文件的内容中的至少一些进行加密或解密。在一些实施方式中,可以在输入文件的名称或名称的结构中指示要执行的操作。在一些实施方式中,可以在输出文件的名称或名称的结构中指示要执行的操作。在一些实施方式中,可以在输入文件或输出文件的位置中指示要执行的操作,如在输入文件或输出文件的路径中表示的一样。例如,如果输入文件应当被签名,则可以通过签名应用将输入文件保存在具有特定目录名称例如“input/to_be_signed’的位置处。

[0064] 在一些实施方式中,签名装置可以适于指示何时输出文件是可用的。在一些实施方式中,签名装置指示通过仿真签名装置提供至主计算机的大容量存储装置的断开事件和重新连接事件可得到所述输出文件。在一些实施方式中,签名装置将输出文件提供至另一大容量存储装置中,所述另一大容量存储装置与签名装置提供至主计算机的用于接收输入文件的大容量存储装置不同,并且当输出文件可用时,将具有输出文件的所述另一大容量存储装置连接至主计算机。

[0065] 公钥和证书

[0066] 在一些实施方式中,签名装置可以存储与用户相关联的公钥私钥对的也存储在签名装置中的与前述私钥对应的公钥。在一些实施方式中,签名装置可以附加地存储该公钥的证书,该证书可以将公钥与例如用户的身份加密地绑定。

[0067] 在一些实施方式中,公钥和/或证书可以在签名装置上的文件中得到。在一些实施方式中,主计算机上的应用可以通过使用用于从签名装置读取文件的标准USB大容量存储装置类接口以读取该文件来获得公钥和/或证书。在一些实施方式中,该文件可以位于固定位置(例如具有特定的固定名称的目录例如“证书”)处。在一些实施方式中,该文件可以具有固定的名称(例如“certificate_file”)。

[0068] 在一些实施方式中,如在本申请的别处中更详细地描述的,签名装置可以依靠外部可移除密钥存储装置,该外部可移除密钥存储装置用于存储私钥并且执行涉及私钥的加密计算。在这种情况下,签名装置可以以适当的方式从外部可移除密钥存储装置获得公钥和/或证书(例如,在外部可移除密钥存储装置包括智能卡的情况下,通过交换适用智能卡

的命令和响应以读取公钥和证书)，并且可以将所获得的公钥和/或证书存储在如下文件中，所述签名装置如上所述使所述文件对主计算机上的应用可用。

[0069] 在一些实施方式中并且对于一些操作，公钥和/或证书可以被包括在输出文件中。例如，在生成签名的情况下，公钥和证书可以被包括在签名输出文件中。

[0070] 配置、状态和参数化。

[0071] 在一些实施方式中，签名装置可以是可配置的。在一些实施方式中，可以通过经由用于读取文件的标准USB大容量存储装置类接口以读取配置文件来获得签名装置的当前配置。在一些实施方式中，配置文件可以具有固定名称和/或固定位置。

[0072] 在一些实施方式中，签名装置可以在任何给定的时间处于一组不同的状态中的一种状态。在一些实施方式中，可以通过经由(用于读取文件的)标准USB大容量存储装置类接口以读取状态文件来获得签名装置的当前状态。在一些实施方式中，状态文件可以具有固定名称和/或固定位置。

[0073] 在一些实施方式中，签名装置的某些操作(例如对输入文件进行签名的签名操作)可以是可配置的。例如，在一些实施方式中，选择用于生成待签名的输入文件的内容的消息摘要的散列算法可以是可参数化的。在一些实施方式中，可以在由签名装置执行所述操之前通过将参数文件保存至签名装置来对签名装置的操作进行参数化。

[0074] 固件更新

[0075] 在一些实施方式中，签名装置适于使得能够实现其固件的更新。在一些实施方式中，可以通过将固件更新文件保存至签名装置来更新签名装置的固件，其中，固件更新文件可以具有特定文件名或者可以被保存在特定位置处。在一些实施方式中，签名装置可以要求由可信的认证机构对固件更新文件进行签名。在一些实施方式中，签名装置适于验证固件更新文件上的签名，并且签名装置仅在发现该签名是有效时利用所接收的固件更新文件的内容来更新其固件。

[0076] 用户许可和PIN输入。

[0077] 在一些实施方式中，在加密操作中私钥的使用(例如，以生成签名或者对文件进行解密)可能受制于用户许可。在一些实施方式中，签名装置适于从用户获得这样的许可。在一些实施方式中，签名装置可以包括用于获得用户许可的用户输入接口。在一些实施方式，签名装置可以例如包括OK(确定)按钮，用户可以致动该OK按钮以指示许可。在一些实施方式中，可以通过个人识别码(PIN)和/或口令来保护对私钥的使用。在一些实施方式中，可能会要求用户输入PIN和/或口令，可以将该PIN和/或口令与参考PIN和/或口令进行比较，并且如果由用户提供的PIN和/或口令与参考PIN和/或口令相匹配，则签名装置可以进行到执行与私钥的加密使用有关的操作。在一些实施方式中，签名装置可以包括用户输入装置，该用户输入装置适于允许用户向签名装置提供PIN和/或口令的值。在一些实施方式中，用户可以在主计算机上输入PIN和/或口令，并且主计算机可以通过经由用于将文件保存至签名装置的标准USB大容量存储装置类接口将包括PIN和/或口令的文件保存至签名装置来将PIN和/或口令传送至签名装置。在一些实施方式中，具有PIN和/或口令的所述文件可以以固定名称进行保存，或者可以被保存在固定位置处。在一些实施方式中，PIN和/或口令可以被包括在相同文件中，所述相同文件还保持由签名装置要处理的输入文件(例如，待签名或待解密的文件)。在一些实施方式中，签名装置可以适于存储PIN和/或口令参考值，并且将

从用户接收到的PIN和/或口令与所存储的参考PIN和/或口令值进行比较。在一些实施方式中，签名装置可以适于将从用户接收到的PIN和/或口令递送至外部可移除密钥存储装置。

[0078] 使用对称加密。

[0079] 在一些实施方式中，签名装置可以适于存储与验证实体共享的秘密加密密钥。在一些实施方式中，签名装置可以适于支持对称加密算法。在一些实施方式中，签名装置可以通过使用对称加密算法(例如对称加密算法如AES(高级加密标准)或加密散列算法如HMAC)将该共享密钥与(签名装置可以如上所述的那样获取的)动态变量进行加密组合来生成一次性口令，并且签名装置可以将所得到的一次性口令保存在可由主计算机如上所述进行检索的输出文件中。在一些实施方式中，签名装置可以适于如上所述的那样在通过用于将文件保存至签名装置的标准USB大容量存储装置类接口接收到的输入文件上生成消息认证码(MAC)，并且将所得到的MAC保存在可由主计算机如上所述进行检索的输出文件中。在一些实施方式中，签名装置可以使用利用共享密钥而参数化的对称加密算法(例如对称加密算法如AES或加密散列算法如HMAC)来生成MAC。在一些实施方式中，签名装置可以利用对称加密/解密算法(例如AES)对(如上所述接收的)输入文件进行加密或解密，并且将所得到的加密或解密文件存储在可由主计算机如上所述进行检索的输出文件中。

[0080] 安全装置。

[0081] 在一些实施方式中，签名装置可以具有自己的用户输出接口，该用户输出接口例如可以包括显示器。在一些实施方式中，签名装置可以具有自己的用户输入接口，该用户输入接口例如可以包括键盘。在一些实施方式中，用户输入接口和用户输出接口可以是不可拆卸的并且不是可供用户自行维护的，而是被所述装置完全控制，并且不受主计算机上的恶意软件的干扰所影响。因此，在这种实施方式中，与例如其中总存在如下可能性的PC相比，可以认为所述装置具有值得信任的用户接口：其中，恶意软件如病毒或者木马(Trojan)向用户提供虚假消息，或者获取用户在键盘上输入的任何内容，或者在存储器中读取与安全性应用相关的敏感数据，或者在数据被签名之前更改该数据。在一些实施方式中，所述装置的固件是不可更改的。在一些实施方式中，所述装置可以具有防篡改设置。

[0082] 其他特性

[0083] 在一些实施方式中，签名装置可以具有其自身的电力自主电源例如电池。在一些实施方式中，可以通过USB连接来向签名装置供电。

[0084] 在一些实施方式中，签名装置可以是便携的且重量轻的。在一些实施方式中，签名装置的重量小于200克。在一些实施方式中，签名装置可以是小型且手持的。在一些实施方式中，签名装置可以是袖珍的。在一些实施方式中，签名装置的尺寸在任何方向最大为15cm。在一些实施方式中，签名装置的长度小于15cm、宽度小于8cm并且厚度小于2cm。

[0085] 在一些实施方式中，签名装置可以具有USB密钥或USB记忆棒的形式。在一些实施方式中，签名装置可以具有USB智能卡阅读器的形式。

附图说明

[0086] 根据以下如附图中示出的本发明的实施方式的更具体的描述，本发明的前述和其他特征和优点将是明显的。

[0087] 图1示意性地示出了根据本发明的方面的示例性设备。

[0088] 图2是根据本发明各方面的用于在电子文件上生成数字签名的步骤的流程图。

[0089] 图3是根据本发明各方面的用于在电子文件上生成数字签名的系统的框图。

具体实施方式

[0090] 下面讨论本发明的一些实施方式。虽然讨论了特定的实施方式，但是应理解该讨论仅出于说明的目的。相关领域的技术人员将认识到可以在不脱离本发明的精神和范围的情况下使用其他的部件和配置。

[0091] 图1示意性地示出了根据本发明的方面的本发明的示例性设备(100)(例如签名装置)。所述设备可以包括：第一通信接口(110)，用于在本地将所述设备连接至主计算机(99)；以及一个或更多个处理部件(150)，用于处理数据以及/或者控制所述设备的其他部件，例如第一通信接口。

[0092] 在一些实施方式中，所述设备可以将其本身作为大容量存储装置提供至所连接的主计算机(99)，其中，所连接的主计算机可以将文件保存至该大容量存储装置，并且所连接的主计算机可以从该大容量存储装置中读取文件。在一些实施方式中，第一通信接口可以包括USB接口，并且所述设备可以将其本身作为USB大容量存储装置类的USB装置提供至所连接的主计算机。在一些实施方式中，第一通信接口可以包括连接器，例如USB连接器。在一些实施方式中，第一通信接口可以包括线缆。

[0093] 在一些实施方式中，所述设备适于：当计算机请求通过(用于从USB大容量存储装置类的装置读取文件的)标准USB大容量存储装置类接口读取输出文件时，通过用于将文件保存在USB大容量存储装置类的装置上的标准USB大容量存储装置类接口从主计算机接收输入文件；使用非对称加密算法对所接收的文件进行加密处理，其中利用与用户相关联的公钥私钥对的私钥将非对称加密算法参数化；将所述加密处理结果存储在输出文件中；并且将输出文件返回至主计算机。

[0094] 在一些实施方式中，所述设备还包括用于向用户提供数据和/或消息的人类输出接口(130)。在一些实施方式中，所述设备还包括用于从用户接收输入的人类输入接口(120)。在一些实施方式中，人类输入接口可以适于获取用户的许可。在一些实施方式中，人类输入接口可以适于接收由用户输入的PIN和/或口令。

[0095] 在一些实施方式中，所述设备可以包括一个或更多个存储部件(160)。在一些实施方式中，一个或更多个存储部件可以适于存储所述私钥。在一些实施方式中，所述设备还可以适于利用用于执行上述非对称加密算法的该私钥来执行加密计算。

[0096] 在一些实施方式中，所述设备还包括第二通信接口(180)，用于与外部可移除密钥存储装置(102)进行通信。在一些实施方式中，外部可移除密钥存储装置可以适于安全地存储与用户相关联的私钥(例如在存储器中；未示出)，并且使用该私钥(例如利用数据处理部件；未示出)执行加密计算。在一些实施方式中，所述设备还适于将用于执行非对称加密算法以处理所接收的文件所需的加密计算中的至少一些加密计算委托给外部可移除密钥存储装置。在一些实施方式中，外部可移除密钥存储装置可以包括智能卡，该智能卡可以例如是PKI智能卡。

[0097] 在一些实施方式中，所述设备还可以包括用于提供时间值的时钟(170)。在一些实施方式中，所述设备可以适于：例如通过利用与该用户相关联的私钥来对时间值进行签名

来将该时间值用作用于生成一次性口令的动态变量。

[0098] 图2示意性地示出了根据本发明的另一方面的本发明的示例性方法(200)。该设备可以包括以下步骤。步骤210:在一些实施方式中,签名装置可以连接至主计算机,并且将其本身提供为USB大容量存储装置类的装置。步骤220:主计算机可以通过以下来向所连接的签名装置发送输入文件:通过用于将文件保存至USB大容量存储装置类的装置的标准接口来将输入文件保存至大容量存储装置,其中所述大容量存储装置由签名装置提供至主计算机。步骤230:签名装置可以从主计算机接收所述输入文件,其中签名装置通过其USB接口连接至该主计算机。步骤240:然后,签名装置可以使用与用户相关联的公钥私钥对的私钥来对所接收的输入文件进行加密处理。步骤250:签名装置可以将输入文件的加密处理结果(例如,签名或经解密的文件或一次性口令)存储在输出文件中。步骤260:主计算机可以通过以下来获得结果:通过用于从USB大容量存储装置类的装置读取文件的标准接口来从大容量存储装置读取所述输出文件,其中所述大容量存储装置由签名装置提供至主计算机。

[0099] 图3示意性地示出了根据本发明的另一方面的本发明的示例性系统(300)。所述系统可以包括:应用服务器(310),用于托管可远程访问的应用;访问装置(320),用于使得用户(390)能够与由应用托管的可远程访问的应用进行交互,并且其中应用服务器和访问装置可以通过公共电信或计算机网络(350)例如互联网彼此通信;签名装置(330),其在本地连接至访问装置,其中,所述签名装置可以包括如结合图1所描述的设备,并且其中签名装置适于:经由访问装置接收输入文件,该输入文件包括要利用与用户相关联的私钥来签名的电子文件(例如电子文档);在所接收的电子文件上生成签名;并且将包括签名的输出文件返回至主计算机。在一些实施方式中,系统可以包括用于验证所生成的签名的验证部件(340)。在一些实施方式中,可以使用结合图2所描述的方法来获得签名。

[0100] 已描述了多个实施方式。然而,应理解可以进行各种修改。例如,可以对一个或更多个实施方式的元件进行组合、删除、修改或补充,以形成其他的实施方式。因此,其他实施方式在所附权利要求的范围内。此外,虽然,可能仅公开了关于本发明的几个实施方式中的一个的特定特征,但是根据任何给定或特定应用的需要或在对任何给定或特定应用有利的情况下,这样的特征可与其它实施方式中的一个或更多个其他特征结合。虽然以上描述了本发明的各种实施方式,但是应理解,这些实施方式仅作为示例提供,而不是限制。具体地,当然不可能为了描述所要求保护的主题而描述部件或方法的每一种可构想到的组合,但是本领域普通技术人员会认识到,许多其他的组合和置换是可能的。因此,本发明的广度和范围不应该被以上所描述的示例性实施方式中的任何示例性实施方式所限制,而是应该仅根据所附权利要求及其等效内容来限定。

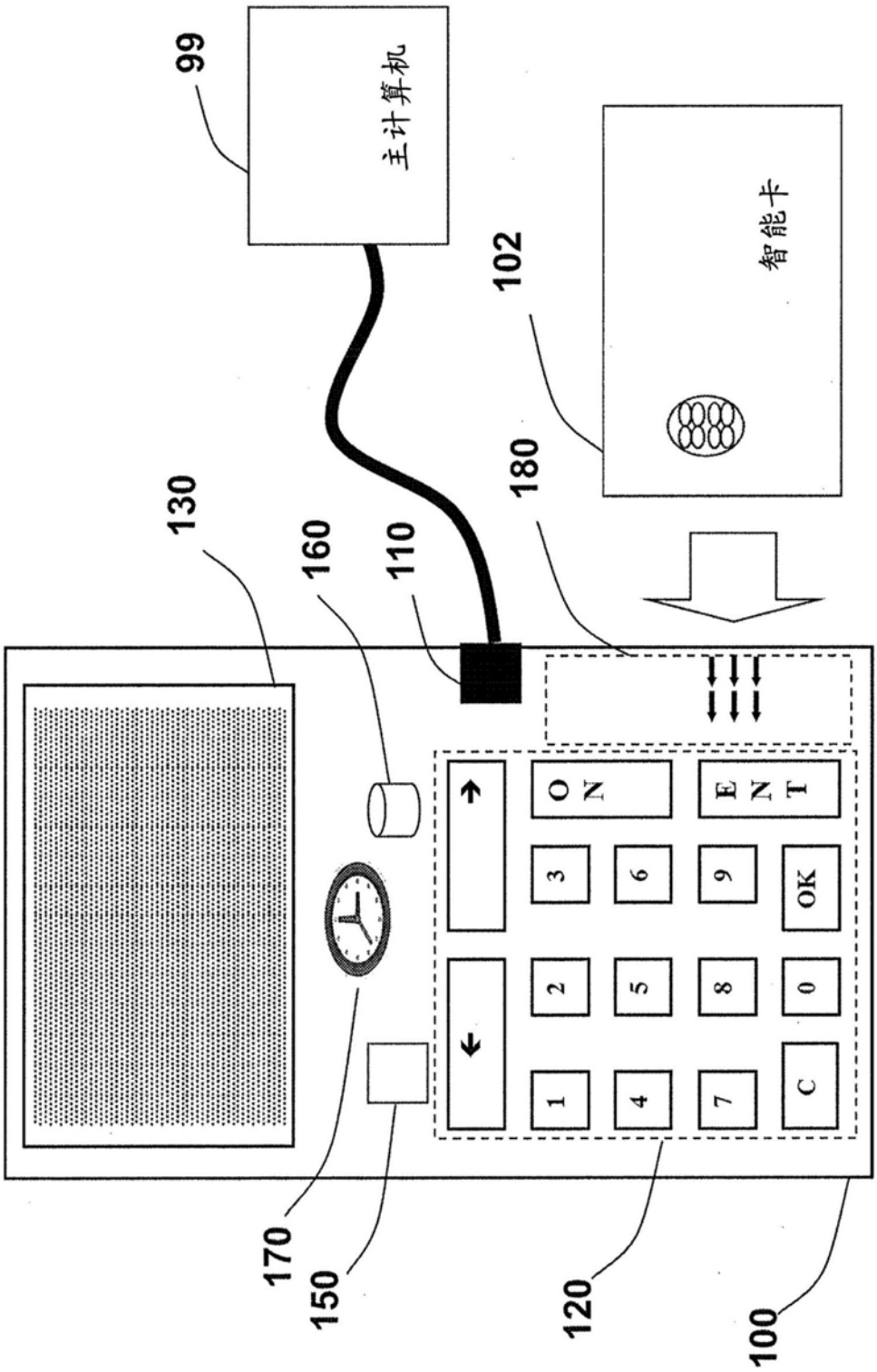


图1

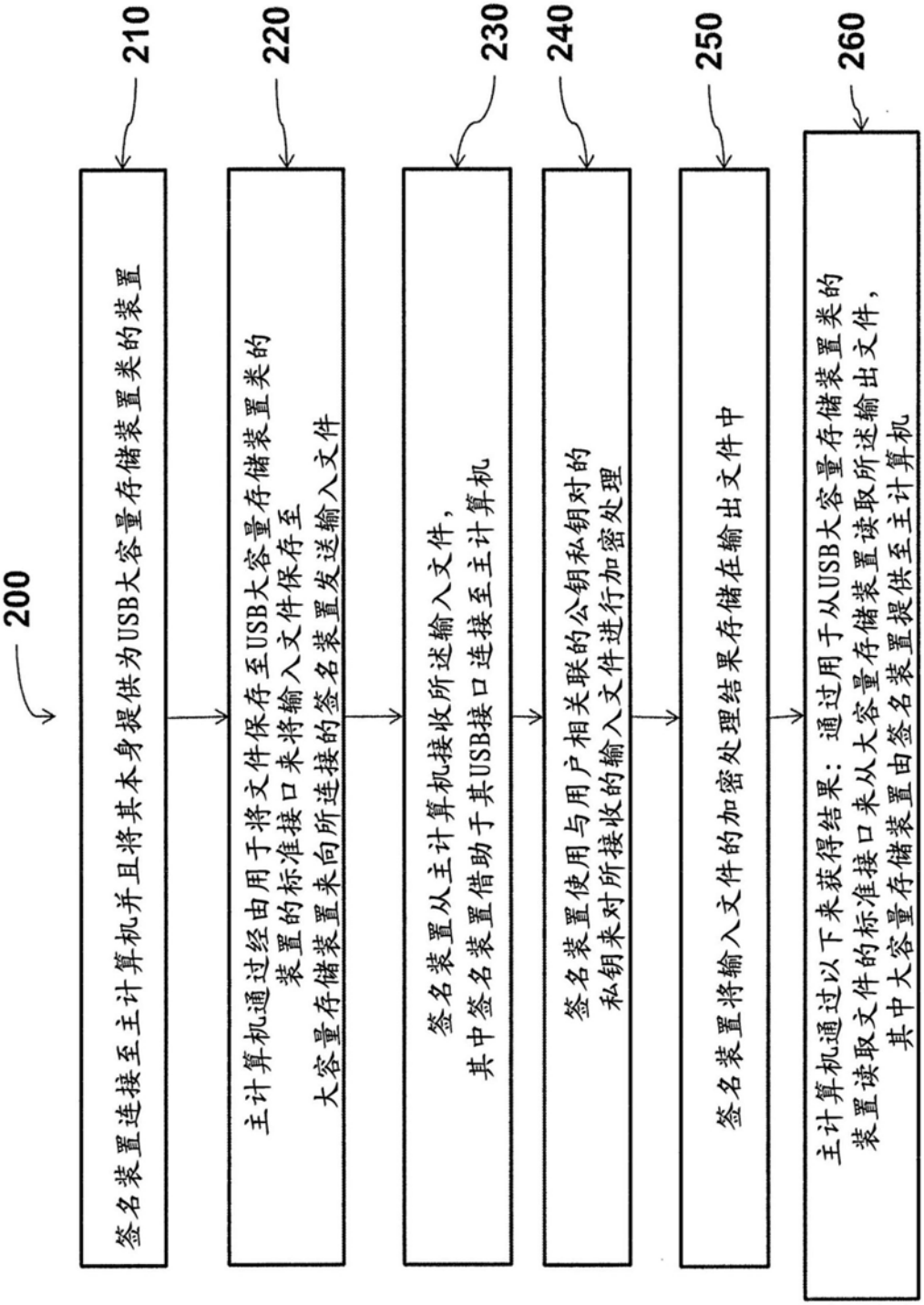

200
210
签名装置连接至主计算机并且将其本身提供为USB大容量存储装置类的装置
220
主计算机通过经由用于将文件保存至USB大容量存储装置类的装置的标准接口来将输入文件保存至大容量存储装置来向所连接的签名装置发送输入文件
230
签名装置从主计算机接收所述输入文件，其中签名装置借助于其USB接口连接至主计算机
240
签名装置使用与用户相关联的公钥私钥对的私钥来对所接收的输入文件进行加密处理
250
签名装置将输入文件的加密处理结果存储在输出文件中
260
主计算机通过以下来获得结果：通过用于从USB大容量存储装置类的装置读取文件的标准接口来从大容量存储装置读取所述输出文件，其中大容量存储装置由签名装置提供至主计算机

图2

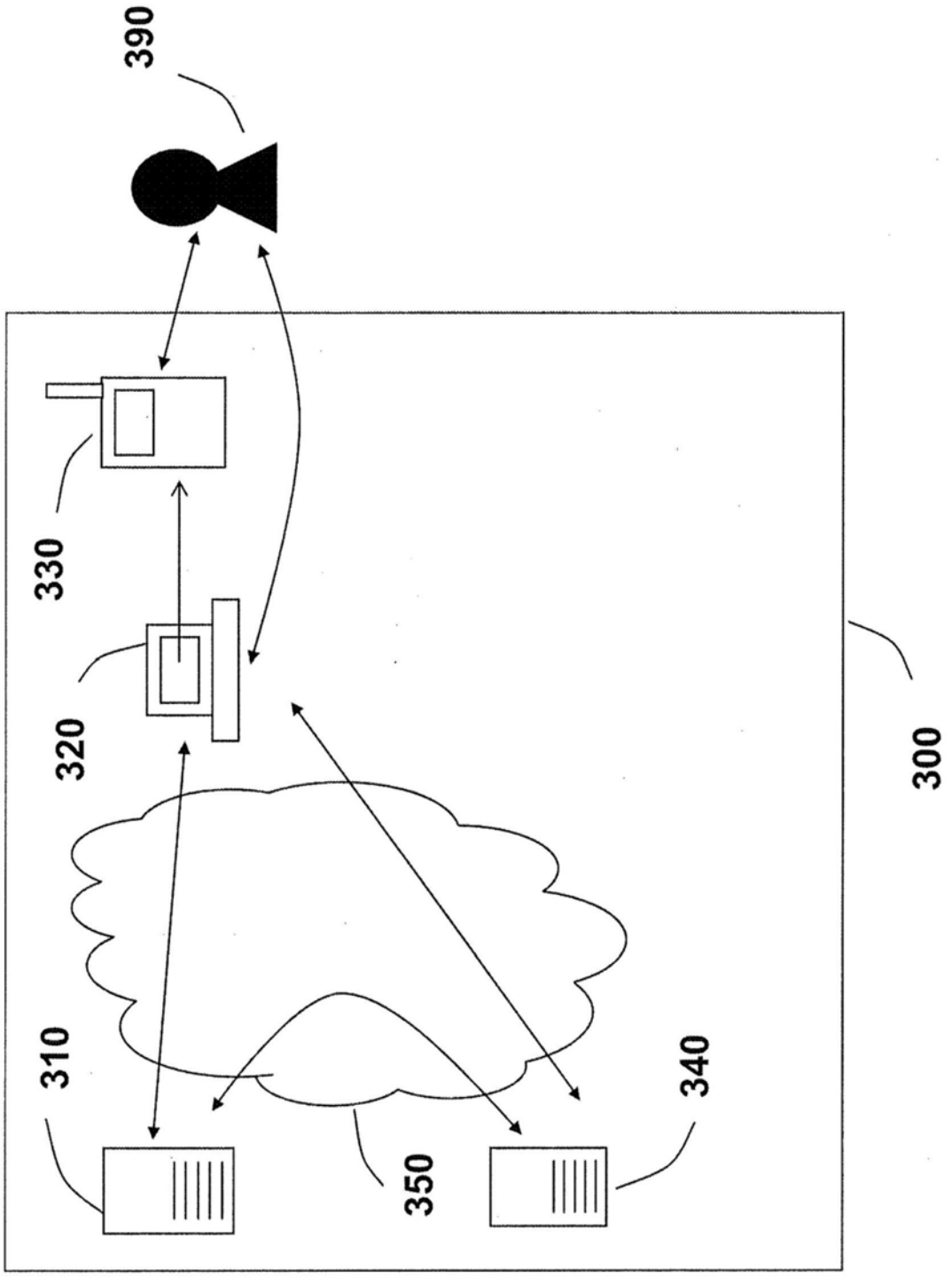


图3