

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200710063745.2

[51] Int. Cl.

G06Q 30/00 (2006.01)

H04L 9/32 (2006.01)

G06F 21/00 (2006.01)

[43] 公开日 2008 年 8 月 13 日

[11] 公开号 CN 101241572A

[22] 申请日 2007.2.8

[21] 申请号 200710063745.2

[71] 申请人 李东声

地址 100083 北京市海淀区清华东路 17 号金码大厦 B 座 1810

[72] 发明人 李东声

[74] 专利代理机构 北京凯特来知识产权代理有限公司

代理人 郑立明 姚巍

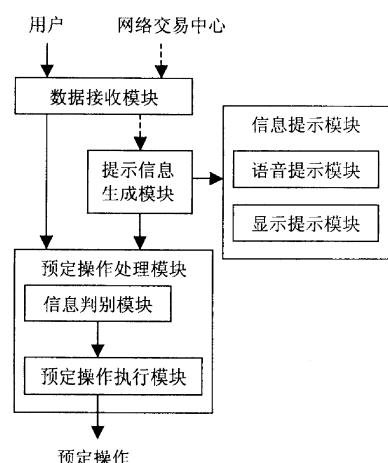
权利要求书 2 页 说明书 6 页 附图 1 页

[54] 发明名称

一种电子签名工具的操作方法及电子签名工具

[57] 摘要

本所述的一种电子签名工具的操作方法及电子签名工具，首先，电子签名工具输出验证提示信息给用户；再由电子签名工具接收用户输入的验证确认信息，并根据验证确认信息与验证提示信息确定是否进行预定操作（比如签名计算、加密计算等）。可以防止网络上其它用户的攻击，实现安全交易。且简单方便，便于普及。



1、一种电子签名工具的操作方法，其特征在于，在需要电子签名工具进行预定操作时包括，

- A、电子签名工具输出验证提示信息给用户；
- B、电子签名工具接收用户输入的验证确认信息，并根据验证确认信息与验证提示信息确定是否进行预定操作。

2、根据权利要求1所述的电子签名工具的操作方法，其特征在于，所述的步骤A包括，

A1、电子签名工具随机生成一组数据作为验证提示信息，提示给用户；或者，

A2、电子签名工具将网络交易中心发来的已经加密的鉴别码解密后作为验证提示信息，提示给用户。

3、根据权利要求1或2所述的电子签名工具的操作方法，其特征在于，所述的电子签名工具通过语音和/或屏幕显示的方式将验证提示信息提示给用户。

4、根据权利要求1所述的电子签名工具的操作方法，其特征在于，所述的步骤B包括，

电子签名工具接收用户输入的验证确认信息，并判断所述的验证确认信息与验证提示信息是否匹配，如是，进行预定操作，否则，拒绝预定操作。

5、根据权利要求4所述的电子签名工具的操作方法，其特征在于，判断所述的验证确认信息与验证提示信息是否匹配包括，

判断所述的验证确认信息与验证提示信息是否相同；或者，

判断所述的验证确认信息与验证提示信息是否符合预定的匹配条件。

6、根据权利要求1或4所述的电子签名工具的操作方法，其特征在于，

所述的预定操作包括，签名计算、加密计算、解密计算、签名校验、生成密钥对、公钥输出和/或密钥导入。

7、一种电子签名工具，其特征在于，包括，
数据接收模块，用于接收用户输入的验证确认信息；
提示信息生成模块，用于生成验证提示信息；
信息提示模块，用于输出验证提示信息给用户；
预定操作处理模块，用于根据验证确认信息与验证提示信息确定是否进行预定操作。

8、根据权利要求7所述的电子签名工具，其特征在于，所述的数据接收模块还用于接收网络交易中心发来的已经加密的鉴别码；且所述的提示信息生成模块将所述的鉴别码解密后作为验证提示信息，提示给用户。

9、根据权利要求7所述的电子签名工具，其特征在于，所述的提示信息生成模块用于在电子签名工具中生成验证提示信息。

10、根据权利要求7所述的电子签名工具，其特征在于，所述的信息提示模块包括，
语音提示模块，用于通过电子签名工具上的语音的方式输入验证提示信息，提示给用户；和/或，

显示提示模块，用于通过电子签名工具上的屏幕显示的方式输入验证提示信息，提示给用户。

11、根据权利要求7所述的电子签名工具，其特征在于，所述的预定操作处理模块包括，
信息判别模块，用于判断接收用户输入的验证确认信息与验证提示信息是否匹配，如是，进行预定操作，否则，拒绝预定操作；
预定操作执行模块，用于执行预定操作。

一种电子签名工具的操作方法及电子签名工具

技术领域

本发明涉及电子技术应用领域，尤其涉及一种电子签名工具的操作方法及电子签名工具。

背景技术

目前，许多用户需要通过网络传输各种数据或网上银行系统办理业务，随着电子证书（电子签名）的立法，在日常的应用实践中有许多用户使用电子签名工具（比如USBKEY等）。电子签名工具可以对数据进行加密、签名、认证，在网络数据传输、网络支付和网上交易时大大提高了安全性。

目前用户在使用个人电子签名工具的联网使用时，由于互联网不安全，存在用户的计算机被木马软件绑架的可能，这样攻击者（也就是黑客）就可以通过远程控制直接对个人电子签名工具进行操作，伪造交易。给用户造成一定的损失。

现有技术在网上交易应用中为了防止自动攻击，常会使用图形鉴别码的方式，也就是中心随机选择一组数字或字母，将含有这组数据的图形通过计算机给用户，让用户按照显示输入，比较正确性。但由于数字和字母数量有限，对应的图形的数量也有限，也可以使用图形穷举对比的方式来进行分析，或者直接将图片发送给远程的攻击者，让攻击者看图形输入对应的数据来进行破解。达不到安全交易的目的。

发明内容

鉴于上述问题，本发明的目的是提供一种电子签名工具的操作方法及电子签名工具，可以防止网络上其它用户的攻击，实现安全交易。且简单方便，便于普及。

本发明的目的是通过以下技术方案实现的：

一种电子签名工具的操作方法，在需要电子签名工具进行预定操作时包括，

A、电子签名工具输出验证提示信息给用户；

B、电子签名工具接收用户输入的验证确认信息，并根据验证确认信息与验证提示信息确定是否进行预定操作。

所述的步骤A包括，

A1、电子签名工具随机生成一组数据作为验证提示信息，提示给用户；或者，

A2、电子签名工具将网络交易中心发来的已经加密的鉴别码解密后作为验证提示信息，提示给用户。

所述的电子签名工具通过语音和/或屏幕显示的方式将验证提示信息提示给用户。

所述的步骤B包括，

电子签名工具接收用户输入的验证确认信息，并判断所述的验证确认信息与验证提示信息是否匹配，如是，进行预定操作，否则，拒绝预定操作。

所述的方法，判断所述的验证确认信息与验证提示信息是否匹配包括，

判断所述的验证确认信息与验证提示信息是否相同；或者，

判断所述的验证确认信息与验证提示信息是否符合预定的匹配条件。

所述的预定操作包括，签名计算、加密计算、解密计算、签名校验、生成密钥对、公钥输出和/或密钥导入。

一种电子签名工具，包括，
数据接收模块，用于接收用户输入的验证确认信息；
提示信息生成模块，用于生成验证提示信息；
信息提示模块，用于输出验证提示信息给用户；
预定操作处理模块，用于根据验证确认信息与验证提示信息确定是否进行预定操作。

所述的数据接收模块还用于接收网络交易中心发来的已经加密的鉴别码；且所述的提示信息生成模块将所述的鉴别码解密后作为验证提示信息，提示给用户。

所述的提示信息生成模块用于在电子签名工具中生成验证提示信息。

所述的信息提示模块包括，

语音提示模块，用于通过电子签名工具上的语音的方式输入验证提示信息，提示给用户；和/或，

显示提示模块，用于通过电子签名工具上的屏幕显示的方式输入验证提示信息，提示给用户。

所述的预定操作处理模块包括，

信息判别模块，用于判断接收用户输入的验证确认信息与验证提示信息是否匹配，如是，进行预定操作，否则，拒绝预定操作；

预定操作执行模块，用于执行预定操作。

由上述本发明提供的技术方案可以看出，本所述的一种电子签名工具的操作方法及电子签名工具，首先，电子签名工具输出验证提示信息给用户；再由电子签名工具接收用户输入的验证确认信息，并根据验证确认信息与验证提示信息确定是否进行关键操作。可以防止网络上其它用户的攻击，实现安全交易。且简单方便，便于普及。

附图说明

图1为本发明所述的电子签名工具的结构示意图。

具体实施方式

本发明所述的一种电子签名工具的操作方法，其具体实施方式是在需要电子签名工具进行预定操作时，包括以下过程：

首先，由电子签名工具输出验证提示信息给用户；所述的验证提示信息可以由电子签名工具内部生成，也可以由电子签名工具将网络交易中心发来的已经加密的鉴别码解密后得到。而电子签名工具输出验证提示信息和方式可以是通过电子签名工具上的语音提示方式将验证提示信息提示给用户，也可以是通过或电子签名工具上的屏幕显示的方式将验证提示信息提示给用户。

其次，电子签名工具接收用户输入的验证确认信息，并根据验证确认信息与验证提示信息确定是否进行预定操作。具体为电子签名工具接收用户输入的验证确认信息，并判断所述的验证确认信息与验证提示信息是否匹配，如是，进行预定操作，否则，拒绝预定操作。

这里的判断所述的验证确认信息与验证提示信息是否匹配包括，判断所述的验证确认信息与验证提示信息是否相同；或者，判断所述的验证确认信息与验证提示信息是否符合预定的匹配条件。

所述的匹配条件包括：

所述的验证确认信息与验证提示信息是否符合一定的加密/解密规则；或者，所述的验证确认信息与验证提示信息是否符合一定的算法，以数字为例验证确认信息与验证提示信息之间可以满足某一运算（如平方，倒序，倍数，相差某一值等）。

文中所述的预定操作包括，签名计算、加密计算、解密计算、签名校

验、生成密钥对、公钥输出和/或密钥导入。

前文中的用户输入的验证确认信息的方式包括，通过计算机键盘、鼠标输入后由计算机通过接口发送给电子签名工具；或者，

直接在电子签名工具上输入（电子签名工具具备直接输入功能）；或者通过电子签名工具和计算机配合输入。

本发明应用于具有提示功能（比如语音或者显示等等）的个人电子签名工具上，当用户需要进行某些预定操作（如关键操作的签名操作）时，个人电子签名工具内随机生成一组数据（数字或字母）作为验证提示信息，并通过提示功能将这串数据提示给用户。用户听到或者看到后，再通过计算机输入验证确认信，发送给个人电子签名工具，个人电子签名工具内部比较所述的验证确认信息与验证提示信息是否一致，相同才签名，进行后续操作，否则就拒绝执行签名操作。

另外，网络交易中心的图形鉴别码也是通过加密后发送给个人电子签名工具，个人电子签名工具在内部解密后得到验证提示信息，再提示给用户。

这样可以杜绝任何外界的攻击的可能性和可行性。

另外，本发明还提供了一种电子签名工具，如图1所示，包括，数据接收模块、提示信息生成模块、信息提示模块与预定操作处理模块，其中，

数据接收模块，用于接收用户输入的验证确认信息；还用于接收网络交易中心发来的已经加密的鉴别码（如图形鉴别码）；此时，所述的提示信息生成模块将所述的鉴别码解密后作为验证提示信息，提示给用户。

提示信息生成模块，用于生成验证提示信息；包括在电子签名工具中随机生成验证提示信息。

信息提示模块，用于输出验证提示信息给用户；包括语音提示模块与显示提示模块，其中，语音提示模块用于通过语音的方式输入验证提示信息，提示给用户，显示提示模块用于通过屏幕显示的方式输入验证提示信息，提

示给用户。语音提示模块与显示提示模块可同时使用也可分别单独使用。

预定操作处理模块，用于根据验证确认信息与验证提示信息确定是否进行预定操作。包括信息判别模块与签名执行模块，其中，信息判别模块用于判断接收用户输入的验证确认信息与验证提示信息是否匹配，如是，进行预定操作，否则，拒绝预定操作；预定操作执行模块用于执行预定操作。

综上所述，应用本发明方法与系统，它主要具有以下几种优点：

1、易于实现：只需对原有电子签名工具进行较小的改动；如加一信息提示模块，就可满足本发明的要求；

2、成本低：只需要对电子签名工具内的软件进行适当功能改进即可。例如，电子签名工具的软件需要具有判断接收用户输入的验证确认信息与验证提示信息是否相同的功能。

3、通用性强：此项方法对于电子签名工具无任何特殊的要求，原则上适用于任何类型的电子签名工具。

4、实用性强，便于普及：因采用的均是成熟的技术，实现起来简单易行，便于推广应用。

5、安全性高：完全解决了个人电子签名工具被远程绑架控制的可能，同时也杜绝了外围破解的风险。

总之，应用本发明方法，增加了电子签名工具应用的安全性，简单方便，便于普及。

以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

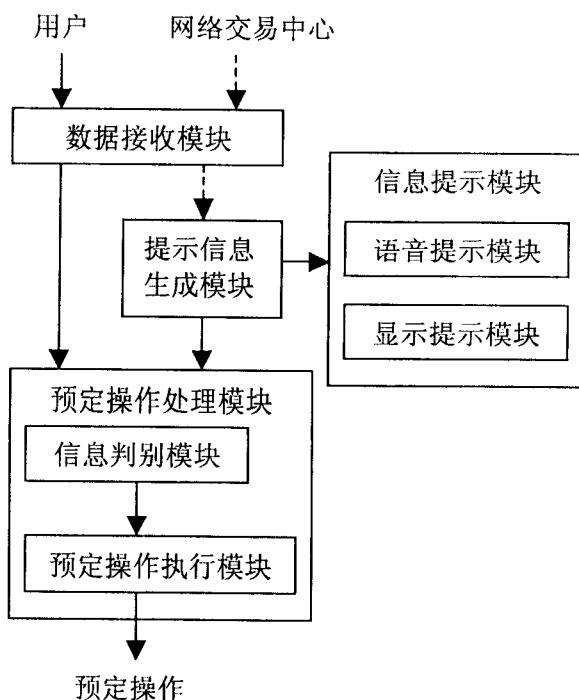


图1