(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 101616148 B
(45)授权公告日 2013.04.24

(21)申请号 200910089139.7
(22)申请日 2009.07.31
(73)专利权人 北京握奇数据系统有限公司
地址 100015 北京市朝阳区东直门外西八间房万红西街 2 号燕东商务花园
(72)发明人 耿建华 胡鹏
(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06Q 30/00(2012.01)

(56)对比文件
CN 101051907 A,2007.10.10, 说明书第5,6,8-13 页、附图 1-6.
CN 1554164 A,2004.12.08, 全文 .

审查员 袁敏

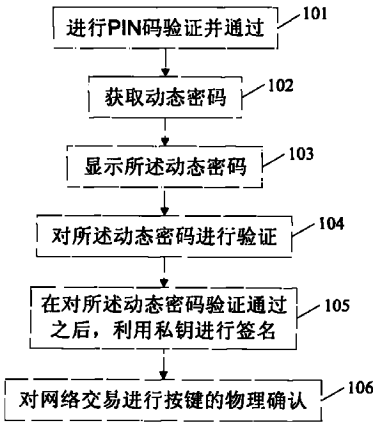
权利要求书2页 说明书7页 附图5页

(54)发明名称

网络交易身份认证方法和装置

(57)摘要

本发明实施例公开了一种网络交易身份认证方法,所述网络交易身份认证方法,在 OCL 设备进行 PIN 码验证通过之后,所述方法还包括 :获取动态密码 ;显示所述动态密码 ;对所述动态密码进行验证 ;在对所述动态密码验证通过之后,利用私钥进行签名 ;对网络交易进行按键的物理确认。本发明实施例还公开了一种网络交易身份认证装置,本发明适用于在网络交易中对用户的身份进行认证。



CN 101616148 B

1. 一种网络交易身份认证方法，其通过使用操作控制列表 OCL 设备进行网络交易，其特征在于，在 OCL 设备进行 PIN 码验证通过之后，还包括：

获取动态密码，所述动态密码为 OCL 设备自身生成的随机数，或者所述动态密码为验证服务器采用自身内部的密钥算法、对 OCL 设备的实体信息和时间或者时间信息进行处理后而生成的；

显示所述动态密码；

对所述动态密码进行验证，所述验证过程在 OCL 设备内部完成；

在对所述动态密码验证通过之后，利用私钥进行签名；

对网络交易进行按键的物理确认。

2. 根据权利要求 1 所述的网络交易身份认证方法，其特征在于，所述获取动态密码包括：

自身生成动态密码；

或者

接收验证服务器发送的动态密码。

3. 根据权利要求 1 或 2 所述的网络交易身份认证方法，其特征在于，所述对所述动态密码进行验证包括：

通过所述 OCL 设备的键盘输入所述 OCL 设备上显示的动态密码；

将所述通过所述 OCL 设备的键盘输入的动态密码与所述 OCL 设备获取的动态密码进行验证。

4. 根据权利要求 1 或 2 所述的网络交易身份认证方法，其特征在于，所述对所述动态密码进行验证包括：

通过所述 OCL 设备上的按键进行物理确认，对所述 OCL 设备获取的动态密码进行验证。

5. 一种网络交易身份认证装置，包括 PIN 码验证单元，用于对 OCL 设备进行 PIN 码验证，其特征在于，还包括：

获取单元，用于接收所述 PIN 码验证单元验证通过的通知，获取动态密码，所述动态密码为 OCL 设备自身生成的随机数，或者所述动态密码为验证服务器采用自身内部的密钥算法、对 OCL 设备的实体信息和时间或者时间信息进行处理后而生成的；

显示单元，用于显示所述获取单元获取的动态密码；

动态密码验证单元，用于对所述获取单元获取的动态密码进行验证，向签名单元发送验证通过的通知，所述验证过程在 OCL 设备内部完成；

签名单元，用于在接收到所述动态密码验证单元验证通过的通知后，利用所述 OCL 设备的私钥进行签名，并提示确认单元进行确认；

确认单元，用于根据所述签名单元的提示，对网络交易进行按键的物理确认。

6. 根据权利要求 5 所述的网络交易身份认证装置，其特征在于，所述装置还包括：

生成单元，用于自身生成动态密码，将所述动态密码发送给所述获取单元；

则所述获取单元还用于接收所述生成单元发送的动态密码。

7. 根据权利要求 5 所述的网络交易身份认证装置，其特征在于，所述装置还包括：

接收单元，用于接收验证服务器发送的动态密码，并将所述动态密码转发给所述获取单元；

则所述获取单元还用于接收所述接收单元转发的动态密码。

8. 根据权利要求6或7所述的网络交易身份认证装置，其特征在于，所述动态密码验证单元包括：

输入子单元，用于通过所述 OCL 设备的键盘输入所述显示单元显示的动态密码；

验证子单元，用于将所述输入子单元输入的动态密码与所述获取单元获取的动态密码进行验证，并向签名单元发送验证通过的通知。

9. 根据权利要求6或7所述的网络交易身份认证装置，其特征在于，所述动态密码验证单元包括：

确认子单元，用于通过所述 OCL 设备上的按键进行物理确认，对所述获取单元获取的动态密码进行验证，并向签名单元发送验证通过的通知。

网络交易身份认证方法和装置

技术领域

[0001] 本发明涉及数据安全技术领域，特别涉及一种网络交易身份认证方法和装置。

背景技术

[0002] 目前，在网络银行应用中，USB Key作为身份认证和电子证书工具被广泛采用。USB Key是一种USB接口的硬件设备，它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用USB Key内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因此保证了用户认证的安全性。

[0003] OCL(Operation Control List，操作控制列表）设备是一种高端的USB Key，与传统的USB Key产品相比，它增加了显示屏和按键等人机交互的接口。当需要使用USB Key内私钥进行签名时，就会启动按键等待操作，在有效时限内按下物理按键后签名才能成功，否则签名操作失败。即使OCL设备的密码被人截取，木马程序发起一个非法的交易申请，由于无法进行物理上的按键操作致使整个交易不能进行下去。另外，面对交易数据在用户客户端提交到OCL设备过程中被篡改的危险，OCL设备的显示屏可以把送到OCL设备的交易数据信息显示出来，用户在确认显示的内容正确无误后按下物理按键即可完成整个交易。

[0004] 通过OCL设备进行网络交易，最重要的就是保护OCL设备中的私钥，在未经允许的情况下，私钥不能被任何对象获得。OCL设备在用户权限的控制上只是采用了PIN(Personal Identification Number，个人标识号）码保护的方式，也就是说，当知道OCL设备的PIN码以后就能随意的使用私钥。

[0005] 在实现本发明的过程中，发明人发现现有技术中至少存在如下问题：

[0006] 在使用OCL设备进行网络交易时，只要获得OCL设备的私钥，就可以随意使用OCL设备进行交易了，网络交易的安全存在一定风险。

发明内容

[0007] 本发明的实施例提供一种网络交易身份认证方法和装置，能够有效地保证网络交易的安全性。

[0008] 本发明实施例采用的技术方案为：

[0009] 一种网络交易身份认证方法，其通过使用OCL设备进行网络交易，在OCL设备进行PIN码验证通过之后，包括：

[0010] 获取动态密码；

[0011] 显示所述动态密码；

[0012] 对所述动态密码进行验证；

[0013] 在对所述动态密码验证通过之后，利用私钥进行签名；

[0014] 对网络交易进行按键的物理确认。

[0015] 一种网络交易身份认证装置，包括PIN码验证单元，用于对OCL设备进行PIN码验证，所述网络交易身份认证装置，还包括：

[0016] 获取单元，用于接收所述 PIN 码验证单元验证通过的通知，获取动态密码；

[0017] 显示单元，用于显示所述获取单元获取的动态密码；

[0018] 动态密码验证单元，用于对所述获取单元获取的动态密码进行验证，向签名单元发送验证通过的通知；

[0019] 签名单元，用于在接收到所述动态密码验证单元验证通过的通知后，利用所述 OCL 设备的私钥进行签名，并提示确认单元进行确认；

[0020] 确认单元，用于根据所述签名单元的提示，对网络交易进行按键的物理确认。

[0021] 本发明实施例网络交易身份认证方法和装置，OCL 设备进行 PIN 码验证通过之后，将会获取一个动态密码并显示出来，然后对所述动态密码进行验证，在对所述动态密码验证通过之后，利用所述 OCL 设备的私钥进行签名，最后对网络交易进行按键的物理确认。与现有技术相比，本发明在保证用户安全登陆 OCL 设备的基础上，又增加了对私钥操作的保护，从而更加有效地保证了数据和交易的安全性；本发明在利用私钥进行签名之前，增加了动态密码的验证过程，即使用户 OCL 设备的私钥被非法获取，也不会因为用户的误操作而对网络交易带来风险，提升了网络交易的可靠性。

附图说明

[0022] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其它的附图。

[0023] 图 1 为本发明实施例一提供的网络交易身份认证方法流程图；

[0024] 图 2 为本发明实施例二提供的网络交易身份认证方法流程图；

[0025] 图 3 为本发明实施例三提供的网络交易身份认证方法流程图；

[0026] 图 4 为本发明实施例四提供的网络交易身份认证装置结构示意图；

[0027] 图 5 为本发明实施例五提供的网络交易身份认证装置结构示意图；

[0028] 图 6 为本发明实施例六提供的网络交易身份认证装置结构示意图。

具体实施方式

[0029] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0030] 为使本发明技术方案的优点更加清楚，下面结合附图和实施例对本发明作详细说明。

[0031] 在本发明的所有实施例中，所述网络交易身份认证方法适用于高端 OCL 设备，但不仅限于此。

[0032] 实施例一

[0033] 本实施例提供一种网络交易身份认证方法，能够有效地保证网络交易的安全性。

[0034] 如图 1 所示，所述网络交易身份认证方法，其通过使用 OCL 设备进行网络交易，所

述方法包括：

[0035] 101、用户通过 OCL 设备输入 PIN 码，OCL 设备对所述 PIN 码进行验证，并通过。

[0036] 102、OCL 设备获取动态密码；

[0037] 103、OCL 设备显示所述动态密码；

[0038] 104、OCL 设备对所述动态密码进行验证；

[0039] 105、在对所述动态密码验证通过之后，OCL 设备利用私钥进行签名；

[0040] 106、用户对网络交易进行按键的物理确认。

[0041] 本发明实施例网络交易身份认证方法，OCL 设备进行 PIN 码验证通过之后，将会获取一个动态密码并显示出来，然后对所述动态密码进行验证，在对所述动态密码验证通过之后，利用所述 OCL 设备的私钥进行签名，最后对网络交易进行按键的物理确认。与现有技术相比，本发明在保证用户安全登陆 OCL 设备的基础上，又增加了对私钥操作的保护，从而更加有效地保证了数据和交易的安全性；本发明在利用私钥进行签名之前，增加了动态密码的验证过程，即使用户 OCL 设备的私钥被非法获取，也不会因为用户的误操作而对网络交易带来风险，提升了网络交易的可靠性。

[0042] 实施例二

[0043] 在本实施例中，OCL 设备自身生成动态密码并显示出来，用户通过 OCL 设备上的键盘或者 PC 上的键盘输入所述 OCL 设备显示的动态密码，或者通过 OCL 设备上的按键进行物理确认，对所述 OCL 设备生成的动态密码进行验证。

[0044] 如图 2 所示，所述网络交易身份认证方法包括：

[0045] 201、用户登录网上银行。

[0046] 202、用户在 PC 上插入 OCL 设备。

[0047] 203、用户通过 OCL 设备上的键盘或者 PC 上的键盘输入 OCL 设备的 PIN 码，并进行验证。

[0048] 204、若验证失败，则提示用户错误并重新输入。

[0049] 205、若验证通过，则 OCL 设备自身生成一个动态密码。

[0050] 其中，OCL 设备自身具有产生随机数的功能，在用户每次登陆网上银行进行身份认证时，OCL 设备都会生成一个随机数作为动态密码。

[0051] 206、OCL 设备将所述动态密码在显示屏上显示出来。

[0052] 207、用户通过 OCL 设备上的键盘或者 PC 上的键盘输入所述显示屏上显示的动态密码，与所述 OCL 设备生成的动态密码进行验证。其中，所述验证过程在 OCL 设备内部完成。

[0053] 其中，在所述 OCL 设备上设置有键盘，用户直接通过所述 OCL 设备的键盘输入所述显示屏上显示的密码，并与 OCL 设备生成的动态密码进行比对。

[0054] 或者，在 PC 的上层软件上设置有一个动态密码的输入框，用户通过 PC 的键盘在该输入框内输入所述显示屏上显示的密码，并与 OCL 设备生成的动态密码进行比对。

[0055] 208、若验证失败，则阻止对 OCL 设备的使用和网络银行的登录请求，提示用户错误并重新输入。

[0056] 209、若验证通过，则 OCL 设备允许用户使用私钥完成签名操作。

[0057] 210、在用户使用私钥完成签名操作后，用户对网络交易进行按键的物理确认。

[0058] 其中，所述步骤 207-209 可以由如下步骤替换：

[0059] 207a、用户按下 OCL 设备上的按键，进行按键的物理确认，对所述动态密码进行验证。从而能够保证是用户本人在使用 OCL 设备，而不是别的木马或者病毒。

[0060] 208a、验证通过，OCL 设备允许用户使用私钥完成签名操作。

[0061] 至此，用户通过 OCL 设备完成身份认证，可以安全地进行网络交易。

[0062] 本发明实施例网络交易身份认证方法，OCL 设备进行 PIN 码验证通过之后，将会生成一个动态密码并显示出来，用户输入所述 OCL 设备显示的动态密码或者通过按键的物理确认，对所述动态密码进行验证，在对所述动态密码验证通过之后，利用所述 OCL 设备的私钥进行签名，最后对网络交易进行按键的物理确认。与现有技术相比，本发明在保证用户安全登陆 OCL 设备的基础上，又增加了对私钥操作的保护，从而更加有效地保证了数据和交易的安全性；本发明在利用私钥进行签名之前，增加了动态密码的验证过程，即使用户 OCL 设备的私钥被非法获取，也不会因为用户的误操作而对网络交易带来风险，提升了网络交易的可靠性。

[0063] 实施例三

[0064] 在本实施例中，位于网络银行后台的验证服务器生成一个动态密码，并将所述动态密码发送给 OCL 设备，OCL 设备将所述动态密码显示出来，用户通过 OCL 设备上的键盘或者 PC 上的键盘输入所述 OCL 设备显示的动态密码，或者通过 OCL 设备上的按键进行物理确认，对所述 OCL 设备接收的动态密码进行验证。

[0065] 如图 3 所示，所述网络交易身份认证方法包括：

[0066] 301-304、与步骤 201-204 相同，在此不再赘述。

[0067] 305、若验证通过，则验证服务器生成一个动态密码。

[0068] 在网络银行的后台部署有一台验证服务器，在 OCL 设备对 PIN 码验证通过之后，验证服务器采用自身内部的密钥算法，并对 OCL 设备的实体信息和时间或者时间信息进行处理，生成一个动态密码。

[0069] 306、验证服务器将所生成的动态密码发送给 OCL 设备。

[0070] 307、OCL 设备将验证服务器发送来的动态密码在显示屏上显示出来。

[0071] 308-311、与步骤 207-210 相同，在此不再赘述。

[0072] 至此，用户通过 OCL 设备完成身份认证，可以安全地进行网络交易。

[0073] 本发明实施例网络交易身份认证方法，在网络银行的后台设置有验证服务器，OCL 设备进行 PIN 码验证通过之后，所述验证服务器生成一个动态密码，并将所述动态密码发送给 OCL 设备，OCL 设备将所述动态密码显示出来，用户输入所述 OCL 设备显示的动态密码或者通过按键的物理确认，对所述动态密码进行验证，在对所述动态密码验证通过之后，利用所述 OCL 设备的私钥进行签名，最后对网络交易进行按键的物理确认。与现有技术相比，在保证用户安全登陆 OCL 设备的基础上，又增加了对私钥操作的保护，从而更加有效地保证了数据和交易的安全性；本发明在利用私钥进行签名之前，增加了动态密码的验证过程，即使用户 OCL 设备的私钥被非法获取，也不会因为用户的误操作而对网络交易带来风险，提升了网络交易的可靠性。

[0074] 实施例四

[0075] 本实施例提供一种网络交易身份认证装置，能够有效地保证数据和交易的安全性。

[0076] 如图4所示，所述网络交易身份认证装置，包括PIN码验证单元401，用于对OCL设备进行PIN码验证，所述网络交易身份认证装置，还包括：

[0077] 获取单元402，用于接收所述PIN码验证单元401验证通过的通知，获取动态密码；

[0078] 显示单元403，用于显示所述获取单元402获取的动态密码；

[0079] 动态密码验证单元404，用于对所述获取单元402获取的动态密码进行验证，向签名单元405发送验证通过的通知；

[0080] 签名单元405，用于在接收到所述动态密码验证单元404验证通过的通知后，利用所述OCL设备的私钥进行签名，并提示确认单元406进行确认；

[0081] 确认单元406，用于根据所述签名单元405的提示，对网络交易进行按键的物理确认。

[0082] 本发明实施例网络交易身份认证装置，PIN码验证单元进行PIN码验证通过之后，获取单元将会获取一个动态密码，并由显示单元显示出来，动态密码验证单元对所述动态密码进行验证，验证通过之后通知签名单元，签名单元利用所述OCL设备的私钥进行签名，并提示确认单元对网络交易进行按键的物理确认。与现有技术相比，本发明在保证用户安全登陆OCL设备的基础上，又增加了对私钥操作的保护，从而更加有效地保证了数据和交易的安全性；本发明在利用私钥进行签名之前，增加了动态密码的验证过程，即使用户OCL设备的私钥被非法获取，也不会因为用户的误操作而对网络交易带来风险，提升了网络交易的可靠性。

[0083] 实施例五

[0084] 在本实施例中，所述网络交易身份认证装置的具体表现形式为OCL设备。OCL设备自身生成动态密码并显示出来，用户通过OCL设备上的键盘或者PC上的键盘输入所述OCL设备显示的动态密码，或者通过OCL设备上的按键进行物理确认，对所述OCL设备生成的动态密码进行验证。

[0085] 如图5所示，所述网络交易身份认证装置，包括PIN码验证单元401，用于对OCL设备进行PIN码验证，所述网络交易身份认证装置，还包括：

[0086] 获取单元402，用于接收所述PIN码验证单元401验证通过的通知，获取动态密码；

[0087] 显示单元403，用于显示所述获取单元402获取的动态密码；

[0088] 动态密码验证单元404，用于对所述获取单元402获取的动态密码进行验证，向签名单元405发送验证通过的通知；

[0089] 签名单元405，用于在接收到所述动态密码验证单元404验证通过的通知后，利用所述OCL设备的私钥进行签名，并提示确认单元406进行确认；

[0090] 确认单元406，用于根据所述签名单元405的提示，对网络交易进行按键的物理确认。

[0091] 进一步，所述装置还包括：

[0092] 生成单元407，用于自身生成动态密码，将所述动态密码发送给所述获取单元402。其中，OCL设备自身具有产生随机数的功能，在用户每次登陆网上银行进行身份认证时，OCL设备都会生成一个随机数作为动态密码。

[0093] 则所述获取单元 402 还用于接收所述生成单元 407 发送的动态密码。

[0094] 其中，当用户通过 OCL 设备上的键盘输入所述显示单元 402 显示的动态密码时，所述动态密码验证单元 404 包括：

[0095] 输入子单元 4041，用于通过所述 OCL 设备的键盘输入所述显示单元 403 显示的动态密码；

[0096] 验证子单元 4042，用于将所述输入子单元 4041 输入的动态密码与所述获取单元 402 获取的动态密码进行验证，并向签名单元 405 发送验证通过的通知。

[0097] 其中，在所述 OCL 设备上设置有键盘，用户直接通过所述 OCL 设备的键盘输入所述显示屏上显示的密码，并与 OCL 设备生成的动态密码进行比对。

[0098] 或者，在 PC 的上层软件上设置有一个动态密码的输入框，用户通过 PC 的键盘在该输入框内输入所述显示屏上显示的密码，并与 OCL 设备生成的动态密码进行比对。

[0099] 其中，当通过 OCL 设备上的按键进行物理确认时，所述动态密码验证单元 404 包括：

[0100] 确认子单元 4043，用于通过所述 OCL 设备上的按键进行物理确认，对所述获取单元 402 获取的动态密码进行验证，并向签名单元 405 发送验证通过的通知。

[0101] 本发明实施例网络交易身份认证装置，PIN 码验证单元进行 PIN 码验证通过之后，生成子单元将会生成一个动态密码，并由显示单元显示出来，动态密码验证单元对所述动态密码进行验证，验证通过之后通知签名单元，签名单元利用所述 OCL 设备的私钥进行签名，并提示确认单元对网络交易进行按键的物理确认。与现有技术相比，本发明在保证用户安全登陆 OCL 设备的基础上，又增加了对私钥操作的保护，从而更加有效地保证了数据和交易的安全性；本发明在利用私钥进行签名之前，增加了动态密码的验证过程，即使用户 OCL 设备的私钥被非法获取，也不会因为用户的误操作而对网络交易带来风险，提升了网络交易的可靠性。

[0102] 实施例六

[0103] 在本实施例中，所述网络交易身份认证装置的具体表现形式为 OCL 设备。位于网络银行后台的验证服务器生成一个动态密码，并将所述动态密码发送给 OCL 设备，OCL 设备将所述动态密码显示出来，用户通过 OCL 设备上的键盘或者 PC 上的键盘输入所述 OCL 设备显示的动态密码，或者通过 OCL 设备上的按键进行物理确认，对所述 OCL 设备接收的动态密码进行验证。

[0104] 如图 6 所示，所述网络交易身份认证装置，包括 PIN 码验证单元 401，用于对 OCL 设备进行 PIN 码验证，所述网络交易身份认证装置，还包括：

[0105] 获取单元 402，用于接收所述 PIN 码验证单元 401 验证通过的通知，获取动态密码；

[0106] 显示单元 403，用于显示所述获取单元 402 获取的动态密码；

[0107] 动态密码验证单元 404，用于对所述获取单元 402 获取的动态密码进行验证，向签名单元 405 发送验证通过的通知；

[0108] 签名单元 405，用于在接收到所述动态密码验证单元 404 验证通过的通知后，利用所述 OCL 设备的私钥进行签名，并提示确认单元 406 进行确认；

[0109] 确认单元 406，用于根据所述签名单元 405 的提示，对网络交易进行按键的物理确

认。

[0110] 其中，所述装置还包括：

[0111] 接收单元 408，用于接收验证服务器发送的动态密码，将所述动态密码转发给所述获取单元 402。在网络银行的后台部署有一台验证服务器，在 OCL 设备对 PIN 码验证通过之后，验证服务器采用自身内部的密钥算法，对 OCL 设备的实体信息和时间或者时间信息进行处理，生成一个动态密码，并将所述动态密码向 OCL 设备发送。

[0112] 则所述获取单元 402 还用于接收所述接收单元 408 转发的动态密码。

[0113] 其中，当用户通过 OCL 设备上的键盘输入所述显示单元 402 显示的动态密码时，所述动态密码验证单元 404 包括：

[0114] 输入子单元 4041，用于通过所述 OCL 设备的键盘输入所述显示单元 403 显示的动态密码；

[0115] 验证子单元 4042，用于将所述输入子单元 4041 输入的动态密码与所述获取单元 402 获取的动态密码进行验证，并向签名单元 405 发送验证通过的通知。

[0116] 其中，在所述 OCL 设备上设置有键盘，用户直接通过所述 OCL 设备的键盘输入所述显示屏上显示的密码，并与 OCL 设备生成的动态密码进行比对。

[0117] 或者，在 PC 的上层软件上设置有一个动态密码的输入框，用户通过 PC 的键盘在该输入框内输入所述显示屏上显示的密码，并与 OCL 设备生成的动态密码进行比对。

[0118] 其中，当通过 OCL 设备上的按键进行物理确认时，所述动态密码验证单元 404 包括：

[0119] 确认子单元 4043，用于通过所述 OCL 设备上的按键进行物理确认，对所述获取单元 402 获取的动态密码进行验证，并向签名单元 405 发送验证通过的通知。

[0120] 本发明实施例网络交易身份认证装置，PIN 码验证单元进行 PIN 码验证通过之后，接收子单元将会接收验证服务器发送的动态密码，并由显示单元显示出来，动态密码验证单元对所述动态密码进行验证，验证通过之后通知签名单元，签名单元利用所述 OCL 设备的私钥进行签名，并提示确认单元对网络交易进行按键的物理确认。与现有技术相比，本发明在保证用户安全登陆 OCL 设备的基础上，又增加了对私钥操作的保护，从而更加有效地保证了数据和交易的安全性；本发明在利用私钥进行签名之前，增加了动态密码的验证过程，即使用户 OCL 设备的私钥被非法获取，也不会因为用户的误操作而对网络交易带来风险，提升了网络交易的可靠性。

[0121] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体 (Read-Only Memory，ROM) 或随机存储记忆体 (Random Access Memory，RAM) 等。

[0122] 以上所述，仅为本发明的具体实施方式，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。

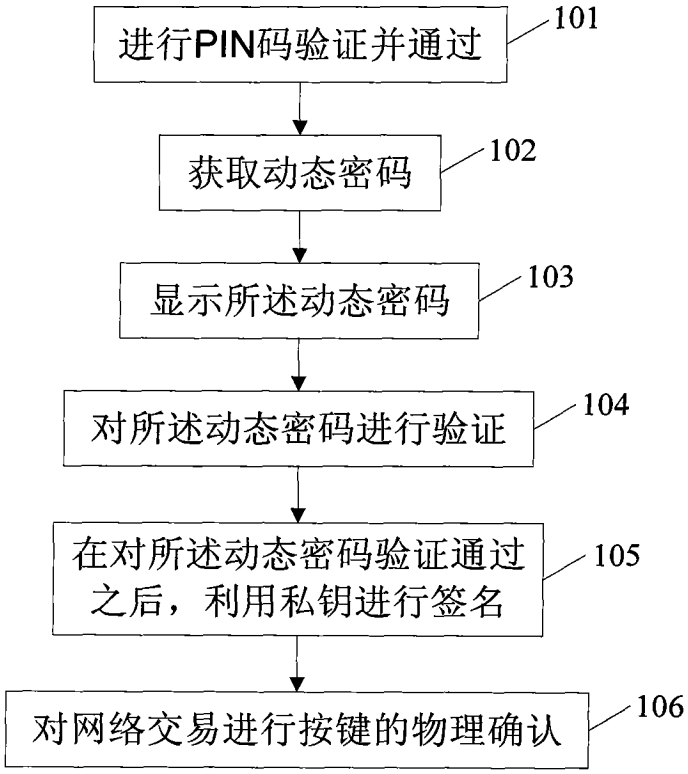

进行PIN码验证并通过
101
获取动态密码
102
显示所述动态密码
103
对所述动态密码进行验证
104
在对所述动态密码验证通过之后，利用私钥进行签名
105
对网络交易进行按键的物理确认
106

图 1

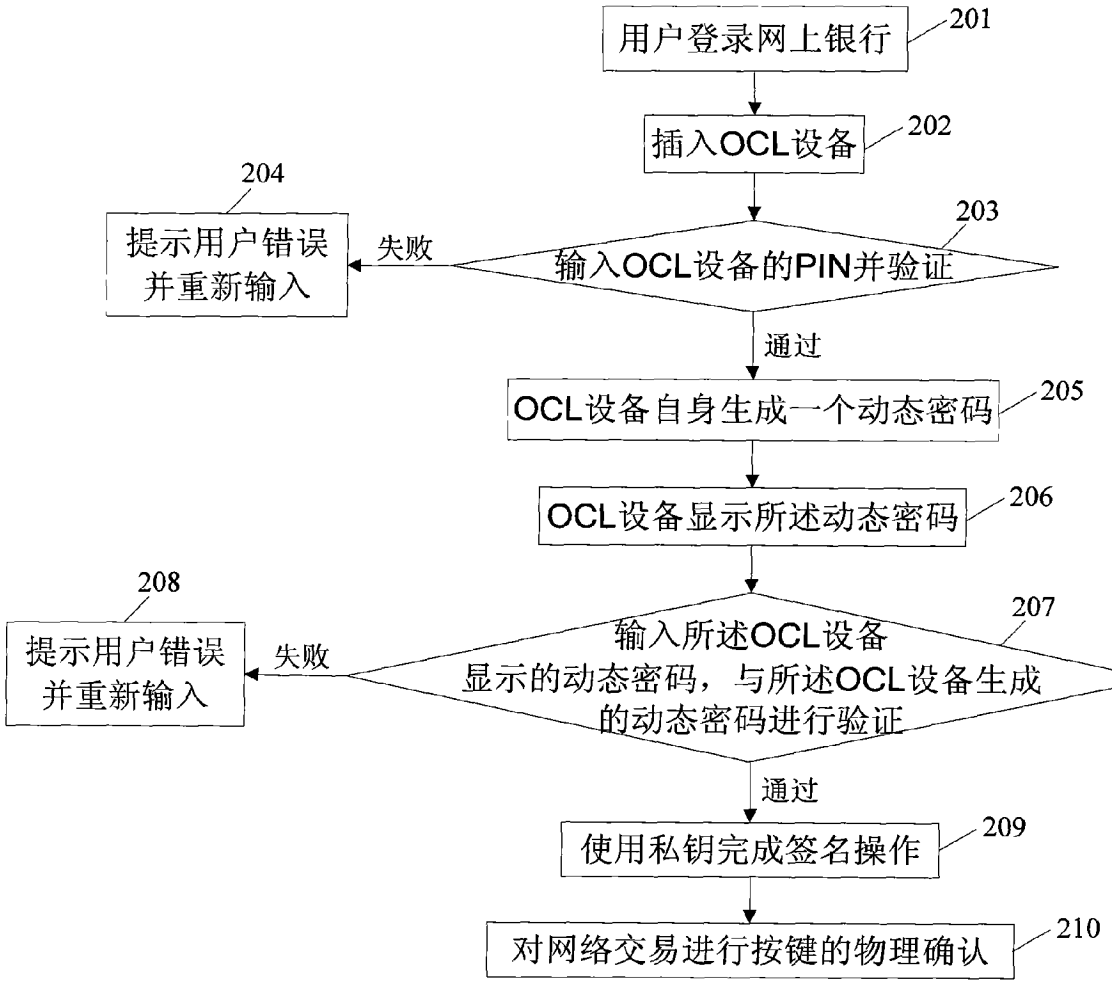

用户登录网上银行
201
插入OCL设备
202
输入OCL设备的PIN并验证
203
失败
提示用户错误
并重新输入
204
通过
OCL设备自身生成一个动态密码
205
OCL设备显示所述动态密码
206
输入所述OCL设备
显示的动态密码，与所述OCL设备生成
的动态密码进行验证
207
失败
提示用户错误
并重新输入
208
通过
使用私钥完成签名操作
209
对网络交易进行按键的物理确认
210

图 2

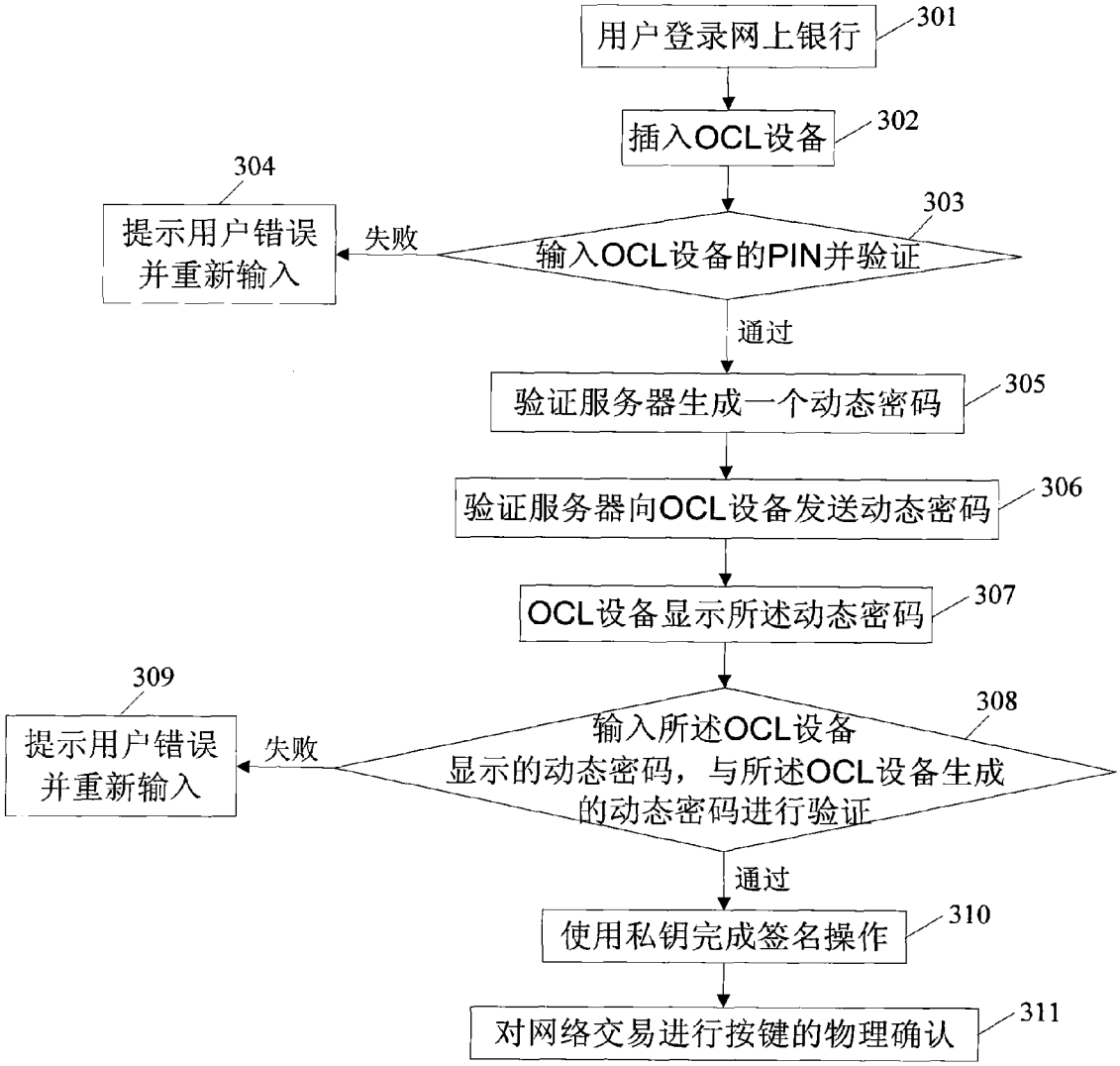

用户登录网上银行
301
插入OCL设备
302
输入OCL设备的PIN并验证
303
失败
提示用户错误
并重新输入
304
通过
验证服务器生成一个动态密码
305
验证服务器向OCL设备发送动态密码
306
OCL设备显示所述动态密码
307
输入所述OCL设备
显示的动态密码，与所述OCL设备生成
的动态密码进行验证
308
失败
提示用户错误
并重新输入
309
通过
使用私钥完成签名操作
310
对网络交易进行按键的物理确认
311

图 3

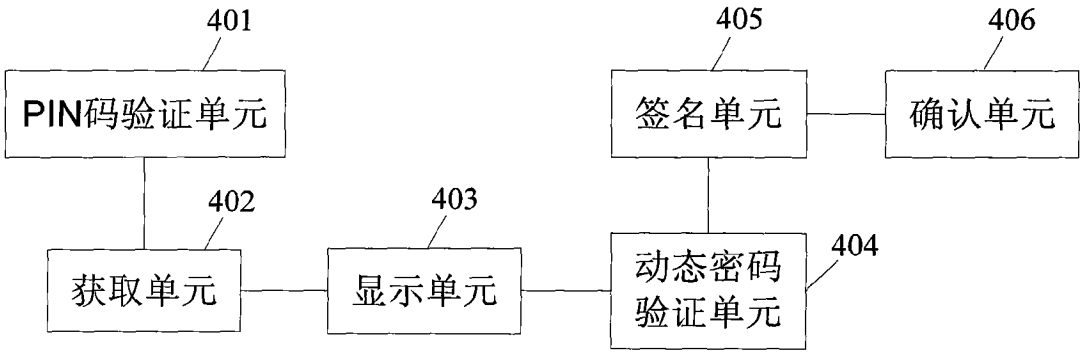

401
PIN码验证单元
405
签名单元
406
确认单元
402
获取单元
403
显示单元
动态密码
验证单元
404

图 4

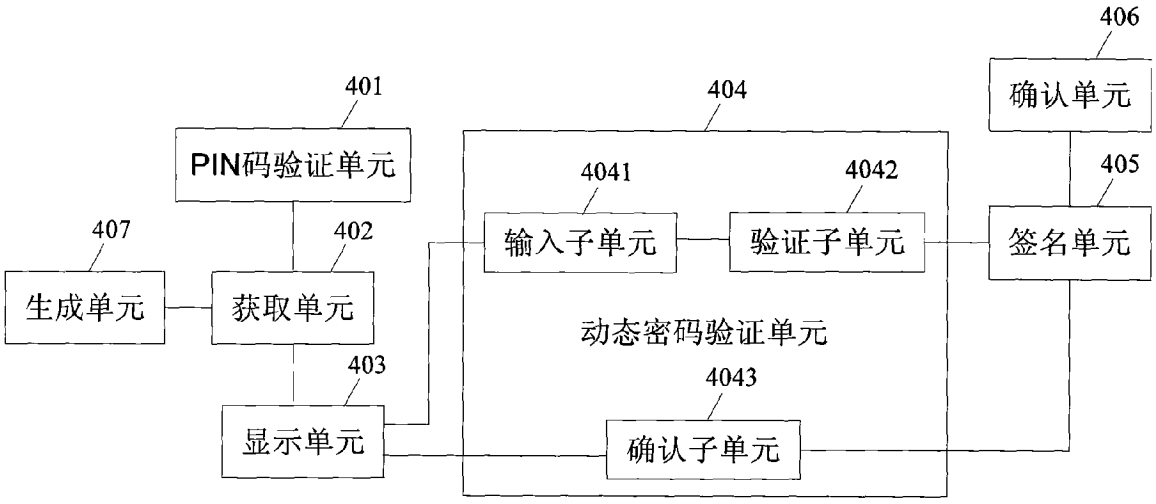

406
确认单元
401
PIN码验证单元
404
4041
输入子单元
4042
验证子单元
405
签名单元
407
生成单元
402
获取单元
动态密码验证单元
403
显示单元
4043
确认子单元

图 5

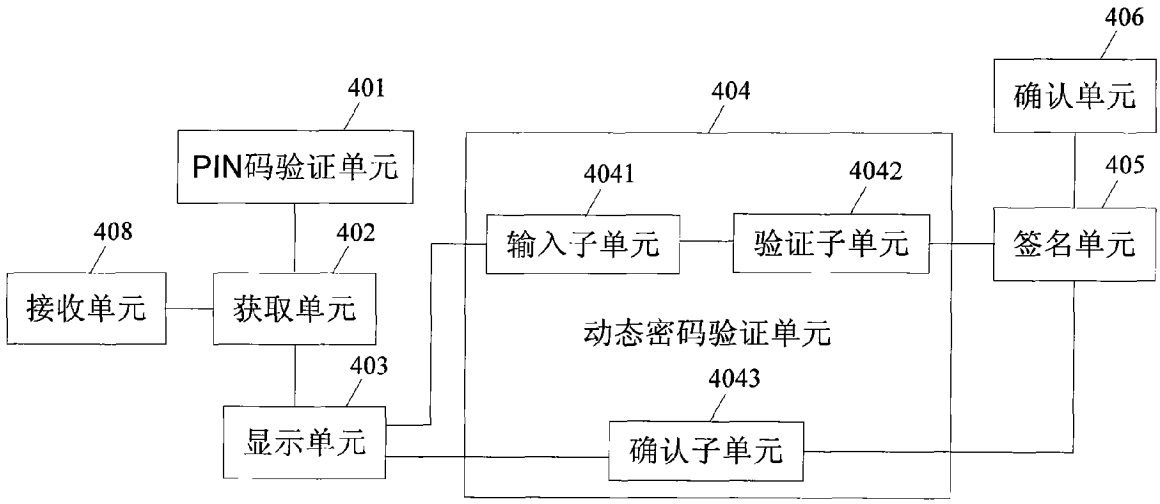

406
确认单元
401
404
PIN码验证单元
4041
4042
405
408
402
输入子单元
验证子单元
签名单元
接收单元
获取单元
动态密码验证单元
403
4043
显示单元
确认子单元

图 6