[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
G07F 19/00

[12] 发明专利申请公开说明书

[21] 申请号 01817862.6

[43] 公开日 2004 年 8 月 25 日

[11] 公开号 CN 1524363A

[22] 申请日 2001.10.24 [21] 申请号 01817862.6
[30] 优先权
[32] 2000.10.24 [33] US [31] 60/242,458
[86] 国际申请 PCT/US2001/032624 2001.10.24
[87] 国际公布 WO2002/035764 英 2002.5.2
[85] 进入国家阶段日期 2003.4.23
[71] 申请人 IT 安全解决方案有限责任公司
地址 美国华盛顿特区
[72] 发明人 史蒂芬·B·戴维斯

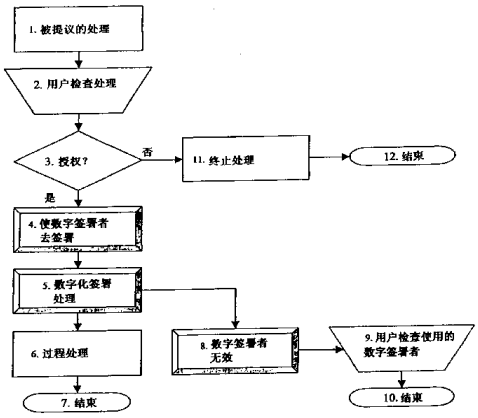
[74] 专利代理机构 北京北新智诚知识产权代理有限公司
代理人 王宏伟

权利要求书 5 页 说明书 14 页 附图 4 页

[54] 发明名称 在实际使用中改善数字签名和公钥基础结构的安全性的过程和装置

[57] 摘要

本发明涉及改善鉴定功能安全性的装置，方法，和商业过程，包括触发一个可使鉴定功能有效的执行器的步骤，授权激活用于一个单独事件的鉴定功能的步骤，和将鉴定功能应用于事件的步骤。该发明还包括用于改善鉴定功能的安全性的计算机可读介质和方法。



ISSN1008-4274

1. 一种用来改善鉴定功能的安全性的装置，所述装置包括：

在单一的事件中使用的用来激活鉴定功能的界面；

其中所述鉴定功能是通过触发执行授权功能的执行器来激活的。

2. 如权利要求 1 所述的装置，其中，所述鉴定功能是一种数字签名功能。

3. 如权利要求 1 所述的装置，其中，一指示器显示鉴定功能已经被激活。

4. 如权利要求 1 所述的装置，还包含在激活所述鉴定功能之前检查所述事件的方法。

5. 如权利要求 1 所述的装置，其中，该执行器由用户触发。

6. 如权利要求 1 所述的装置，其中，所述装置还包括一种安全标识符技术，在使用一种安全标识符确认用户的身份以后，用它来激活鉴定功能。

7. 如权利要求 6 所述的装置，其中，安全标识符是从含有密码和生物特征标识符的组中挑选的。

8. 如权利要求 7 所述的装置，其中，取消激活数字签名的能力是使用鉴定取消列表或约定钥匙列表来完成。

9. 如权利要求 1 所述的装置，其中，授权功能是从一个或更多含有数字签名功能、密码功能和混列功能的组中挑选的。

10. 如权利要求 9 所述的装置，其中，事件鉴定功能是公钥基础结构的组成部分。

11. 如权利要求 9 所述的装置，其中，事件鉴定功能是鉴定基础结构的组成部分。

12. 如权利要求 1 所述的装置，其中，使用一次后，鉴定功能被无效。

13. 如权利要求 1 所述的装置，其中，独特的鉴定功能用于每一事件。

14. 如权利要求 1 所述的装置，其中，该装置以选自于含有智能卡、USB 标记、计算机外围设备和无线通讯设备的组合的设备形式来实现。

15. 如权利要求1所述的装置，其中，该事件由包括信用处理，借贷处理，银行处理，ATM处理，因特网处理，借助任意通讯网络的处理，计算机登录，远程登录，网络登录，合同处理，设施访问处理，设备

授权处理，运载工具授权处理，和用户识别的组中选择。

16. 一种改善鉴定功能的安全性的方法，包含的步骤有：

触发使鉴定功能有效的执行器；

授权激活对单一事件的鉴定功能；和

将鉴定功能应用于事件。

17. 如权利要求16所述的方法，还包含显示鉴定功能已经激活的步骤。

18. 如权利要求16所述的方法，其中，所述触发步骤由用户完成。

19. 如权利要求16所述的方法，其中，授权所述触发步骤包括：在使用安全标识符技术已经确认用户的身份后，激活鉴定功能的步骤。

20. 一种改善鉴定功能的安全性的商业过程，包含的步骤有：

执行鉴定功能；

授权激活对单一事件的使用的鉴定功能；

将鉴定功能应用于事件；和

执行基于鉴定功能的事件。

21. 如权利要求20所述的商业过程，还包含显示已经激活鉴定功能的步骤。

22. 如权利要求20所述的商业过程，其中所述执行步骤由用户完成。

23. 如权利要求20所述的商业过程，其中，所说的执行步骤的鉴定功能包括：使用安全标识符技术鉴定用户的身份后，激活鉴定功能的步骤。

24. 如权利要求20所述的商业过程，其中，所述事件可以通过授权基础结构来取消或授权。

25. 如权利要求20所述的商业过程，其中，所述授权基础结构是使用公钥基础设施来实现的。

26. 如权利要求25所述的商业过程，其中，公钥基础机构使用鉴定取消列表或约定钥匙列表来取消事件或用户。

27. 如权利要求20所述的商业过程，其中，所述事件由含有信用处理，借贷处理，银行处理，ATM处理，因特网处理，借助任意通讯网络的处理，计算机登录，远程登录，网络登录，合同处理，设施访问处理，设备授权处理，运载工具授权处理，和用户识别的组中选择。

28. 存储可改善鉴定指示器的安全性的程序的计算机可读介质，该程序包括：

允许用户使鉴定指示器有效的功能；

授权激活对单一事件使用的鉴定指示器的功能；和

将鉴定指示器应用于事件的功能。

29. 一种改善数字签名的安全性的装置，包括：

触发可使用于处理的数字签名有效的执行器的方法；

授权激活使用在处理中的数字签名的方法；和

将数字签名应用于处理的方法。

在实际使用中改善数字签名和公钥基础结构的安全性的过程和装置

背景技术

1．发明领域

[0001]本发明是关于改善数字签名和公钥基础结构的安全性的装置和方法，因此这些技术能够将数学技巧和软件算法应用于实际，广泛使用的具体实现包含硬件，软件，和加密安全技术的组合。特别是，本发明是关于数字签名和公钥基础结构的使用，用来合法替换，或担当一个实际的，人类签名的代理。

2．相关技术

[0002]物理签名的历史几乎与书写的历史一样长，并且它曾经是由一个刻上的签名来实现或通过某些记号来被鉴定，例如由一个图章戒指留下的蜡印。20 世纪末出现了对一个数字签名加密的概念——个数学函数打乱或压缩一个文档，并在之后使用公钥技术加密杂乱的信息。这种技术是一种有效的数学的或软件的解决方法，但是却未能用于实际的广泛的应用，直至使用数字签名来替代传统签名的合法基础已经形成了。

[0003]同样，智能卡作为一种达到和实现数字签名的方法（如同其他功能一样）已经出现。这些设备在一个便携式设备中放置了一个处理器和内存。该技术在美国没有广泛流行，而在欧洲较为流行。在多数情况下，智能卡已经实际上将使用者的签名的功能替换为了一个信用卡（和信用卡号）的功能，虽然好像智能卡在使用时替代了这两者。

[0004]智能卡的一个关键的局限性是它们没有使得个人将其用于合法签名的必要的操作控制类型。一方面，某些智能卡在设备占有的有效使用方面没有任何安全保护。在另一方面，某些智能卡可以经由一个PIN（个人鉴定号码）激活。这个方法的问题是 PIN“解锁”了智能卡对任何类型的访问限制。如果可以将它同一个房子的一扇锁上的门相比较——用于解锁一个智能卡的 PIN 就像是插进房子的门中的一把钥匙，并且之后当你在里面的时候，它不被取下——允许其他人自由进出。这一因素，结合通常的读取智能卡设备的很差的安全特性，意味着智能卡一旦被激活（即，只要你在家里，门就处于解锁状态）。可以混杂着使用。这对于一个实际的，合法约束的签名是不适合的。

[0005]数字签名解决方案通常包含可以在所有时间内，或者，最好是，一旦应用程序通过一个口令或生物鉴定过程（一个安全鉴别器）被激活时，实现数字签名功能的硬件和/或软件。这个安全鉴别器解锁数字签名的过程，就像在转动一个汽车上的钥匙来点火发动汽车（或是在门锁中转动一个钥匙来打开门）。

[0006]这个方法明显的问题和局限是一个合同约定的签名是一个离散

的事件。传统的合同甚至需要在每一页，主协议，或一个合同的章节部分都需要单独的签名和草签。一个人每一次签署或草签一个合同的某些部分，都制定了一个单独的安全决议，该决议需要用户对这个离散决议的数字签名进行控制。

发明内容

[0007]为了减轻上述的控制的缺乏，依照本发明的“数字签署者”或“数字印章”将数字签名技术和一个智能卡的标记功能结合了起来，但是添加了一个新的元素——一个人性化界面，允许用户控制每一个签名事件的数字签名的激活——从而使得数字签名技术能够用于一个物理的，合法约束的签名的功能。

[0008]依照本发明的一个方面，一个改善鉴定功能安全性的设备包含一个界面用作激活一个用于一个单一事件的鉴定功能，其中所述鉴定功能是通过触发一个实现鉴定功能的执行器激活的。

[0009]依照本发明的另一个方面，一个改善鉴定功能的安全性的方法包含触发一个实现鉴定功能的执行器的步骤，用于单一事件的鉴定功能的授权激活步骤，和对事件应用鉴定功能的步骤。

[0010]依照本发明的一个更进一步的方面，一个改善鉴定功能安全性的商务过程包含执行一个鉴定功能的步骤，用于一个单一事件的鉴定功能的授权激活的步骤，和基于鉴定功能的对事件的操作的步骤。

[0011] 依照本发明的另一个方面，一个用来储存改善鉴定执行器安全性的程序的计算机可读介质，该程序包含允许用户使用一个鉴定执行器的功能，一个用来授权激活一个用于单个事件的鉴定执行器的功能，和一个将鉴定执行器应用于事件的功能。

[0012]依照本发明的一个附加的方面，一个用于改善数字签名的安全性的设备包含激活一个执行器从而使数字签名能用于一个事务处理的方法，授权激活数字签名用于事务处理的方法，将数字签名应用于事务处理的方法。

[0013]显而易见的，对本领域技术人员来说，仅通过例证的方式描述了初步的实施例，而在本发明的范围内可以有许多不同的修正。本发明的这些和其他方面将会在下面被更详细的描述。

附图的简要说明

[0014]图 1 显示了顶级的传统的程序协议处理体系结构。

[0015]图 2 显示了顶级的标准的数字签名协议处理体系结构。

[0016]图 3 显示了顶级的数字签署者/印章的数字签名协议处理体系结构。

[0017]图 4 显示了用于数字签署者/印章处理的顶级事务处理流程图。

最佳实施例的详细描述

[0018]为了减轻在使用标准数字签名技术时缺乏控制这一问题，“数字签署者”或“数字印章”将数字签名技术同一个智能卡的标记功能结合起来，并且添加了一个新的元素——一个人性化界面，允许用户控制每一个签名事件的数字签名的激活——从而使得数字签名技术能够用于一个物理的，合法约束的签名的功能。

[0019]如图 1 所示，在标准物理合同 100 中，个人签署的合同在物理签名 120 和什么被签署的合同之间的联系特性是很清楚的。签署合同表示一个关于被提议处理的条款的协议，由甲方 130 提出。然而，如图 2 所示，标准的数字合同 200，201，和 202 并不总是允许个体签署合同以辨别数字签名 220，221，和 222，和什么被签署之间的联系由于授权数字签名，这一现象经常发生，举个例子，通过激活在一个读取器 215 中的安全性令牌 210，可以授权不止一个数字签名的使用，而不需要个人实际知晓。这一点在什么合同或多份合同被数字式签署，以及在个体和甲方 230 之间什么被达成协议上产生了混淆，在将来问题的处理上带来潜在的问题。

[0020]如图 3 所示，数字签署者/图章的解决方案通过重新存储数字签名 320 和被签署之间的联系来改善对数字协议 300 的授权过程。这个解决方案引入了对在数字签名域中契约性签名的控制。通过在数字签名处理中捆绑一个附加的物理控制和安全层实现这一目的。这个处理允许个人通过将一个安全性令牌 310 插入一个包含合同信息的读取器 315 中获得数字合同的信息。在一个数字签名通过激活一个执行器

312 而被授权之前，个人能够终止并评估是否继续进行处理。执行器 312，它可能简单的就像一个智能卡上的一个按键一样，被用于激活在读取器 315 中的数字签名设备 310，来完成一个单一的数字签名事件。允许个人控制数字签名的使用，并因此帮助甲方 330 确认处理的合法性。这个组件需要被实现因此它需要一个实际的人的物理干涉，并且它控制了数字签名的硬件和/或软件，使得他们将只生成一个单独的数字签名（即，在每一次使用之后立即停用）。任何合适的方法都可以被用于作为一个执行器提供它满足这些方针。执行器可能出现在数字签署者/印章设备中，或是同它相分离。另一个执行器的例子是一个智能卡读取器上的一个按钮。

[0021]数字签署者/印章解决方案的另一个方面是指示器，它指示了被授权的数字签名是否已经出现。做到这点很简单，就像一个可听到的“哔哔声”或声调，一个可见的发光，或者一个执行器按钮返回一个“不可按下”状态。允许用户确定是否授权和开始另一个签名，或者在处理过程中是否存在失败。其他的指示器也可以被提供给数字签署者/印章设备，包括一个设备已经失效的指示器，一个设备已经重新有效的指示器，和显示数字签名事件是否完全成功或事件是否失败的指示器。

[0022]数字签署者/印章设备可以附加的使用安全标识符技术，例如一个口令或生物鉴定系统，用作数字签署者/印章设备的常规激活——允许执行器是一个非常简单按钮或其他组件或动作（就像在钥匙对汽车“鉴定”它自己之后，旋转动作激活一个汽车的点火系统一样）。

当一个安全标识符技术被使用时，数字签名在执行器被触发之后被授权，并在安全标识符技术通过确认被提供的正确的口令或其他信息而授权了用户之后提供。

[0023]数字签署者/印章设备可以选择性的支持附加能力如处理记录的本地储存——或者储存整个处理，或者储存某些关键元素例如参与者，处理时间，甚至处理关键元素的一个总和，等等。设备也可以有能力将记录输出给一个远程系统用作储存或稍后的检查。支持来自外部设备的检查。数字签署者/印章设备也能够选择性地允许检查直接由设备签署的处理，反对不会被用户相信的通过另一设备提供的一个显示的处理。这种控制的最终水平确保了用户知道什么被签署，同样的提供整体的签名处理的控制。操作的限制和花费趋向于限制这个发明实现的实用性。数字签署者/印章设备的体系也更好的把签名从实现签名的实体中分离了出来。因此使用这个解决方案的智能卡或其它设备可以被用于多重处理类型，不是一个单一的金融，商务，或个人的处理类型。

1．介绍

[0024]数字签署者/印章处理包含了一个常规的全面的处理，它有几个步骤被引入以提供期望的用户控制。以下是相关的术语：

• 执行器——用来使在一个安全性令牌中的数字签署者/印章功能有效的一个组件或动作。由本发明想象的执行器的例子是在汽车中一个按键或旋转钥匙动作。

•指示器——一个用来使一个用户获知数字签名被执行器授权、数字签名事件成功或是失败以及安全性令牌被激活或是无效的组件或动作。

•数字签名——在硬件或软件中实现的一个数学函数，它捆绑一块数据给一个用户。数学上，一个数字签名可以包含一个打乱功能来把一个数据流压缩到很小，和/或一个仅仅只能由一个用户实现的公钥加密功能。

•读取器——一个使用一个安全性令牌使得处理数据和数字签名通讯的设备。读取器可以提供关于事件的信息给安全性令牌，并能够同安全性令牌使用无线通讯技术交换信息。

• 安全标识符——一个密码，生物性鉴别者，或其他授权方法。

• 安全性令牌——一个设备，例如实现数字签名和数字签署者/印章功能的一个智能卡，USB 令牌，或无线通讯设备。一个安全性令牌，用于本发明的用途，可以是一个常规用途设备，如一个支持数字签名生成的个人电脑或简单的信用卡。

•处理——用于本发明的用途中的一个合同，决议，或其他相互作用，包括至少一个用户和其他方（称为甲方）。任何其他的用户和甲方可以依照本发明使用该设备授权这个处理，或是他们可以使用其他方法

来授权这个处理。我们所感兴趣的处理是那些需要由用户清晰的授权——如一个合法合同或购买。

•用户——一个授权处理的人类个体。对多用户而言可能通过给设备提供独特的对话或功能，从而使用一个单一的设备，很像一个共享的电脑。注意一点，第三方也能够作为一个用户授权一个处理，因为发行数字签名的授权是由设备的持有者，而不是特定的用户进行约束。它也可能允许一个单独的用户拥有多重的标识符或角色联系一个设备。

2. 实施例

[0025]参照图 4，下面提供一种示范处理的处理流程，突出了数字签署者/印章的具体要素。在开始任何一种处理之前，将对用户提供一种安全性令牌以及任何必要的安全标识符。安全性令牌可能由一家能够合法授权予一种特定事件类型的官方来发布并配置。安全性令牌也可以由那些能够授权予不同事件类型的若干机构或系统来配置用途。这样的授权机构有能力阻止事件的完成，或取消完成的事件，甚至可以取消安全性令牌。

i．被提议的处理（第 1 步）

[0026]任何处理都以被创建的被提议的处理的一些初步结果开始。被提议的处理信息可能通过读取器或任何其它合适手段提供给安全性令牌。

ii. 用户检查（第 2 步）

[0027]在签署它之前，用户先检查被提议的处理。这与传统的合法绑定的合同或购买在处理的完成上是一致的。理论上，检查处理的方法将在用户完全信任的环境中实现。一个实例是由安全性令牌提供的某类屏幕或其它界面。并且，处理信息由安全性令牌存入日志，用来提供该过程的独立记录。

[0028]实际上，成本、尺寸和内存约束可能使这些功能不切实际，因此，可能不得不对某一类型的工程技术做出妥协。

iii. 授权决定（第 3 步）

[0029]在用户检查完被提议的处理之后，用户确定是否继续进行处理。如果用户确定继续进行，则进行第 4 步，否则，进行第 11 步。

iv. 有效的数字签署者（第 4 步）

[0030]用户将使用执行器组件或作用，并结合安全性令牌，来使数字签署者功能有效。注意数字签署者功能最好只为单一的用途而有效。

v. 数字签名处理（第 5 步）

[0031]数字签署者功能可以数字化签署处理，并将后续的处理过程（第 6 步）的结果返回给读取器。数字签署者设备将最优先处理对安全状态（第 8 步）。

vi. 处理过程（第 6 步）

[0032]读取器，甲方，任何其它参与处理者，如附加方和公证人，以及任何涉及处理的附加过程，将继续进行，以完成处理的过程。如果需要附加的数字签名，最好独立授权（返回到第 1 步）

vii. 结束处理（第 7 步）

[0033]完成基本处理过程流程。

viii. 数字签署者无效（第 8 步）

[0034]一旦用户授权的数字签名已经产生，那么数字签署者设备将使安全性令牌在没有额外用户授权的情况下，不能产生附加的数字签名。该设备可能可选择的给出一种指示：它是无效的。一旦成功产生数字签名，该安全性令牌就最好自动失效。

ix. 用户检查数字签署者的使用（第 9 步）

[0035]指示器将向用户提供通知：数字签署者被使用。

[0036]有必要处理错误来确保数字签署者/印章过程的安全被保护，这是执行特性。

x. 结束数字签署者过程（第 10 步）

[0037]数字签署者/印章设备最好返回到它的初始状态，并且为支持另一处理的过程做好准备（第 1 步）。

[0038]注意该数字签署者/印章过程不必绑定到一种单一类型的处理。而且，数字签署者/印章设备不必专门仅仅用于鉴定和授权处理。因此，单一的数字签署者/印章设备能够用于所有用户的信用卡处理、支票签名和合同签名——非常像某人的物理签名可以为所有的交易工作。该设备也可以用于自动取款机、借贷、和银行处理；借助因特网或其它通讯网络的处理，包括在无线环境中执行的处理；直接、网络或远程登录计算机或其它系统；设施访问；设备或运载工具授权；以及用户识别处理。

xi. 终止处理（第 11 步）

[0039]如果用户确定他不想继续进行处理，那么数字签署者/印章设备将不被有效，从而拒绝或取消事件授权。该取消可以作为经鉴定的取消列表或约定钥匙列表存储在该设备中或外部方式中。

xii. 结束终止的处理（第 12 步）

[0040]该设备返回到初始状态，准备继续进行新的处理（第 1 步）。

3. 发明的结论、分支和范围

[0041] 接下来是数字签署者/印章系统的选择性应用：

- **因特网处理**——数字签署者处理的安全性有助于降低因特网处理关于“谁授权什么”的含糊性，因而可以除去与“卡不在现场”处理（如借助电话或因特网的处理，那儿接收商不能看到卡或卡

持有者）相关的较高费用。还有，诸如数字签署者/印章过程的解决方法可能有必要可信地执行因特网业务，没有无节制的法律风险或不用恢复使用传统邮件和签名来提供“真正的”签名。

- **计算机和网络登录**——用户可以使用数字签署者/印章设备并改善登陆的安全性。

- **信用卡和 ATM 系统**——传统上，物理信用卡处理可能招致许多安全性问题，由于这些卡经常被盗或错放。还有，有些处理是在卡持有者不在场（如侍者在餐馆处理账单）的情况下进行的。数字签署者/印章设备和过程可以整合到传统信用卡处理过程中，从而有助于降低这种安全性问题。由于数字签署者没有绑定到一个具体的卡或卡号中，因而可以创建一种单一的授权系统。这还带来额外的好处：对用户来说，降低了增加新卡或新服务的成本，因为降低了基础设施的成本。最后，数字签署者/印章设备和系统提供一种解决丢失钱包的实际问题的方法——用户不必试图记起哪几张卡丢失了，唯一要做的事情是确认数字签署者/印章设备是否丢失，并且用户只要给卡片发行者打个电话就可以使它失效。

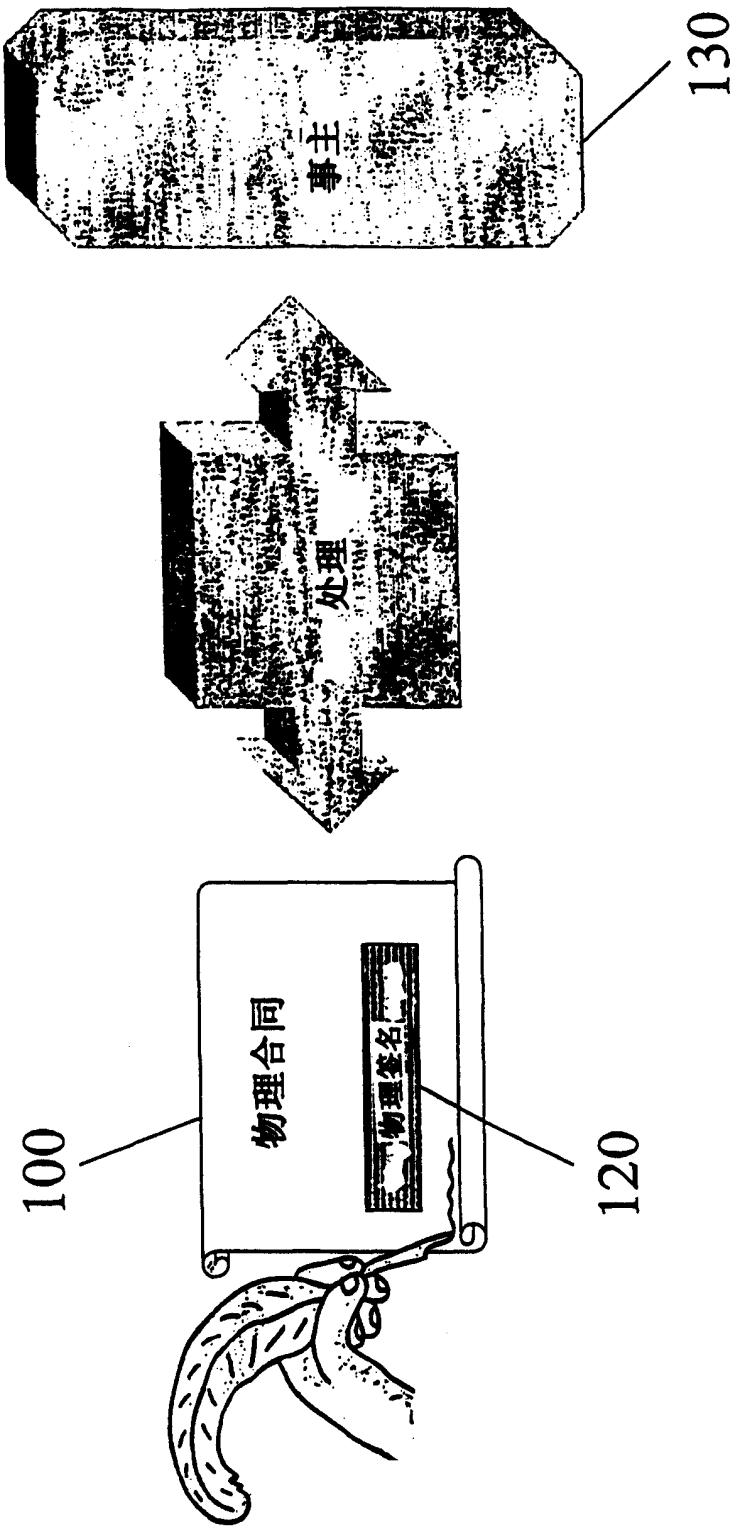
- **设备有效和设施访问**——便携式电话以及甚至汽车都使用个人身份号码（PIN）和其它的安全设备来授权它们的激活。数字签署者/印章设备可以替代这些不同的工具，从而简化消费者的生活，并且对个人来说，使安全性能够适合满足个人、业务、合法、保险和法律生效的要求。新服务，如电子闹钟，也可以根据本发明使

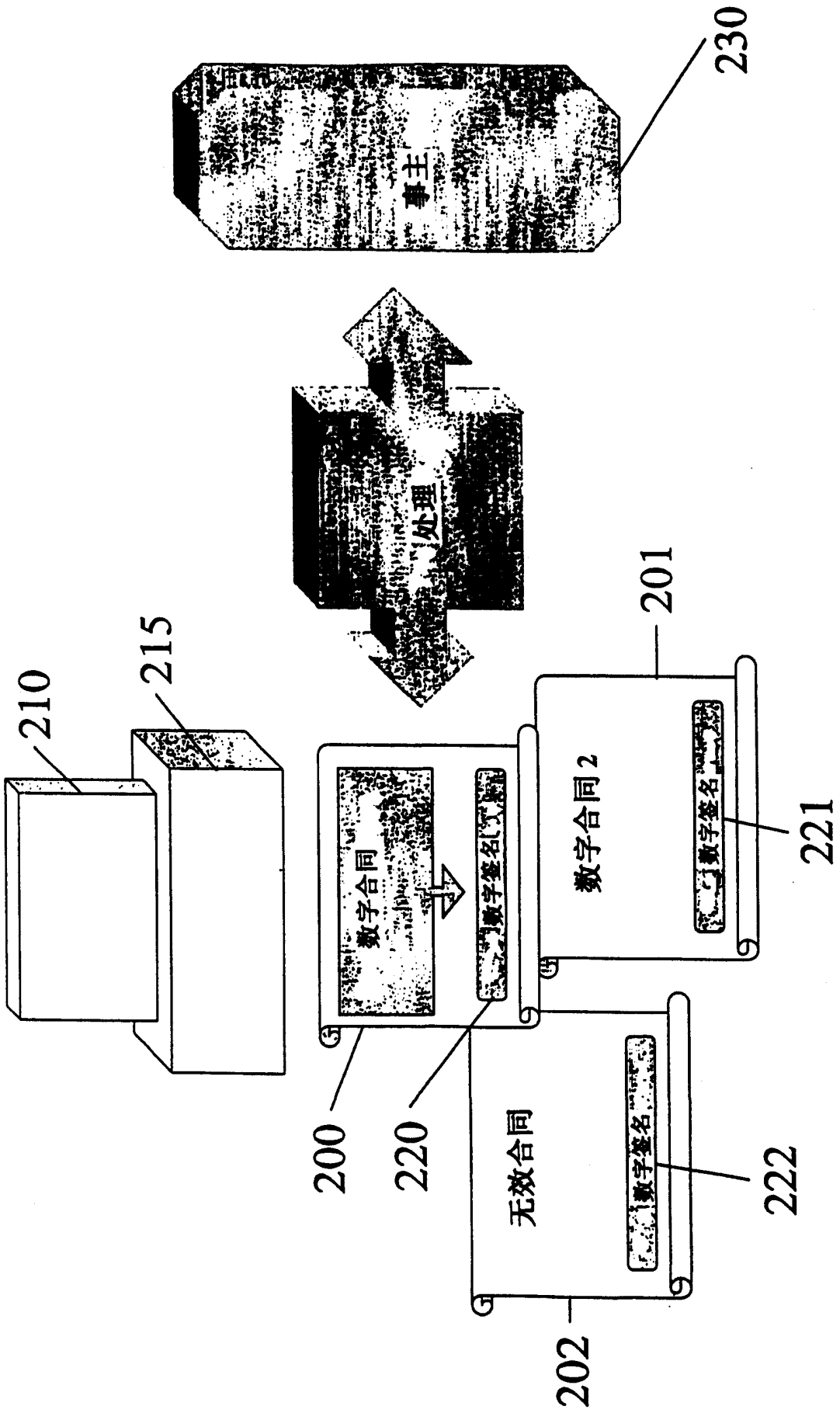
用该设备和系统来创建。

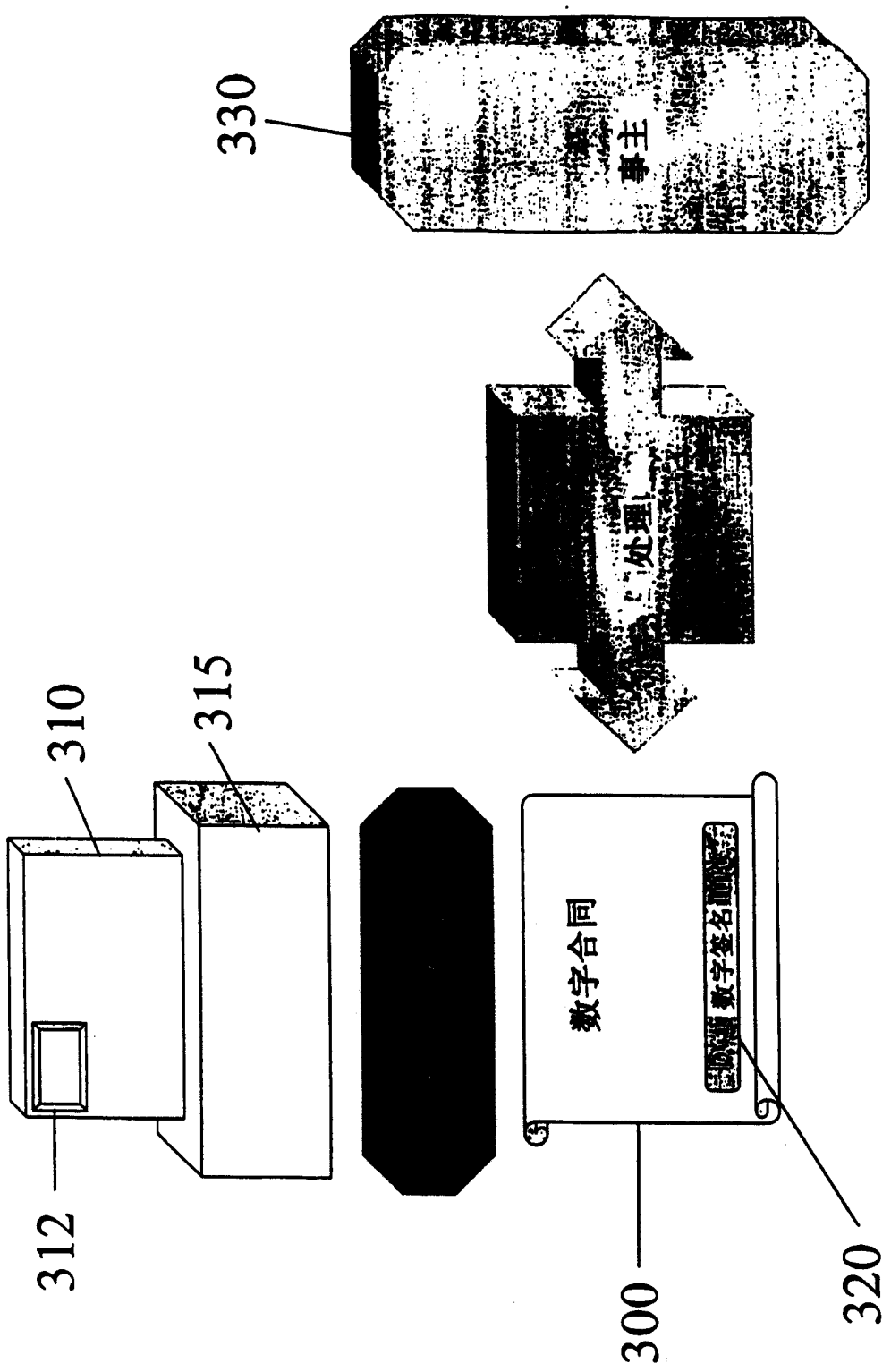
- **识别和隐私**——数字签署者/印章设备和系统可以授权予一种新水平的隐私或对个体的控制识别，通过控制个体和处理之间的连接来进行，从而不依靠处理团体。一种强大的识别系统意味着：可选择电子“角色”的合法创建可以被使用，不会危害处理的合法性，或者相反地，可以实施一种强大而可追踪的识别基础结构。

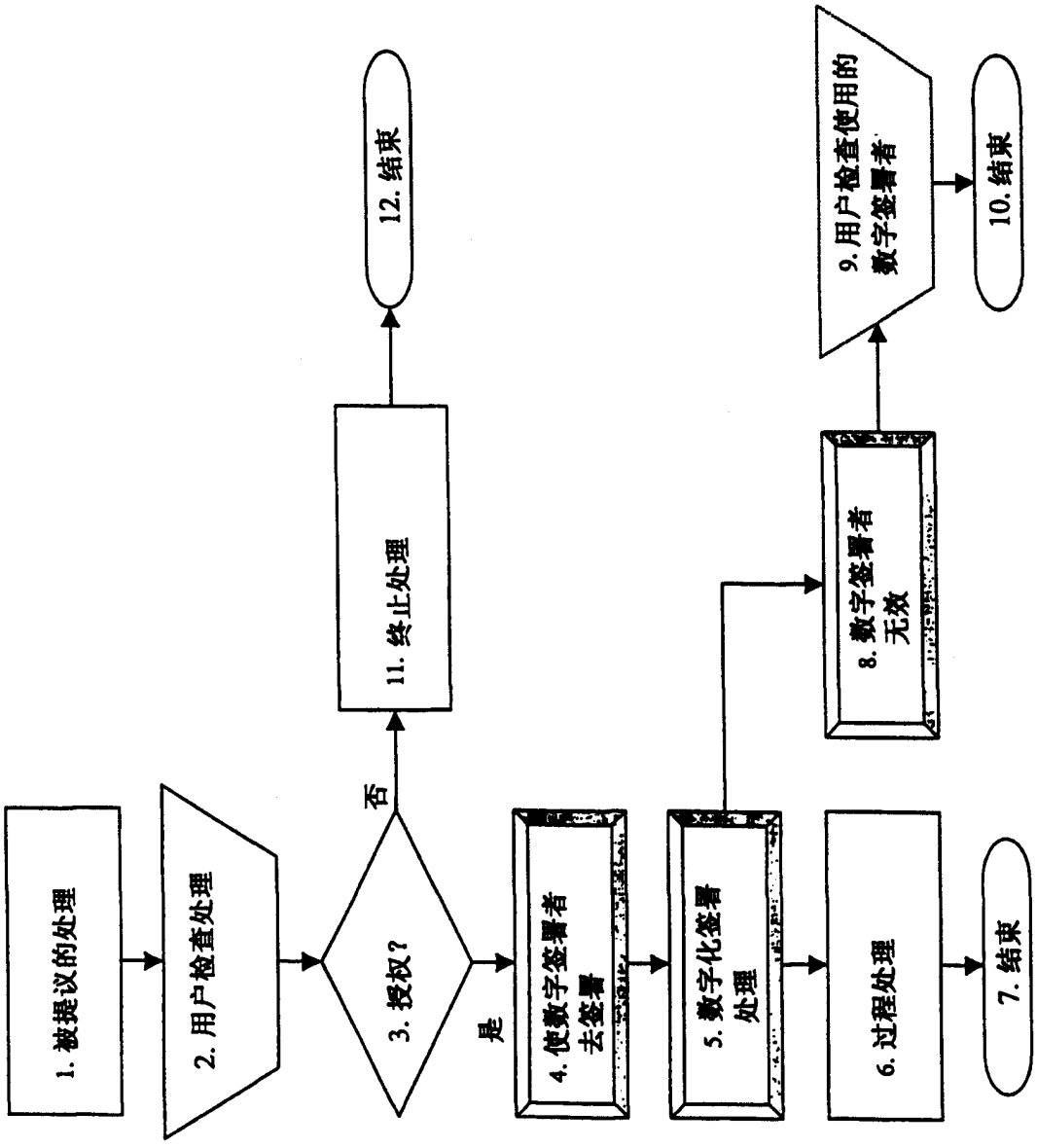
[0042]在大纲中显示的或在图中块指定的个体组件，在电子工艺和它们的具体设计中都是众所周知的，并且，对该工作或执行本发明的最佳模式来说，操作并不是至关重要的。

[0043]尽管本发明已经由最佳实施例进行了描述，但可以理解本发明不限于所披露的实施例。相反，本发明倾向于覆盖包括在权利要求中的精神和范围之内的不同的修改和等效的设备。随后的权利要求的范围将给予最广泛的解释，以便包含所有这样的修改和等效的设备以及功能。


130
委托
处理
物理合同
物理签名
100
120


230
事主
处理
201
210
215
数字合同
数字签名
数字合同2
数字签名
221
200
220
无效合同
数字签名
222
202


330
事主
处理
310
315
312
数字合同
数字签名
300
320


1. 被提议的处理
2. 用户检查处理
3. 授权?
否
是
11. 终止处理
12. 结束
4. 使数字签署者去签署
5. 数字化签署处理
8. 数字签署者无效
9. 用户检查使用的数字签署者
10. 结束
6. 过程处理
7. 结束