[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 1/00
G07F 7/10

[12] 发明专利申请公开说明书

[21] 申请号 01810390.1

[43] 公开日 2003 年 7 月 23 日

[11] 公开号 CN 1432148A

[22] 申请日 2001.5.17 [21] 申请号 01810390.1
[30] 优先权
[32] 2000. 5.31 [33] FR [31] 00/07041
[86] 国际申请 PCT/FR01/01522 2001.5.17
[87] 国际公布 WO01/92996 法 2001.12.6
[85] 进入国家阶段日期 2002.11.29
[71] 申请人 格姆普拉斯公司
地址 法国热姆诺
[72] 发明人 P·吉拉尔 J·-L·吉罗

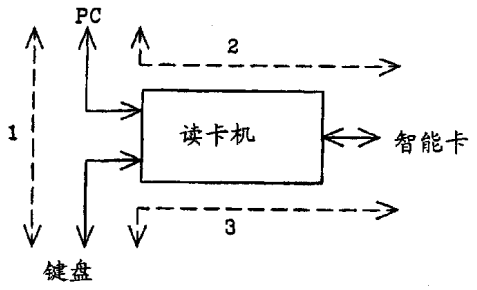
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 张志醒

权利要求书 2 页 说明书 13 页 附图 4 页

[54] 发明名称 防止欺骗性修改发送给安全电子媒体的数据的方法

[57] 摘要

本发明涉及一种用于防止对用户经读卡机发送给安全媒体的数据进行修改的方法。该方法的特征是，它包括对数据的某些部分进行选择和存储，并通过验证这些选定数据是否与用户按请求在该卡机的安全通信模式下输入的数据相符，来获得该选定数据的真实性验证。本发明的方法适用于防止对利用电子签名来签署的命令和/或文件的修改。



ISSN1008-4274

1．一种用于防止对由用户经读卡机发送给安全媒体的数据进行修改的方法，其特征在于，它包括选择和存储一定的数据项，并通过验证这些数据与用户在读卡机的安全通信模式下按请求输入的数据相同来确认这些数据项的真实性。

2．一种依照权利要求1的防止方法，其特征在于，数据为一条命令。

3．一种依照权利要求2的防止方法，其特征在于，该命令为一个密钥产生命令。

4．一种依照权利要求1的防止方法，其特征在于，该数据为一个利用由安全媒体产生的电子签名来签署的文件。

5．一种依照权利要求4的防止方法，其特征在于，它包括选择和存储要签署的文件中的一定的单词，和通过验证这些选定单词与用户在读卡机的安全通信模式下按请求输入的单词相同来确认该文件的真实性。

6．一种依照权利要求5的防止方法，其特征在于，选定用于验证的单词是由用户在安全通信模式下选取的。

7．一种依照权利要求5－6之一的防止方法，其特征在于，选定用于确认的单词是由安全媒体来选取的。

8．一种依照权利要求7的防止方法，其特征在于，由安全媒体选取的单词是被随机选择的。

9．一种依照权利要求7的防止方法，其特征在于，由安全媒体选取的单词是被确定性地选择的，要签署的文件为一种结构化的文件。

10．一种依照权利要求9的防止方法，其特征在于安全媒体按照编号来选择确认单词。

11．一种依照权利要求4－10中任何一种的防止方法，其特征在于，它还包括请求确认所选定用于确认的单词在文件中的位置。

12．一种依照权利要求11的防止方法，其特征在于，选定单词的位置是由要签署的文件的行号和列号限定。

13．一种依照权利要求12的防止方法，其特征在于，安全媒体选择要签署的文件的一个整列和/或整行作为确认单词。

14．一种依照权利要求4－13中任意一个要求的防止方法，其特

征在于，要签署的文件为 ASCII 格式。

15. 一种能够利用在媒体与读卡机之间有安全通信模式的读卡机与安全媒体进行通信的终端，该安全模式不让任何信息通过该终端，其特征在于，它具有一种能够实现下列步骤的程序：

－向安全媒体发送数据；

－请求输入验证数据；

－在一种安全模式中将验证数据发送给安全媒体。

16. 一种依照权利要求 15 的终端，其特征在于，它包括至少一个功能键或一系列功能键用来激活该安全模式。

17. 一种依照权利要求 15－16 之一的终端，其特征在于，它还包括具有与该终端安全通信模式的小型扫描仪。

18. 一种依照权利要求 15－17 之一的终端，其特征在于，它由一部移动电话（GSM）构成。

19. 一种依照权利要求 15－17 之一的终端，其特征在于，它由一台个人计算机构成。

20. 一种依照权利要求 15－17 之一的终端，其特征在于，它由配有一个集成键盘和屏幕的智能卡构成。

21. 一种依照权利要求 15－17 之一的终端，其特征在于，它由个人数字助理（PDA）构成。

22. 一种依照权利要求 15－21 之一的终端，其特征在于，该安全媒体由智能卡构成。

23. 一种依照权利要求 15－21 之一的终端，其特征在于，该安全媒体是由 PCMCIA 卡构成。

24. 一种智能卡，它能够经过具有安全通信模式的读卡机与终端进行通信，其特征在于，它有能够实现下列步骤的程序：

－选择和存储在非安全通信模式下从终端接收到的数据；

－请求对该数据进行确认；

－将存储的数据与验证过程中在安全通信模式下从该终端接收到的数据进行比较。

防止欺骗性修改发送给安全电子媒体的数据的方法

本发明涉及一种方法，其用于防止欺骗性修改由用户发送给电子媒体（如智能卡）的数据。这样的数据可以由命令和/或信息连同用于鉴别其真实性的电子签名构成。从上下文可以看出本发明适用于安全媒体通过读卡机连接到PC机（指家用个人计算机）的场合。

随着电子商务的发展，无论是公司对公司，还是公司对个人，都需要实现一种法律框架，使任何争端能够在进法庭之前解决。这一法律框架正在开始付诸实施，无论在欧洲还是美国，都是以识别电子签名作为证明手段。

在这些情况下，考虑实现用来产生可靠的电子签名的技术设施是很重要的，也就是说要尽可能地使这些设施无可争议。通常，采用公共密钥加密技术，可以对数字文件产生数字签名。通常大量采用的密码算法，如DSA，Schnorr或El Gamal，都是在产生电子签名的方法中使用一种散列函数。这样的一种伪随机函数包括将要签署的初始文本转化为一种散列文本，这种文本打破签名产生过程的线性特性。

产生电子签名的算法通常是采用硬件和软件来安装的，一般为提供软件和公共密钥的一台PC机，和一种包含用户密钥和加密签名算法的保密媒体。

根据实际应用，保密媒体可以是一个智能卡或一个PCMCIA卡等。大多数便携PC机都配有PCMCIA集成读卡机。某些这种PCMCIA格式的智能卡甚至可以是智能卡读卡机。

接着假定电子签名是由一种需要使用识别码（PIN码）的智能卡产生的，并且读卡机是一种非常简单的既没有键盘也没有屏幕的GemPC420型连接器。这是因为具有输入/输出（GCR500型）的读卡机要昂贵得多，由于这种读卡机是独立的，很少用来连接到PC机上，但是如果使用这种读卡机，会便于本发明的实现。

通常情况下，认为一种产生电子签名的方法必须产生具有下列特征的签名：

－可靠性：一个有效的签名是签署该签名的关联文件的用户的审慎意愿。因此，签名协议必须保证用户主动且单独参与。从而需要在

签署之前对该用户进行鉴定。在一种使用智能卡的系统中，两个因素保证了用户的主动到场：提供只有他拥有的物质因素（卡）和输入只有他自己才知道的数据（一个PIN码或一个口令）。

－不可伪造性：只有用户才能产生给定文件的签名。这一特性是通过采用公认的安全加密算法和一个可靠的公共密钥基础结构，以及采用抵抗物理和逻辑攻击的存储密钥的设施（如智能卡）来保证的。

－不可重复使用性：与一个文件相关联的签名不能被重复使用和与另一个文件相关联，就是说，必须能够检测出任何与该签名相关的信息的修改。这一特性是通过采用一种已知的使用一种散列函数和算法方法来保证的，该方法通过访问在各个签名之间新生的随机数来产生随机数字签名。

－不可否认性：文件的用户不能在签署了一个文件之后否认他已经慎重签署了该文件。这一特性取决于系统的整体安全性，因此仅当系统遭受攻击的可能性微乎其微时情况如此。相反，用户可以通过以系统的薄弱为理由否认其签名。必须注意，在该方面，必须考虑甲方的攻击。

这是因为用户可能有意在系统中加入一个漏洞，以便在过后能够否认签名。例如，如果由用户自己来产生其公共密钥，他可以有意选择一个薄弱的密钥，而随后声称他随意选择的被证明是一个薄弱的并已被破解的密钥。

通常认为采用PC机和智能卡的系统是充分可靠的，保证产生的签名是不可否认的。但是，，近期出现了利用特洛伊木马病毒来进行的攻击，对这一观点提出合理的质疑。

特洛伊木马病毒是一种恶意的代码段，它将自身隐藏在执行平常任务的程序中。

由于用户缺乏警惕性，当前用在家用PC机上的操作系统意味着很容易将包含一个特洛伊木马病毒的程序引入PC机，而且一旦就位，特洛伊木马病毒就拥有所有的权限。这样，例如，特洛伊木马病毒可以隐藏在流行的自由获得的程序中，或者在因特网上的共享软件中，如屏幕保护程序。还有类属的特洛伊木马病毒，如“Back Orifice”，它可以控制整个过程PC机，并修改其全部内容或某些内容，或者在网络程序（如因特网探测器）中开发出一种错误（bug）的特洛伊木马病

毒。

通过特洛伊木马可以实现多种攻击，但要考虑的是三种主要的攻击:

－窃取用户的 PIN 码: PIN（个人身份识别码）码设定一种允许鉴别持卡者的身份的认证值。

在操作系统中、应用软件包中、读卡机驱动程序中或用于智能卡的特定驱动程序中，安装在某处的特洛伊木马病毒随时可以复制用户输入的 PIN 码并将其传给特洛伊木马始发者。随后，该始发者从合法拥有者那里窃取智能卡，并在其不知情的情况下使用。

－修改由用户为智能卡设定并发送的命令。

例如，这种攻击可能在由 PC 机请求产生一个卡载密钥时进行。特洛伊木马病毒可以截获这一命令，自身产生一个密钥，用该密钥来自做此卡并发送一份拷贝。很明显，在这种情况下，就失掉了电子签名相关的特性，因为智能卡的拥有者不再是唯一能够产生可靠签名的人。

－在用户查看和利用智能卡签署之间对要签署文件的修改。

当用户为了签署其认可而输入其 PIN 码时，应用软件将要签署的文件传送到卡上，在签署之前该智能卡对文件进行散列处理（这里涉及的是一种要签署的数据量与智能卡的处理能力不兼容的情况）。

但是，一个特洛伊木马病毒能够截获向智能卡传送的数据，并对其进行修改。而后用户将签署一个他不仅没有认可，而且从没有见过的文件。这种情况显然是不能接受的。那么，很显然，随着电子商务和电子签名变得越来越广泛，这种攻击可以被用作反驳签名的一个理由。

当前，在诸如 GemPC420 的集成现代智能卡读卡机的系统中，对窃取 PIN 码的特定问题进行了考虑和控制。这样，图 1 中显示的这种读卡机具有特殊的机构，通常称作“委托通道”或计算机安全性的可靠通道，用来避免特洛伊木马病毒对 PIN 码的窃取。

图 1 显示了 GemPC420 的运行原理。该机位于 PC 机和键盘之间。因此能中断键盘和 PC 机间的所有通信。读卡机具有三个运行模式，对应于 PC 机、键盘和智能卡读卡机之间的三个通信电路。图 1 中，这些电路编号为 1、2 和 3。

电路 1 对应于一个没有使用智能卡和 PC 机与键盘对话的运行模式。电路 2 对应于 PC 机借助于 APDU（应用协议数据单元）与智能卡对话的模式，APDU 是由 ISO 标准定义的，用来标准化读卡机和智能卡之间的交换。最后，电路 3 对应于委托通道：读卡机切断 PC 机和键盘之间的通信，用户的按键由读卡机直接送到智能卡。读卡机依照 PC 机的指示进入模式 3，然后，利用用户按键码由 PC 机完成将 APDU 发送给智能卡的操作。

为了更安全和容易使用，读卡机上的一个发光二极管（LED）闪烁，表示读卡机正处于模式 3，并且仅在这种情况下闪烁。

这样，特洛伊木马病毒就不能截获用户的 PIN 码，因为 PIN 码不是任何时候都通过 PC 机。仅当读卡机处在由闪烁发光二极管表示的委托通道模式时，用户才必须输入其 PIN 码。这是因为特洛伊木马病毒可以在屏幕上显示一个消息，要求用户输入其 PIN 码，尽管如此，并没有将读卡机切换到委托通道模式。在这种情况下，读卡机不会切断键盘到读卡机的通信，使特洛伊木马病毒获取 PIN 码。

总之，显然 GemPC420 读卡机解决了特洛伊木马窃取 PIN 码的问题。其它读卡机也可以采用其它技术，来达到同样效果。

可以利用在装配有 USB（通用串行总线）键盘的计算机（如苹果计算机）上使用 USB 通信协议的读卡机。该原理与前面描述的原理非常类似：读卡机具有两个 USB 接口。第一个接口连接到计算机的一个 USB 端口，第二个接口用于连接键盘。在通常情况下，读卡机传送键盘和计算机之间交换的信息。当读卡机在其通道上接受到一个隔离命令时，它切断键盘和 PC 间的连接。随后在键盘上打印的信息不是被送到计算机，而是直接由读卡机使用。因此，以这种方式输入的 PIN 码从未输入到 PC 机，这样就不会出现成为特洛伊木马病毒的攻击对象的危险。

在本文的其余部分中，起初的原理是：解决方案采用 GemPC420 读卡机，但显然还可以采用任何其它具有委托通道的读卡机，如可以用刚刚描述的 USB 读卡机。

除了窃取 PIN 码的问题之外，还有对命令和／或要签署的文件的修改的问题需要解决。

此时，例如出现在读卡机驱动程序中的特洛伊木马病毒可以在用

户接受后修改发送给智能卡的签署文件。例如，特洛伊木马病毒可能将文件“I the undersigned X acknoledge that I owe FF10 to Y”改变为“I the undersigned X acknoledge that I owe FF10000 to Y”。

特洛伊木马病毒还可能修改一条命令，如通过其自身产生一个密钥，它保存该密钥的拷贝，并向智能卡发送存储该密钥的指示，而不是向智能卡发送产生一个卡载密钥的命令。

本发明的目的是对此问题进行补救，提出一种新的解决此类攻击的方案。

为此，本发明提出一种方法，该方法是利用一种包括连接到配有特定软件的计算机的智能卡的系统来实现的。智能卡选择和存储一定数量的用户发送数据项，并要求在不经过PC机的安全通信模式中，核实该数据项的真实性。

为此，智能卡要求用户在键盘上输入所有或部分要发出的命令或从要签署的初始文本中选择的单词，然后，验证它们确实与开始接收到的相同。

依照本发明的方法主要包括确认在继续执行命令和／或产生文件的电子签名之前，没有发生旨在修改该命令和／或要签署的文件的攻击。

本发明的目的是产生一种用来防止对用户通过读卡机发送给安全媒体的数据进行修改的更特殊的一种方法，其特征在于，它包括选择和存储一定的数据项，并通过确认这些数据项是否与用户在读卡机的安全模式中根据要求输入的数据相同，来获得该选定数据项的真实性验证。

依照本发明的方法的第一个应用，数据为一种命令。

依照派生的结果，该命令为密钥产生命令。

依照本发明的方法的第二个应用，数据为利用一种安全媒体产生的电子签名来签署的文件。

依照本发明的一个特征，该方法包括选择和存储要签署的文件中一定的单词，并通过验证这些选择的单词确与用户在读卡机的安全通信模式下按要求输入的单词相同来确认该文件的真实性。

依照本发明的一个特征，为验证选择的单词是用户在一个安全通

信模式下选择的。

依照本发明的另一个特征，为验证选择的单词是由安全媒体来选择的。

依照本发明的一个特征，由安全媒体选择的单词是随机选定的。

依照本发明的另一个特征，由安全媒体选择的单词是确定性选择的，要签署的文件为一个结构化文件。

依照一种派生的实现方法，安全媒体按编号选择用于验证的单词。

依照一种派生的实现方法，该方法还包括要求核实用于验证所选定单词在文件中的位置。

依照本发明的一个特征，选定单词的位置是由要签署的文件的行号和列号来定义的。

依照一种派生的实现方法，安全媒体选择要签署的文件的一整列和/或一整行作为验证单词。

依照本发明的一个特征，要签署的文件为 ASCII 格式。

本发明还涉及一种能够借助于在媒体和读卡机之间有安全通信模式的读卡机与该安全媒体进行通信的终端，该安全模式不让任何信息通过终端，该终端具有能够实现下列步骤的程序：

- 向安全媒体发送数据；
- 要求输入验证数据；
- 在一种安全通信模式下，将该验证数据发送给安全媒体；

依照本发明的一个特征，该终端包括保留至少一个功能密钥或一系列功能密钥，用来激活安全模式。

依照本发明的一个特征，该终端还包括与终端有安全通信模式的微型扫描器。

依照一种应用，该终端由一种移动电话（GSM）构成。

依照另一种应用，该终端由个人计算机构成。

依照另一种应用，该终端由配有集成屏幕和键盘的智能卡构成。

依照另一种应用，该终端由个人数字助理（PDA）构成。

依照一种应用，安全媒体由智能卡构成。

依照另一种应用，安全媒体由 PCMCIA 卡构成。

本发明还涉及能够通过具有安全通信模式的读卡机与终端进行通

信的智能卡，其特征在于具有能够实现下列步骤的程序：

- 选择和存储在非安全通信模式下从终端接收的数据；

- 要求对该数据进行验证；

- 将存储的数据与验证步骤中在安全通信模式下从终端接收的数据进行比较。

本发明提供了一种有效的方案，来解决特洛伊木马病毒对用智能卡签署的命令或文件进行修改问题。对这种方法可能产生的批评是对于用户来讲它缺少人机控制，但是很少可以无约束地增加安全性，而且，可以随意地调节安全性/人机控制的比值。

下面结合附图，通过说明性的和非限定性的例子对本发明进行描述，通过阅读这些描述可以清楚地了解本发明的特性和优势，附图中：

- 图 1 是已经描述过的 GemPC420 智能卡读卡机的示意图；

- 图 2 显示了一个要签署的结构化文本的例子。

- 图 3 显示了一个要发送的按行和列组织的文本的例子。

- 图 4 是实现依照本发明的用于通过一台 GemPC420 读卡机签署文件的方法的流程图。

- 图 5 是实现依照本发明的利用读卡机或具有集成键盘和屏幕的智能卡来签署文件的方法的流程图。

- 图 6 是实现依照本发明的用于通过一台 GemPC420 读卡机产生命令的方法的流程图。

- 图 7 是实现依照本发明的利用读卡机或具有集成键盘和屏幕产生命令的方法的流程图。

首先描述的是依照本发明的方法在防止对要签署的文件的修改方面的应用。

如果仍采用前面文本的例子“I the undersigned X certify that I own 10 frances to Y”，并且如果特洛伊木马病毒通过攻击将“10”改为“1000”，则依照本发明的方法必须能显示出这一修改。

为此，选择词“10”来进行验证。随后，智能卡要求应用程序加亮（例如用红色或粗体）由用户输入要进行验证的词，并显示“请输入高亮的词来进行验证”类型的消息。从卡上接收到词“1000”的特洛伊木马病毒在要输入“10”的用户的屏幕上将显示的文本中词“10”加亮。如果这一输入是在常规模式下进行的（GemPC420 的模式 1），

则特洛伊木马将有机会用1000来替换用户输入的密钥，而智能卡将成功地进行1000与1000之间的比较。如果输入使用了读卡机的安全设施（GemPC420的模式3），则特洛伊木马将不能修改用户键入的密钥，智能卡将比较10和1000，由此检查出对文件的修改。

因而，很显然本发明提出的解决方案不是一定能检查出攻击的。在前面的例子中，如果智能卡选择没有被特洛伊木马修改的文件的词来进行验证(如“undersigned”)，那么它将不能检测到攻击而签署已被修改的文件。因此，重要的是，要以这样的方式来实现本发明的解决方案，即便是可能出现的攻击，要使其成功的可能性减小到可忽略不计。

很显然，用于验证的词及其数目的选择是至关重要的。

关于要验证的词的数量，主要是考虑在希望的安全度和输入校验所引起的不便之间折中。当用户重新键入要签署的文件的全部文本时，安全性是最高的。实际上，验证词的数量取决于所希望的安全度和从应用的角度看要保护的对象。

对于要验证的词的选择，必须要有若干限制。一方面，由用户和/或卡来选择要验证的词，另一方面，这些词要是随机和/或确定性选择的。

而且，有必要对验证词的选择进行初步的评价。因为到目前为止，一直认为要签署的文件是以智能卡可理解的格式的文本，其单词可以直接与键盘输入相比较。

ASCII格式的文本很容易满足这些规范。一种专用格式的文件如微软字处理软件（Microsoft word）是不能直接使用的。另一方面，完全可能输出要签署的微软字处理软件文件的ASCII版本。这一版本必须由用户察看，因为它将形成竞争一项交易或合同时的参考资料。一种中间的解决方法可以包括使用多功能文本格式RTF（Rich-Text Format），可以将描述性属性(粗体，下划线)加入文本，而保留ASCII码。价格上的投入是一部卡载多功能文本分析仪。

实际上，本发明可以用于任何文本格式，但是应当注意某些格式比其它格式更实用。例如，与一种在键盘的触摸板（触摸屏）或图形板装置上的输入相比，可以构想（即使实现的技术较困难）“位图”格式（例如通过数字化纸张文件获得）。这样的装置允许例如图形签

字，为此用户将不再用验证单词，而是验证复制的图形的某些部分。

此后，认为所用的是ASCII格式的文本。

在下面的描述中，参考图2和3，考虑一个要签署的例子文本，其文如下："I the undersigned Pierre Girard certify that I owe the sum of ninety fraces to Mr Jean-Luc Giraud. Effected 31 January 2000 in Gemenos"。

实现依照本发明的方法的第一个重点是要确定是否由智能卡和/或用户来选择要验证的单词。

由于由智能卡选择的要验证的词可能落在一个合同或文件的无关紧要的术语上（如上述例子中的"unsigned"），可以认为用户是最能够指定文本中的重要术语的。他可以在读卡机的模式3中向智能卡表示在该智能卡接收文件之前他希望对哪些词进行验证。当智能卡接受文件并请求验证时，用户在读卡机的模式3中验证计划好的单词。

然而，这一方法不能防御甲方对系统的攻击，用户可能要求智能卡对文件中的无关紧要的单词进行验证（本例中的"unsigned"），而后通过声称已经被特洛伊木马的攻击来否认其签名。

为了获得最高级的安全性最好是做这样的协调，即用户所选用的验证单词（防御特洛伊木马攻击）与智能卡所选择的单词（防御甲方攻击）是相同的。

实现依照本发明的方法的第二个重点是要确定是随机地还是确定地选择要验证的单词。

当用户选择要验证的词时，他的行为是事先不可预知的行为，他将使用他的常识，来选择文件的主要单词。因此，特洛伊木马成功实施攻击的机会很小。

对于由读卡机来选择要验证的单词，可以在随机策略或确定性选择算法之间不断变动。根据其定义，随机策略是特洛伊木马不可预知的。但是，如果在文件中无关紧要的单词数量和验证单词的数量之间的比例很大，那么随机选择单词的智能卡将很少有机会落在特洛伊木马和甲方攻击的潜在目标的单词上。

为了避免这一问题，智能卡可能试图确定文件的重要单词。例如，可能会立刻想到所有的总额和日期。但是，按照现在的情况，这样的一个算法实现起来相当困难。

为了便于由智能卡判读文本和选择相关的验证单词，如在 XML（扩展的 Mark-up 语言）中，可以方便地将结构化文本传送给智能卡，智能卡需要有相应的卡载分析仪。图 2 说明了一个这样的结构化文本。这样，智能卡可以选择诸如日期或总额之类的重要单元来进行验证。

也可以设想标准文本“with holes”，其中仅需填写如姓名信息、日期和数量等。

最后，应当注意，智能卡可以有一个混合的策略，用随机选择的单词补充其确定选择。

除了选择和要验证的单词数量之外，精确指定单词也是很重要的。

这是因为在文件中确定数量单词存在的验证显然不足以确定其含义。还必须保证遵循单词的顺序。例如，确认在单词“of”和“ninety”之间没有加入“One hundred and”是很重要的。因此，精确指定单词“of”和“ninety”各自的位置将是很重要的。

为此，如图 3 所示可以采用按行和列组织的文本，以便精确指定要验证的单词的位置。

在输入验证单词时，智能卡可以要求用户输入第二行的第 5－8 号单词和第 3 行的第一个单词。随后，用户将输入要求的单词及其在文本中的位置。一种表示惯例是“12w6 of”，确认单词“of”是在第二行的第六个位置。

为了避免删除、插入和移动单词，一种可能采用的策略包括要求验证文本的列数。在本例中，如果智能卡要求验证第 14 列，则用户将输入“c14 g e i a”。

在下面的完整的例子中，参考图 4 的流程图概述了依照本发明的该方法的实现。

该方法是利用存储在 PC 机上的能够借助于 GemPC420 读卡机与智能卡进行通信的适当软件来实现的。

1. 软件在用户的屏幕上显示要签署的文件（仍用图 2 和 3 中的例子）。

2. 软件切换 GemPC420 到模式 3。用户核实绿色发光二极管在闪烁。

3. 用户向智能卡指出他希望通过输入“12w5-8 sum of ninety

france13w1 Mr”来输入进行验证的单词。

4. 该软件将 GemPC420 切换到模式 2，然后将要签署的文件传送给智能卡。如果要签署的文件的量很大，智能卡可能在浮动中将其进行散列处理，同时进行下面的两个步骤。

5. 智能卡核实用户的输入与接收到的文本是一致的，否则中止协议（这样可以避免特洛伊木马的攻击）。

6. 智能卡选择用户必须输入进行验证的单词。例如，智能卡选择日期，然后随机选择第 17 列和单词“Pierre”。智能卡将该选择发送给软件。

7. 软件将这些要验证的词变成红色和高亮度，并将 GemPC420 切换到模式 3。用户确认绿色的发光二极管在闪烁。

8. 用户输入智能卡所要求的验证数据：“14w2-4 31 January 2000 c17 duua 11w4 Pierre”。

9. 智能卡确认验证数据与接收到的文件相一致，否则中断协议（这样可以避免特洛伊木马和/或甲方的攻击）。

10. 软件要求用户输入其 PIN 码，以便证实他希望签署文件（此时 GemPC420 正处于模式 3）。用户确认绿色发光二极管在闪烁。

11. 用户输入其 PIN 码。

12. 智能卡确认该 PIN 码，如果是正确的，则签署文件并将签名返回给软件。

在采用读卡机或具有集成屏幕和键盘的智能卡的场合，参考图 5 的流程图，签署过程可以简化如下：

1. 软件在用户的屏幕上显示要签署的文件（仍用图 2 和 3 中的例子）。

2. 用户指出他希望通过在读卡机（智能卡的）键盘上输入“12w5-8 13w1”来输入进行验证的单词。

3. 该软件将要签署的文件传送给智能卡。如果要签署的文件的量很大，智能卡可能在浮动中将其进行散列处理，同时进行下面的两个步骤。

4. 读卡机（智能卡）显示用户要求核实的单词“12w5-8 sum of ninety francs13w1 Mr”

5. 用户确认这些验证的单词确与他希望签署的文本一致，否则中

止协议（这样可以避免特洛伊木马的攻击）。

6. 智能卡选择用户必须输入进行验证的单词。例如，智能卡选择日期，然后随机选择第 17 列和单词“Pierre”。该选择被显示在读卡机或智能卡的屏幕上。

7. 用户在读卡机(智能卡的)的键盘上输入要验证的单词:“14w2-4 31 January 2000 c17 duua 11w4 Pierre”。

8. 智能卡确认验证数据与接收到的文件相一致，否则中断协议(这样可以避免特洛伊木马和/或甲方的攻击）。

9. 软件要求用户输入其 PIN 码，以便证实他希望签署文件。

10. 用户输入其 PIN 码。

11. 智能卡确认该 PIN 码，如果是正确的，则签署文件并将签名返回给软件。

依照本发明的该方法也可以在 GSM 类型的终端（移动电话）或 PDA（个人数字助理）上实现，假定后者具有至少一个功能键或一系列的功能键用来激活安全模式，和可以用来确认安全模式是否被激活的输出。

可以设想多种可能的方式来实现依照本发明的方法。

第一种方式包括产生本发明提出的系统（能够控制读卡机和向用户提供指示的用来实现依照本发明的方法的软件）和可扩展的 Word 或 Excel 等软件包之间的接口。在这种环境中，需用 Visual Basic 编制一个与签名 API（应用程序接口）的接口和用于加亮要在文本中重新输入的单词的功能函数。

通过利用 Java 程序将用于实现本发明的软件集成到 Web 页中，可以获得该系统的另一个可能的实现方式。

此外，依照本发明方法的一个缺陷是需要用户费事地输入一定的单词，这与接口技术朝着用户友善性发展的趋势是背道而驰的。该问题的一种解决方法是可以在实现本发明的系统上增加一个安全的小型扫描仪，它与读卡机连接到相同的通信端口，或直接设置到读卡机上。在读卡机和小型扫描仪连接在相同的端口的情况下，读卡机当然地配置在 PC 机和小型扫描仪之间，如同 GemPC420 的键盘一样。该小型扫描仪允许用户输入显示在屏幕上或打印的词，为他保存一个新的输入。

依照本发明的该防止方法还可以用于解决由特洛伊木马修改发送给智能卡的命令的问题。

为此，本发明提出一种用来防止对发送给安全媒体（所研究的例子中为智能卡）的命令修改的方法。该方法实现的步骤与关于防止对签署的文件的修改所描述的步骤相同。

接收到命令后，例如卡上密钥产生命令，智能卡将要求用户核实这一命令。

在安全媒体连接到 GemPC420 读卡机上时，该方法按照图 6 中的下列步骤进行:

1. 通过在 PC 机的屏幕上显示一条消息，请用户核实他的命令。

2. 软件将 GemPC420 切换到模式 3。用户确认绿色的发光二极管在闪烁。

3. 用户核实他的命令（如通过键入产生卡上密钥的命令 GENK）。

4. 智能卡将用户的输入与接收到的命令比较。如果比较得到不符的结果，则中止协议，否则智能卡执行该命令（产生密钥）。

在采用终端或具有集成屏幕和键盘的智能卡的场合，该方法依照图 7 所示的步骤进行。

1. 将智能卡接受到的命令显示在终端屏幕上。

2. 用户确认该命令就是他希望产生的命令，然后通过终端上的功能键进行确认，否则中止协议。

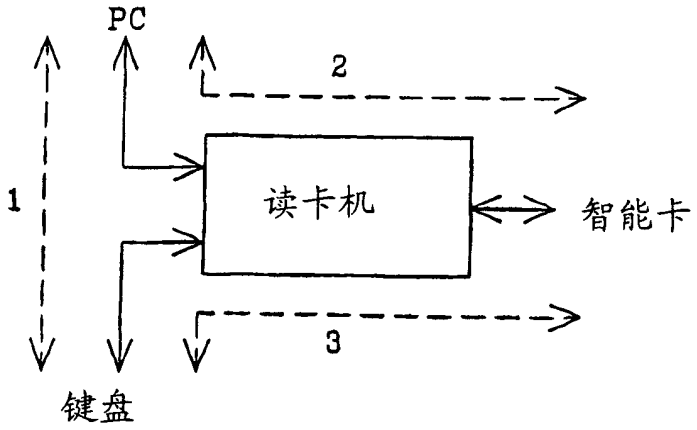


图 1

```
<contract>
I the undersigned <signer>Pierre Girard</signer> <object>certify
that I owe</object> the sum of <amount>ninety
<currency>francs</currency></amount> to <party>Mr Jean-Luc
Giraud</party>. Effected <date>31 January 2000</date>
<where>in
Gemenos</where>.
</contract>
```

图 2

```
          1111111111222222222233333333 3
1234567890123456789012345678901234 5
1 I the undersigned Pierre Girard certify
2 that I owe the sum of ninety francs to
3 Mr Jean-Luc Giraud.
4 Effected 31 January 2000 in Gemenos.
```

图 3

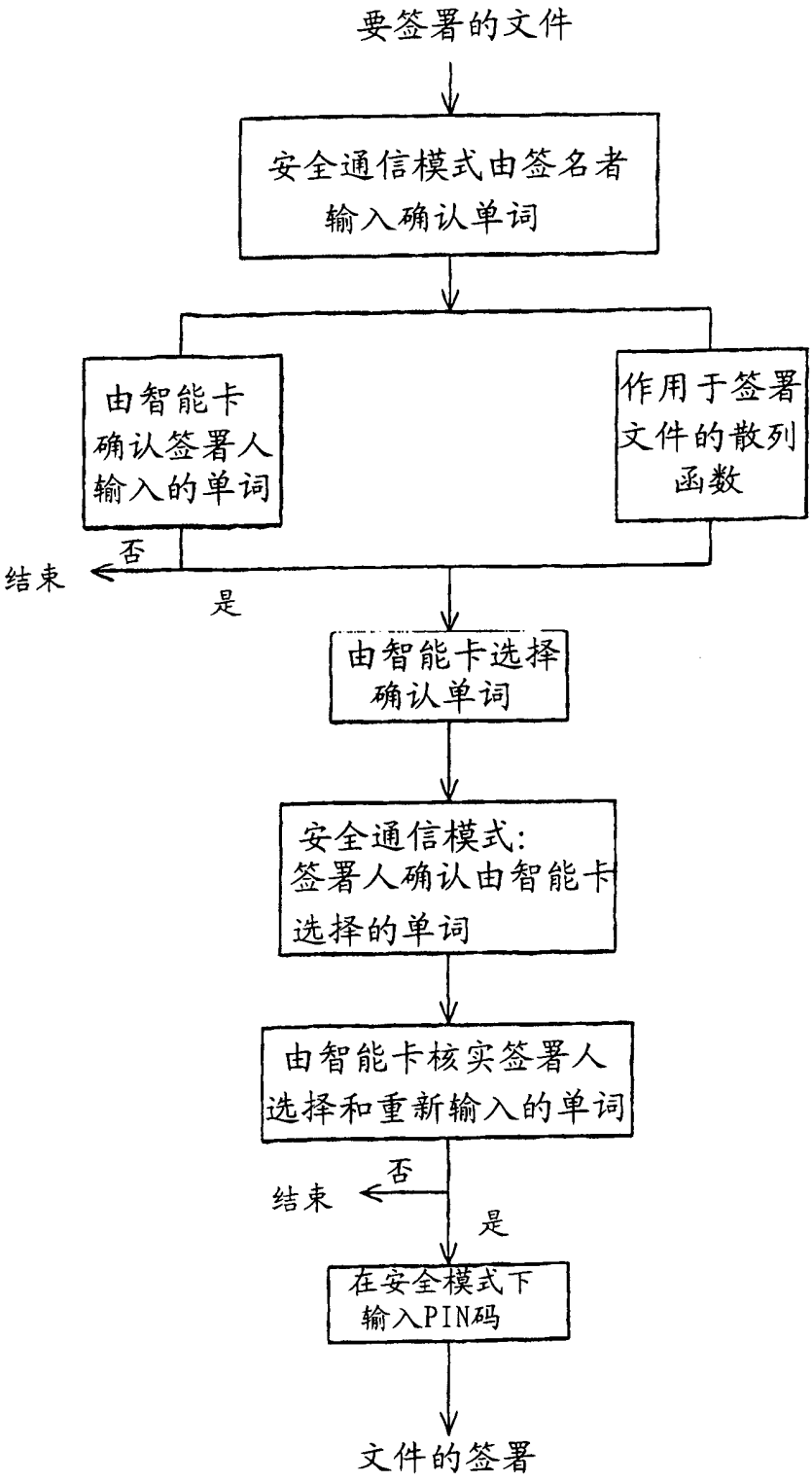

要签署的文件
安全通信模式由签名者输入确认单词
由智能卡确认签署人输入的单词
作用于签署文件的散列函数
否
结束
是
由智能卡选择确认单词
安全通信模式:签署人确认由智能卡选择的单词
由智能卡核实签署人选择和重新输入的单词
否
结束
是
在安全模式下输入PIN码
文件的签署

图 4

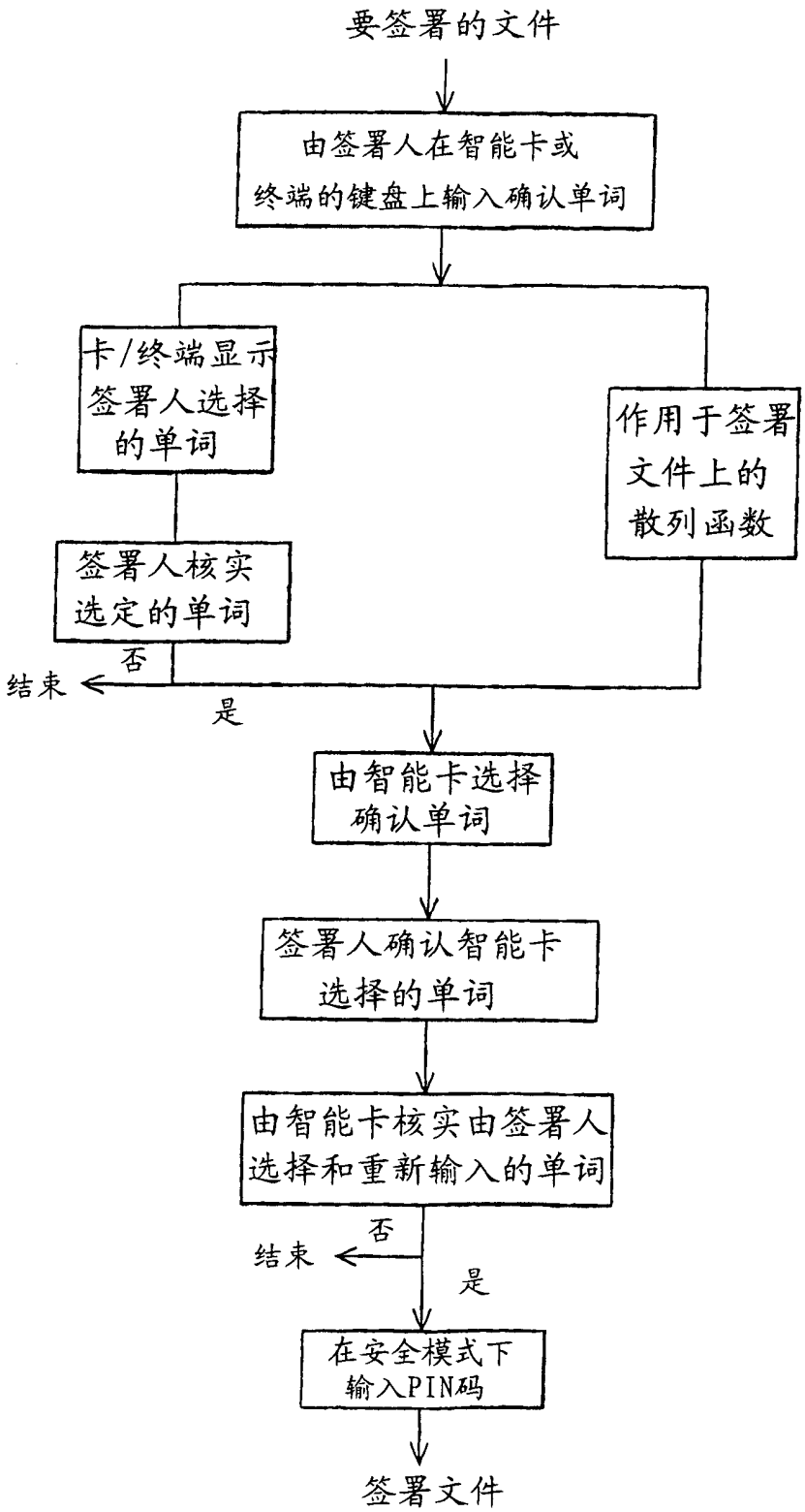

要签署的文件
由签署人在智能卡或终端的键盘上输入确认单词
卡/终端显示签署人选择的单词
作用于签署文件上的散列函数
签署人核实选定的单词
否
结束
是
由智能卡选择确认单词
签署人确认智能卡选择的单词
由智能卡核实由签署人选择和重新输入的单词
否
结束
是
在安全模式下输入PIN码
签署文件

图 5

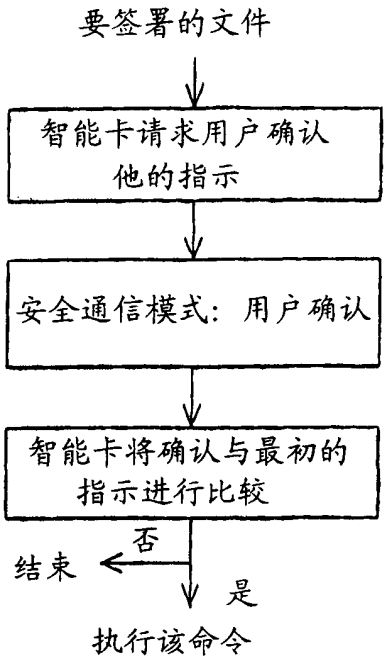

要签署的文件
智能卡请求用户确认他的指示
安全通信模式：用户确认
智能卡将确认与最初的指示进行比较
否
结束
是
执行该命令

图 6

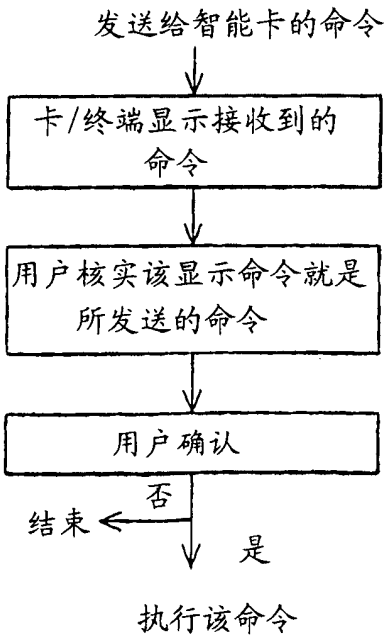

发送给智能卡的命令
卡/终端显示接收到的命令
用户核实该显示命令就是所发送的命令
用户确认
否
结束
是
执行该命令

图 7