(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 101789864 B
(45)授权公告日 2012.10.10

(21)申请号 201010107212.1

(22)申请日 2010.02.05

(73)专利权人 中国工商银行股份有限公司
地址 100140 北京市西城区复兴门内大街55号

(72)发明人 谭路远 伊劲松 闫记东 张安龙 付新丽 曾凯 李丹 王静媛

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 任默闻

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 101102194 A,2008.01.09,
WO 2008004312 A1,2008.01.10,
CN 101309141 A,2008.11.19,
WO 2010000298 A1,2010.01.07,
CN 1614924 A,2005.05.11,

审查员 李文娟

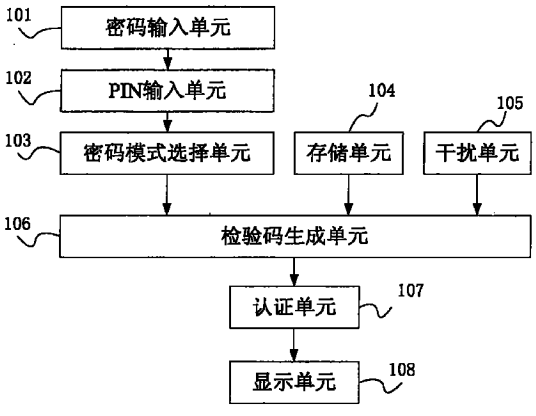
权利要求书 3 页 说明书 7 页 附图 5 页

(54)发明名称

一种网上银行后台身份认证方法、装置及系统

(57)摘要

本发明实施例提供了一种网上银行后台身份认证方法、装置及系统，该装置包括：密码输入单元，接收用户输入的多要素密码；PIN输入单元，接收用户输入的PIN；密码模式选择单元，向用户提示多要素密码生成模式选择请求，接收用户输入的多要素密码生成模式；存储单元，存储用户密钥和密码算法；干扰单元，生成干扰因子；校验码生成单元，根据用户选择的多要素密码生成模式获取当前干扰因子、预存的用户密钥以及对应的密码算法，根据干扰因子、用户密钥和对应的密码算法生成校验码；认证单元，用校验码对多要素密码进行认证生成认证结果；显示单元，显示认证结果。用以解决网上银行等金融交易系统后台服务器的身份鉴别和交易认证问题。



CN 101789864 B

1. 一种网上银行后台身份认证方法，其特征是，所述的方法包括：

外部交易页面向用户提供多要素密码和多要素密码生成模式；

接收用户输入的多要素密码；

向用户提示个人识别码 PIN 输入信息；

接收用户输入的 PIN；

确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求；

接收用户输入的多要素密码生成模式；

根据输入的多要素密码生成模式获取当前的干扰因子、预存的用户密钥以及对应的密码算法，并根据当前的干扰因子、获取的用户密钥和对应的密码算法生成所述多要素密码的校验码；

用所述的校验码对所述的多要素密码进行认证。

2. 根据权利要求 1 所述的方法，其特征是，所述的多要素密码生成模式包括：一次密码 OTP 生成模式和短签名密码 SIGN 生成模式。

3. 根据权利要求 2 所述的方法，其特征是，接收用户通过键盘或触摸屏输入的 OTP 生成模式；

根据所述的 OTP 生成模式获取当前的干扰因子、预存的用户密钥以及对应的 OTP 密码算法，并根据所述的干扰因子、用户密钥和 OTP 密码算法生成 OTP 校验码，用所述的 OTP 校验码对所述的多要素密码进行认证。

4. 根据权利要求 2 所述的方法，其特征是，接收用户通过键盘或触摸屏输入的 SIGN 生成模式；

根据所述的 SIGN 生成模式，向用户提示短签名因子信息输入请求；

接收用户通过键盘或触摸屏输入的短签名因子信息，其中，所述短签名因子信息由外部交易页面在向用户提供多要素密码和多要素密码生成模式的同时进行提供；

根据所述的 SIGN 生成模式获取当前干扰因子、预存的用户密钥以及 SIGN 密码算法，根据输入的短签名因子信息、所述的干扰因子、用户密钥和 SIGN 密码算法生成 SIGN 校验码，用所述的 SIGN 校验码对所述的多要素密码进行认证。

5. 根据权利要求 4 所述的方法，其特征是，所述的短签名因子信息包括：交易帐号、交易金额和 / 或交易字符串。

6. 根据权利要求 1 所述的方法，其特征是，所述的干扰因子包括：时钟数据和 / 或事件计数数据。

7. 一种网上银行后台身份认证装置，其特征是，所述的装置包括：

密码输入单元，用于接收用户输入的多要素密码；

PIN 输入单元，用于向用户提示 PIN 输入请求，接收用户输入的 PIN；

密码模式选择单元，用于确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求，接收用户输入的多要素密码生成模式；

存储单元，用于存储用户密钥和密码算法；

干扰单元，用于生成干扰因子；

校验码生成单元，用于根据用户选择的多要素密码生成模式获取当前干扰因子，并获取预存的用户密钥以及对应的密码算法，根据所述的干扰因子、用户密钥和对应的密码算

法生成校验码；

认证单元，用所述的校验码对所述的多要素密码进行认证，生成认证结果；

显示单元，用于显示所述的认证结果；

所述用户输入的多要素密码和多要素密码生成模式由外部交易页面向用户提供。

8. 根据权利要求 7 所述的装置，其特征是，所述的多要素密码生成模式包括：一次密码 OTP 生成模式和短签名密码 SIGN 生成模式。

9. 根据权利要求 8 所述的装置，其特征是，所述的存储单元存储有 OTP 密码算法和 SIGN 密码算法；

所述的密码模式选择单元接收用户输入的 OTP 生成模式；

所述的校验码生成单元根据所述的 OTP 生成模式获取当前干扰因子、预存的用户密钥以及 OTP 密码算法，根据所述的干扰因子、用户密钥和 OTP 密码算法生成 OTP 校验码。

10. 根据权利要求 8 所述的装置，其特征是，所述的装置还包括：短签名因子输入单元，用于根据用户输入的短签名密码 SIGN 生成模式，向用户提示短签名因子信息输入请求，接收用户通过键盘或触摸屏输入的短签名因子信息；其中，所述短签名因子信息由外部交易页面在向用户提供多要素密码和多要素密码生成模式的同时进行提供；

其中，

所述的存储单元存储有 OTP 密码算法和 SIGN 密码算法；

所述的校验码生成单元根据所述的 SIGN 生成模式获取当前干扰因子、预存的用户密钥和 SIGN 密码算法、以及输入的短签名因子信息，并根据所述的干扰因子、用户密钥、输入的短签名因子信息和 SIGN 密码算法生成 SIGN 校验码。

11. 根据权利要求 10 所述的装置，其特征是，所述的短签名因子信息包括：交易帐号、交易金额和 / 或交易字符串。

12. 根据权利要求 7 所述的装置，其特征是，所述的干扰单元包括：

时钟，用于产生时间数据；

事件计数器，用于生成事件计数数据。

13. 一种网上银行后台身份认证系统，其特征是，所述的系统包括：身份认证装置和交易终端；

所述的交易终端与网上银行后台认证服务器连接，用于通过交易页面向用户提示多要素密码、多要素密码生成模式；

所述的身份认证装置包括：密码输入单元，用于接收用户输入的多要素密码；PIN 输入单元，用于向用户提示 PIN 输入请求，接收用户输入的 PIN；密码模式选择单元，用于确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求，接收用户输入的多要素密码生成模式；存储单元，用于存储用户密钥和密码算法；干扰单元，用于生成干扰因子；校验码生成单元，用于根据用户选择的多要素密码生成模式获取当前干扰因子，并获取预存的用户密钥以及对应的密码算法，根据所述的干扰因子、用户密钥和对应的密码算法生成校验码；认证单元，用所述的校验码对所述的多要素密码进行认证生成认证结果；显示单元，用于显示所述的认证结果。

14. 根据权利要求 13 所述的系统，其特征是，所述的多要素密码生成模式包括：一次密码 OTP 生成模式和短签名密码 SIGN 生成模式。

15. 根据权利要求 14 所述的系统，其特征是，所述的存储单元存储有 OTP 密码算法和 SIGN 密码算法；

所述的密码模式选择单元接收用户输入的 OTP 生成模式；

所述的校验码生成单元根据所述的 OTP 生成模式获取当前干扰因子、预存的用户密钥以及 OTP 密码算法，根据所述的干扰因子、用户密钥和 OTP 密码算法生成 OTP 校验码。

16. 根据权利要求 14 所述的系统，其特征是，所述的装置还包括：短签名因子输入单元，用于根据用户输入的短签名密码 SIGN 生成模式，向用户提示短签名因子信息输入请求，接收用户通过键盘或触摸屏输入的短签名因子信息，其中，所述短签名因子信息由外部交易页面在向用户提供多要素密码和多要素密码生成模式的同时进行提供；

其中，

所述的存储单元存储有 OTP 密码算法和 SIGN 密码算法；

所述的校验码生成单元根据所述的 SIGN 生成模式获取当前干扰因子、预存的用户密钥和 SIGN 密码算法、以及输入的短签名因子信息，并根据所述的干扰因子、用户密钥、输入的短签名因子信息和 SIGN 密码算法生成 SIGN 校验码。

17. 根据权利要求 16 所述的系统，其特征是，所述的短签名因子信息包括：交易帐号、交易金额和 / 或交易字符串。

18. 根据权利要求 13 所述的系统，其特征是，所述的干扰单元包括：

时钟，用于产生时间数据；

事件计数器，用于生成事件计数数据。

一种网上银行后台身份认证方法、装置及系统

技术领域

[0001] 本发明关于身份鉴别和交易认证技术，特别是关于网上银行等金融交易系统的身份鉴别和交易认证技术，具体的讲是一种网上银行后台身份认证方法、装置及系统。

背景技术

[0002] 在现有技术中，针对身份鉴别和交易授权认证的方案有如下几种：（一）静态密码：用户使用时常常设置弱密码，如生日、电话号等；容易被窃取和监听，如通过木马盗取和网络嗅探等。（二）刮刮卡和动态密码卡：实现一次一密，但无法保证交易数据的安全，存在交易数据被篡改的风险。（三）时间型动态令牌：基于时间的一次性密码产生器，能够保证一次一密，针对窃取和嗅探风险有一定的安全提升，但也不能完全根除风险。同时，仍不能防范数据被篡改。（四）USBKEY 和软证书：利用 PKI 体系，对数据进行数字签名和加密，保证数据的完整、不可抵赖、机密性等；但此种方式实施成本较高，需要后台部署 CA、RA、验签组件等；用户需要进行证书的申请、更新、恢复等管理操作，使用复杂。同时，软证书容易被复制和盗取；USBKEY 设备需要安装驱动和相关用户端组件才能使用，存在兼容性、易用性问题，且目前只能适用于计算机终端，无法在手机、电话、电视等渠道使用。同时，此种方式由于上层应用和底层签名加密之间有诸多环节，仍存在篡改数据的风险和被远程控制，造成恶意利用用户证书的风险。

[0003] 上述各种认证方案，要么安全性不高，存在被窃取和嗅探风险，不能对交易数据进行保护等；要么易用性不高，后台部署及用户使用复杂、无法在各种渠道广泛使用。

发明内容

[0004] 本发明实施例提供了一种网上银行后台身份认证方法、装置及系统，用以解决网上银行等金融交易系统后台的身份鉴别和交易认证的问题。

[0005] 本发明的目的之一是，提供一种身份认证方法，该方法包括：外部交易页面向用户提供多要素密码和多要素密码生成模式；接收用户输入的多要素密码；向用户提示个人识别码 PIN 输入信息；接收用户输入的 PIN；确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求；接收用户输入的多要素密码生成模式；根据输入的多要素密码生成模式获取当前的干扰因子、预存的用户密钥以及对应的密码算法，并根据当前的干扰因子、获取的用户密钥和对应的密码算法，生成所述多要素密码的校验码；用所述的校验码对所述的多要素密码进行认证。

[0006] 本发明的目的之一是，提供一种身份认证装置，该装置包括：密码输入单元，用于接收用户输入的多要素密码；PIN 输入单元，用于向用户提示 PIN 输入请求，接收用户输入的 PIN；密码模式选择单元，用于确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求，接收用户输入的多要素密码生成模式；存储单元，用于存储用户密钥和密码算法；干扰单元，用于生成干扰因子；校验码生成单元，用于根据用户选择的多要素密码生成模式获取当前干扰因子，并获取预存的用户密钥以及对应的密码算法，根据所述的干扰因

子、用户密钥和对应的密码算法生成校验码；认证单元，用所述的校验码对所述的多要素密码进行认证生成认证结果；显示单元，用于显示所述的认证结果；用户输入的多要素密码和多要素密码生成模式由外部交易页面向用户提供。

[0007] 本发明的目的之一是，提供一种身份认证系统，该系统包括：身份认证装置和交易终端；所述的交易终端与网上银行后台认证服务器连接，用于通过交易页面向用户提示多要素密码、多要素密码生成模式；所述的身份认证装置包括：密码输入单元，用于接收用户输入的多要素密码；PIN 输入单元，用于向用户提示 PIN 输入请求，接收用户输入的 PIN；密码模式选择单元，用于确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求，接收用户输入的多要素密码生成模式；存储单元，用于存储用户密钥和密码算法；干扰单元，用于生成干扰因子；校验码生成单元，用于根据用户选择的多要素密码生成模式获取当前干扰因子，并获取预存的用户密钥以及对应的密码算法，根据所述的干扰因子、用户密钥和对应的密码算法生成校验码；认证单元，用所述的校验码对所述的多要素密码进行认证生成认证结果；显示单元，用于显示所述的认证结果。

[0008] 本发明的有益效果在于，本发明通过从交易页面获取多要素密码、密码生成模式和短签名信息，将多要素密码、密码生成模式和短签名信息在本发明装置的显示器上通过挑战的方式输入，本发明装置通过用户输入的信息和自身存储的信息、编码方法生成校验码，用校验码对输入的多要素密码进行认证，从而实现对交易页面及其后台服务器真实性的认证。这种反向认证方法提高了交易认证的安全性。本发明身份认证装置为脱机使用，无需和手机、电话、计算机进行连接，此种脱机使用的方式，一是使得装置可适用于多个电子渠道，为多个渠道使用同一认证介质提供了基础。二是改善了认证介质的易用性，降低了装置使用难度，无需安装驱动和控件程序。本发明身份认证装置及系统可用于验证服务器端身份，同时支持一次密码 (OTP，One-Timepassword) 和短签名 (SIGN) 两种工作模式。本发明认证装置提供 PIN 码保护，避免因身份认证装置丢失而造成的风险。支持 PIN 码的修改和重置。

附图说明

[0009] 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他的附图。

[0010] 图 1 为本发明实施例身份认证方法流程图；

[0011] 图 2 为本发明实施例身份认证装置结构框图；

[0012] 图 3 为本发明实施例身份认证装置外观示意图；

[0013] 图 4 为本发明实施例身份认证装置内部结构框图；

[0014] 图 5 为本发明实施例身份认证系统的示意图；

[0015] 图 6 为本发明实施例身份认证系统 OTP 工作模式流程图；

[0016] 图 7 为本发明实施例身份认证系统 SIGN 工作模式流程图。

具体实施方式

[0017] 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他实施例，都属于本发明保护的范围。

[0018] 如图 1 所示，本发明具体实施方式提供了一种身份认证方法，该方法包括：接收用户输入的多要素密码（步骤 S101）；向用户提示个人识别码 PIN 输入信息（步骤 S102）；接收用户输入的 PIN（步骤 S103）；确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求（步骤 S104）；接收用户输入的多要素密码生成模式（步骤 S105）；根据所述的多要素密码生成模式获取当前干扰因子，并获取预存的用户密钥以及对应的密码算法，并根据当前干扰因子、用户密钥和密码算法生成校验码（步骤 S106）；用校验码对多要素密码进行认证（步骤 S107）。

[0019] 本具体实施方式的身份认证方法是基于身份认证装置的身份认证方法，可实现包括时间或者事件等多个干扰要素的一次性、多要素密码，用于用户身份鉴别及交易认证；同时，本实施例的身份认证方法提供短签名功能，可以保证交易数据不可篡改，不可抵赖。

[0020] 本具体实施方式多要素密码的第一层次的保护范围是基于当前干扰因子（包括当前时间，计数器等）产生一个动态密码；多要素密码的第二层次的保护范围是为了进一步防止交易关键信息被劫持和篡改的考虑，在基于当前干扰因子的基础上，加上交易关键信息，一并作为动态密码（或者叫验证码）的产生因子。本实施例的身份认证方法的应用场景不限于互联网，还包括手机、电话、ATM 等多种电子渠道。

[0021] 如图 2 所示，本发明具体实施方式的身份认证装置包括：密码输入单元 101 用于接收用户输入的多要素密码；PIN 输入单元 102 用于向用户提示 PIN 输入请求，接收用户输入的 PIN；密码模式选择单元 103 用于确定所述的 PIN 正确后，向用户提示多要素密码生成模式选择请求，接收用户输入的多要素密码生成模式；存储单元 104 用于存储用户密钥和密码算法；干扰单元 105 用于获取干扰因子；校验码生成单元 106 用于根据用户选择的多要素密码生成模式获取当前干扰因子，并获取预存的用户密钥以及对应的密码算法，根据当前干扰因子、用户密钥和对应的密码算法生成校验码；认证单元 107 用于校验码对多要素密码进行认证；显示单元 108 用于显示认证结果。

[0022] 具体实施方式的身份认证装置有两种工作模式，一种是一次密码 (OTP, One-Time password) 工作模式，另外一种是短签名 (SIGN) 工作模式。OTP 工作模式主要根据干扰因子和客户密钥，按照一定算法，如摘要算法、或对称加密算法等，产生一次性动态密码，通过此一次性密码达到身份鉴别和交易认证的目的。SIGN 工作模式主要根据客户输入元素（如交易金额和交易帐号），干扰因子、客户密钥，按照一定的算法，如摘要算法、或对称加密算法等，产生和交易数据相关一次性交易密码，通过此密码，保证交易数据的不可篡改，交易的不可抵赖。

[0023] 本发明通过从交易页面获取多要素密码、密码生成模式和短签名信息，将多要素密码、密码生成模式和短签名信息在本发明装置的显示器上通过挑战的方式输入，本发明装置通过用户输入的信息和自身存储的信息、编码方法生成校验码，用校验码对输入的多要素密码进行认证，从而实现对交易页面及其后台服务器真实性的认证。这种反向认证方法提高了交易认证的安全性。

[0024] 实施例

[0025] 以网上银行登录为例，介绍 OTP 工作模式的处理流程。本发明实施例的身份认证系统包括：身份认证装置和网上银行交易终端；交易终端与网上银行后台认证服务器连接，用于将后台认证服务器产生的 OTP 密码通过交易页面向用户提示。

[0026] 如图 3 所示，本实施例的身份认证装置包括：显示屏、输入键和外壳。输入键又可分为功能键和数字键盘。显示屏用于显示提示输入 OTP 密码和 PIN 码的指令信息，回显客户输入等功能；数字键盘主要用于输入 OTP 密码、PIN 码、交易数据等信息；功能键有开关键，用于启动和关闭装置；PIN 键，用于进入 PIN 码修改程序；OTP 键，用于进入 OTP 工作模式，根据当前干扰因子、客户密钥和 OTP 加密算法，产生一次性动态密码的 OTP 校验码；SIGN 键，用于进入 SIGN 工作模式，并根据客户输入元素、当前干扰因子、客户密钥和 SIGN 加密算法产生短签名密码的 SIGN 校验码。外壳，用于固定和保护内部零件及电路，并且具有美观和便于携带、使用的功能。本实施例的身份认证装置大小如同银行卡，易于携带，同时可根据需求进行灵活的外观定制。

[0027] 如图 4 所示，本实施例的身份认证装置的内部结构包括：中央处理器，用于根据各种条件和请求进行计算处理；显示单元、输入单元、存储单元、干扰因子单元和电源单元。其中，显示单元包括显示屏和显示驱动芯片等，用于显示身份认证装置的提示信息、客户输入及密码信息等；输入单元包括键盘和输入控制逻辑，用于客户输入 OTP 密码或 SIGN 密码、身份认证装置 PIN 码、交易挑战、功能选择等；存储单元，用于存储客户密钥，每个身份认证装置的客户密钥不同，可使用硬件随机发生器产生，存储单元还保存加密算法等其他信息；干扰因子单元，用于提供时间或者事件干扰因子，如果是时间因子则提供时钟晶振，如果是事件因子，则提供事件计数器；作为一种特例，身份认证装置可省略干扰因子单元，为防范密码重复，防止重发攻击，可在要求客户输入的交易元素中增加随机变量或时间戳等一次性信息，从而保证客户密码的随机性，实现一次一密；电源单元，用于提供身份认证装置电能的组件，例如电池、可更换备用电池的双电池电源、可充电电池等。身份认证装置可采用触控开关实现开盖自毁等物理保护。

[0028] 身份认证装置有两种工作模式，一种是 OTP 工作模式，另外一种是 SIGN 工作模式。OTP 工作模式主要根据干扰因子和客户密钥，按照一定算法，如摘要算法、或对称加密算法等，产生一次性动态密码的校验码，通过此一次性密码与校验码的比对，达到后台身份鉴别和交易认证的目的。

[0029] 如图 5 所示，为本实施例的网上银行后台身份认证系统，该系统包括：身份认证装置 201 和 ATM 终端 202；ATM 终端 202 与网上银行后台认证服务器连接，用于通过交易页面向用户提示多要素密码、多要素密码生成模式和短签名因子信息；身份认证装置 201 包括：中央处理器、显示器、开关按键、数字按键、密码模式选择键、存储器、干扰生成器、校验码生成器以及电池；其中，中央处理器分别与显示器、开关按键、数字按键、密码模式选择键、存储器、干扰生成器、校验码生成器以及电池相连接；开关按键接收用户进行的触按，执行开机动作；显示器向用户提示多要素密码和个人认证码 PIN 输入请求，用户通过数字按键输入多要素密码和 PIN；显示器向用户提示密码模式选择信息，用户通过密码模式选择键输入密码模式；存储器存储用户密钥和密码算法，干扰生成器生成干扰因子，校验码生成器根据用户输入的密码模式获取对应的密码算法，并根据输入的干扰因子、预存的用户密钥和对

应的密码算法生成多要素密码的校验码，并将校验码与输入的多要素密码进行比对，显示器显示比对结果；中央处理器控制显示器、开关按键、数字按键、密码模式选择键、存储器、干扰生成器和校验码生成器，电池提供工作电能。

[0030] 如图 6 所示，OTP 工作模式包括以下步骤：用户携带身份认证装置在网上银行终端上进行交易。其中，

[0031] 步骤 S201，客户访问网上银行登录页面，输入登录 ID；

[0032] 步骤 S202，页面提示在身份认证装置上输入的 OTP 密码；

[0033] 步骤 S203，客户按下身份认证装置的开关键，开启身份认证装置，即通过输入单元输入该 OTP 密码，并向处理单元发送指令启动身份认证装置；

[0034] 步骤 S204，身份认证装置的显示单元提示客户输入 PIN 码；

[0035] 步骤 S205，客户通过输入单元输入 PIN 码，处理单元从存储单元中获取正确的 PIN 码，并同客户输入的 PIN 码比较，如正确则显示单元提供功能选择提示，如错误则处理单元进行 PIN 码错误累计并记录在存储单元，当未超过最大错误次数时，显示单元提示客户重新输入 PIN 码，当达到最大 PIN 码错误次数时，处理单元拒绝再次比对 PIN 码和计算密码，身份认证装置处于锁死状态，只能进行 PIN 码重置，才能继续使用身份认证装置；

[0036] 步骤 S206，PIN 码正确，显示单元提示客户选择 OTP 或者 SIGN 功能；

[0037] 步骤 S207，客户按 OTP 键；

[0038] 步骤 S208，输入单元指示处理单元获得当前干扰因子，从存储单元获得客户密钥，并根据获得的当前干扰因子和客户密钥，使用 OTP 算法，得到一次性 OTP 密码的校验码，校验码可以是 6 位数字组成，根据需要可自定义长度和密码取值范围；

[0039] 步骤 S209，将得到的 OTP 校验码与输入的 OTP 密码进行比对，如果一致，则通过显示单元提供给客户验证成功，否则验证失败。

[0040] 客户按身份认证装置开关键关闭身份认证装置，此时输入单元指令处理单元将身份认证装置处于关闭状态，如客户不手工关闭身份认证装置，身份认证装置在显示 OTP 密码校验结果 15 秒后会自动关闭，此时间可根据需要自定义，此超时自动关闭由处理单元主动发起。

[0041] SIGN 工作模式主要根据客户输入元素，干扰因子、客户密钥，按照一定的算法，产生和交易数据相关一次性交易密码的校验码，通过此校验码，校验 SIGN 密码的合法性，从而判断后台服务器的真实性。

[0042] 如图 7 所示，SIGN 工作模式包括以下步骤：

[0043] 步骤 S301，客户进入交易录入页面，录入交易元素；

[0044] 步骤 S302，系统进行数据和交易的合法性校验后，回显交易确认页面，并提示客户使用动态身份认证装置进行短签名认证，并显示 SIGN 密码和交易元素（如：转出转入账号、交易金额和 / 或交易字符串等）；交易字符串可以是用户在后台预留的信息，比如：用户的昵称为 Lily，则系统进行数据和交易的合法性校验后，回显交易确认页面，并提示客户使用动态身份认证装置进行短签名认证，并显示 SIGN 密码和用户昵称输入请求，此时用户需在身份认证装置上分别输入显示的 SIGN 密码和 Lily。

[0045] 步骤 S303，客户按身份认证装置的开关键开启身份认证装置，输入该 SIGN 密码，并指令处理单元处于工作状态；

[0046] 步骤 S304，处理单元指令显示单元提示输入 PIN 码；

[0047] 步骤 S305，客户输入正确的 PIN 码，输入单元将客户输入的 PIN 传递给处理单元，处理单元从存储单元获取客户 PIN 码，并同客户输入的 PIN 码进行比对；

[0048] 步骤 S306，如果 PIN 码一致则指示显示单元提示客户进行 OTP 或者 SIGN 功能选择；

[0049] 步骤 S307，客户按 SIGN 键进入交易短签名功能；输入单元指令处理单元处于短签名功能；

[0050] 步骤 S308，交易页面提示短签名功能需要输入的内容；

[0051] 步骤 S309，客户根据交易页面提示的内容，在身份认证装置上输入交易账号和金额和 / 或交易字符串（如，用户的昵称 Lily），可以是分多个字段录入，或者将上述信息拼接成一个签名串一次性录入。此录入长度可支持 256 字节，或者根据需求进行自定义。如果输入错误，可使用后退键除去错误输入，如果要除去一行或全部输入，可按住后退键 2 秒，之后将清空某一行或全部客户输入，此操作可根据需求对输入单元进行自定义。输入单元最终将客户输入的交易信息传递给处理单元。短签名内容可以使用账号和金额，也可是后台随机从上述内容中选取的某些局部数字，亦或可以提示对交易验证码进行短签名；对于本交易，优先推荐对交易转出账号和金额进行签名；

[0052] 步骤 S310，客户在身份认证装置输入完成后，再按 SIGN 键，输入单元指令处理单元进行短签名。首先从存储单元中获取客户密钥和 SIGN 密码算法，并获取当前干扰因子，根据当前干扰因子、客户密钥和输入的交易元素，按照 SIGN 密码算法计算生成短签名密码的校验码；

[0053] 步骤 S311，将输入的 SIGN 密码与校验码进行比对，如果一致，则通过显示单元提供给客户验证成功，否则验证失败。

[0054] 为支持客户使用此认证装置，需要在服务方部署动态密码管理系统，用于客户密钥产生、存储、使用、作废、冻结、解冻等生命周期管理，提供动态密码校验、错误累计功能，提供干扰因子同步功能，提供查询、统计、监控等功能。

[0055] 身份认证装置对 OTP 和 SIGN 密码校验时，如果正确则记录下来，当前干扰因子以后不可再使用；如果错误，则进行错误累计，可进行密码错误日累计或历史累计。

[0056] 在 SIGN 工作模式中，干扰因子参与运算，可使相同交易元素的短签名密码每次都不同，避免交易密码重发风险。

[0057] OTP 工作模式和 SIGN 工作模式都可用于身份鉴别和交易认证，不局限于上述场景。例如，OTP 工作模式和 SIGN 工作模式可用于验证服务器端身份，当客户登录系统时，动态密码管理系统后台首先使用 OTP 或者 SIGN 工作模式计算出一个密码，并显示或传递给客户，客户通过自己的认证装置可同样获得当前的密码，如果密码同服务器一致，说明服务器是真实的，不是钓鱼网站或电话欺诈。当使用 SIGN 工作模式时，也可不针对交易数据，而是使用约定好的某个信息，如当前交易验证码，或者预留在服务器端的信息进行短签名。优先推荐使用 OTP 工作模式进行客户或者服务器的身份鉴别，使用 SIGN 工作模式进行交易短签名。

[0058] 身份认证装置有 PIN 码保护，使用时，必须输入正确的 PIN 码才能进行后续操作。

[0059] 身份认证装置出厂时没有 PIN 码，客户拿到后第一次使用时，强制客户必须设置

PIN 码。例如，客户第一次使用时，按开关键开启装置，装置提示客户设置 PIN 码，客户通过数字键盘设置 6 位 PIN 码，并重新输入一次，此装置校验一致，则 PIN 码设置成功。

[0060] 身份认证装置支持 PIN 码修改，客户按装置开关键启动，输入 PIN 码进入功能选择菜单，客户按 PIN 键进入 PIN 码修改功能，客户使用数字键盘设置 6 位新 PIN 码，并重新输入一次，装置校验一致，则 PIN 码修改成功。

[0061] 身份认证装置支持 PIN 码重置，当客户遗忘 PIN 码时，需要到柜面处理，装置提供使用挑战应答方式的 PIN 码重置功能。在柜面，客户按此装置开关键开启，按 2 秒 PIN 键，此时装置根据当前干扰因子，和特定 PIN 重置算法得到 PIN 重置挑战值，如 6 位数字，客户将这 6 位挑战告知柜员，柜员在系统中录入，后台系统根据此挑战，客户当前干扰因子、客户密钥计算 PIN 重置应答，应答也可是 6 位数字，返回柜员终端，柜员通过打印密码信封，或者口头告知客户，客户在认证装置上输入此 PIN 重置应答码，装置校验正确后，将装置重置为无 PIN 码状态，或者重置为某个默认值。

[0062] 身份认证装置中的干扰因子可采用时钟晶振或者事件计数器，优先推荐时钟晶振，上述干扰因子可能受到环境和人为因素的影响，造成同服务器端记录的不一致。如温度过高或过低造成时钟晶振不准，人为试用事件型 OTP 而未与后台校验，造成此装置和服务器端计数不一致。当出现上述情况时，需要对装置干扰因子进行同步处理。

[0063] 客户可到柜面进行同步，客户使用此装置连续产生两个 OTP 密码，并告知柜员提交后台，后台根据客户提交的两个密码在干扰因子的一定变动范围内进行匹配，例如时钟晶振则在正负 24 小时内试算 OTP 密码，如果是事件计数则在正负 50 范围内试算 OTP 密码，只要能够匹配上客户连续输入的两个密码，即可定位装置干扰因子当前计数，调整服务器端记录，完成装置同步。上述匹配窗口可根据需求进行自定义。

[0064] 身份认证装置大小如同银行卡，易于携带，同时可根据需求进行灵活的外观定制。装置的工作处于低功耗状态，其电量可有效保证装置使用 3 年以上，当电量耗尽或者到达有效期时，客户可更换一个新的装置，新装置采用新的客户密钥。

[0065] 各种电子渠道可利用此装置进行身份鉴别和交易认证，如果配合原渠道的静态密码一起使用，将能够实现双因子认证，保证客户交易安全。

[0066] 本发明通过交易短签名的实现方式，将交易元素参与到密码生成过程中，使得此密码只能用于此交易，如果篡改交易或者用此密码去做其他交易，服务器端都无法验证通过；通过短签名保证了交易数据的不可篡改，同时也起到了交易不可抵赖的作用，提高了交易认证的安全性。本发明身份认证装置为脱机使用，无需和手机、电话、计算机进行连接，此种脱机使用的方式，一是使得装置可适用于多个电子渠道，为多个渠道使用同一认证介质提供了基础。二是改善了认证介质的易用性，降低了装置使用难度，无需安装驱动和控件程序。本发明身份认证装置及系统可用于验证网上银行后台服务器端身份，同时支持 OTP 和 SIGN 两种工作模式。本发明认证装置提供 PIN 码保护，避免因身份认证装置丢失而造成的风险。支持 PIN 码的修改和重置。

[0067] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

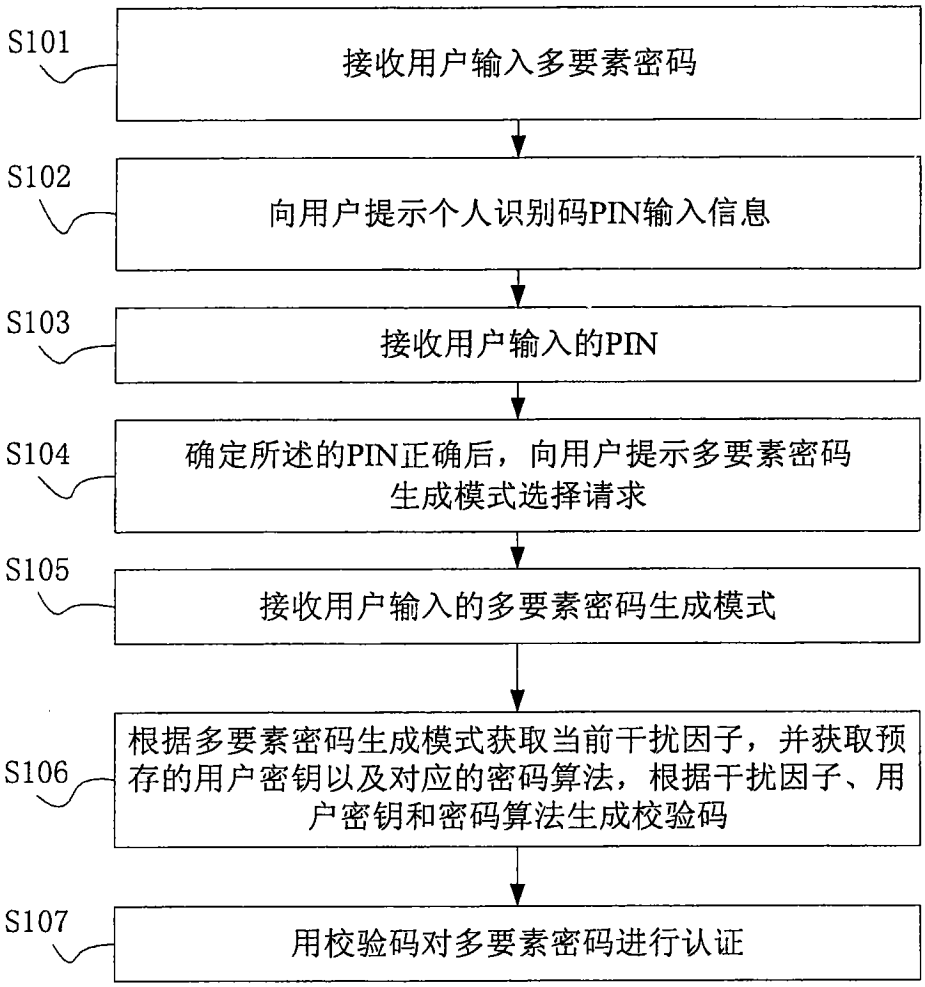

S101
接收用户输入多要素密码
S102
向用户提示个人识别码PIN输入信息
S103
接收用户输入的PIN
S104
确定所述的PIN正确后，向用户提示多要素密码生成模式选择请求
S105
接收用户输入的多要素密码生成模式
S106
根据多要素密码生成模式获取当前干扰因子，并获取预存的用户密钥以及对应的密码算法，根据干扰因子、用户密钥和密码算法生成校验码
S107
用校验码对多要素密码进行认证

图 1

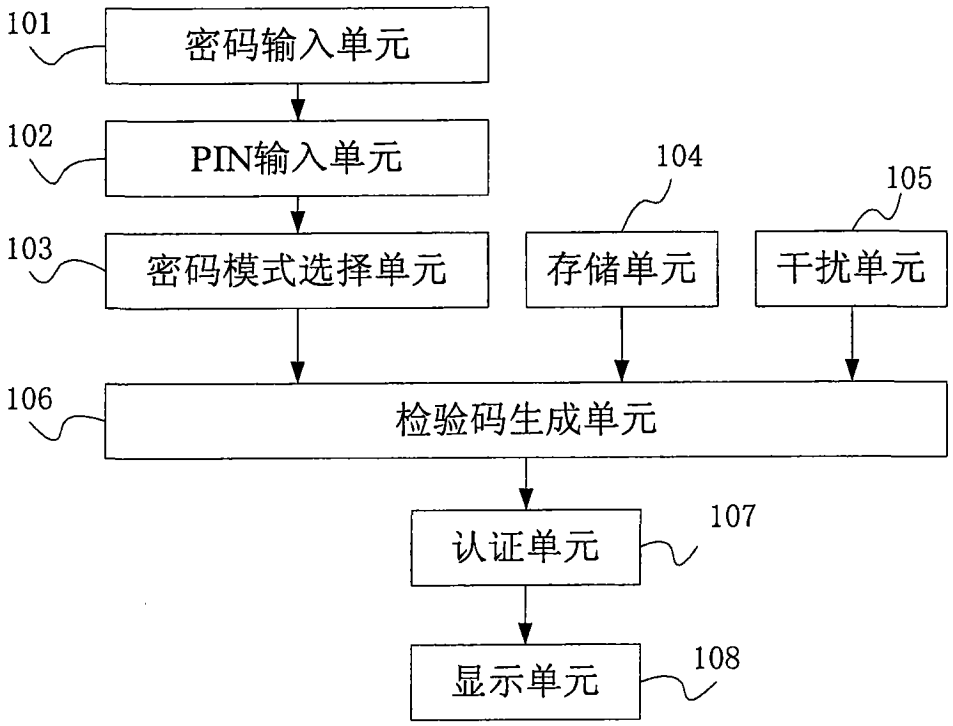

101
密码输入单元
102
PIN输入单元
103
密码模式选择单元
104
存储单元
105
干扰单元
106
检验码生成单元
107
认证单元
108
显示单元

图 2

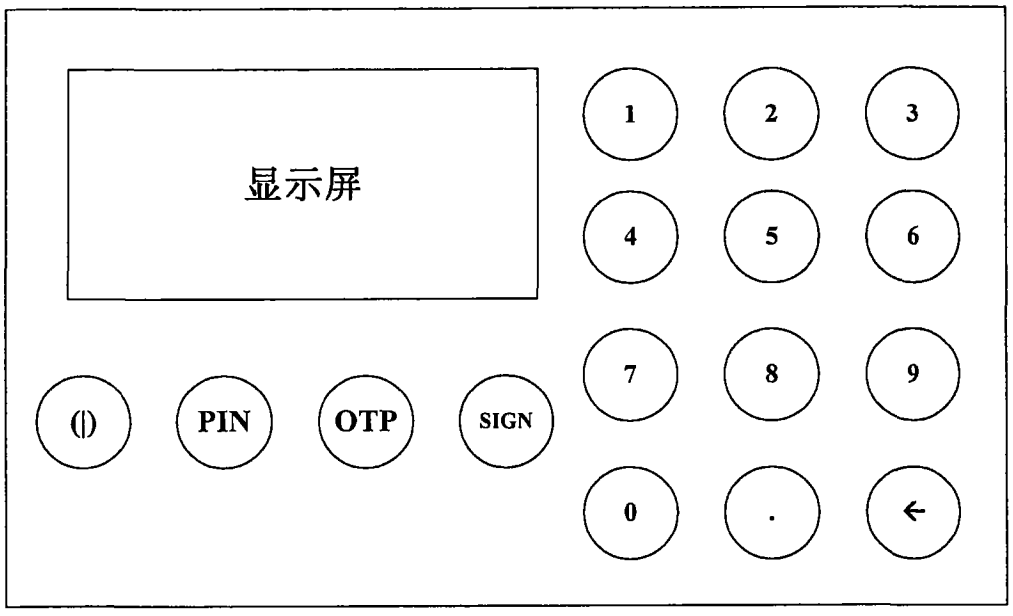

显示屏
1
2
3
4
5
6
7
8
9
0
.
PIN
OTP
SIGN

图 3

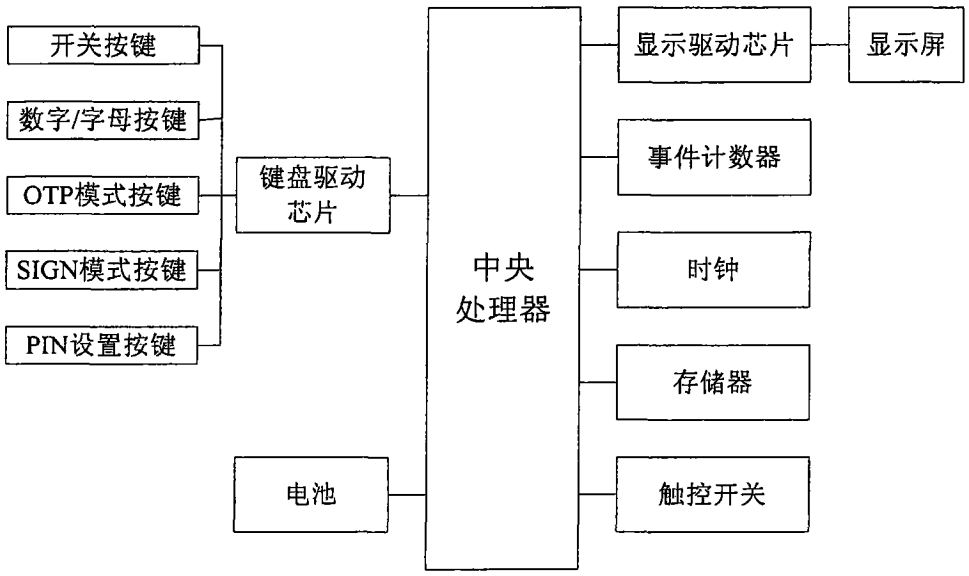

开关按键
数字/字母按键
OTP模式按键
SIGN模式按键
PIN设置按键
键盘驱动芯片
中央处理器
显示驱动芯片
显示屏
事件计数器
时钟
存储器
触控开关
电池

图 4

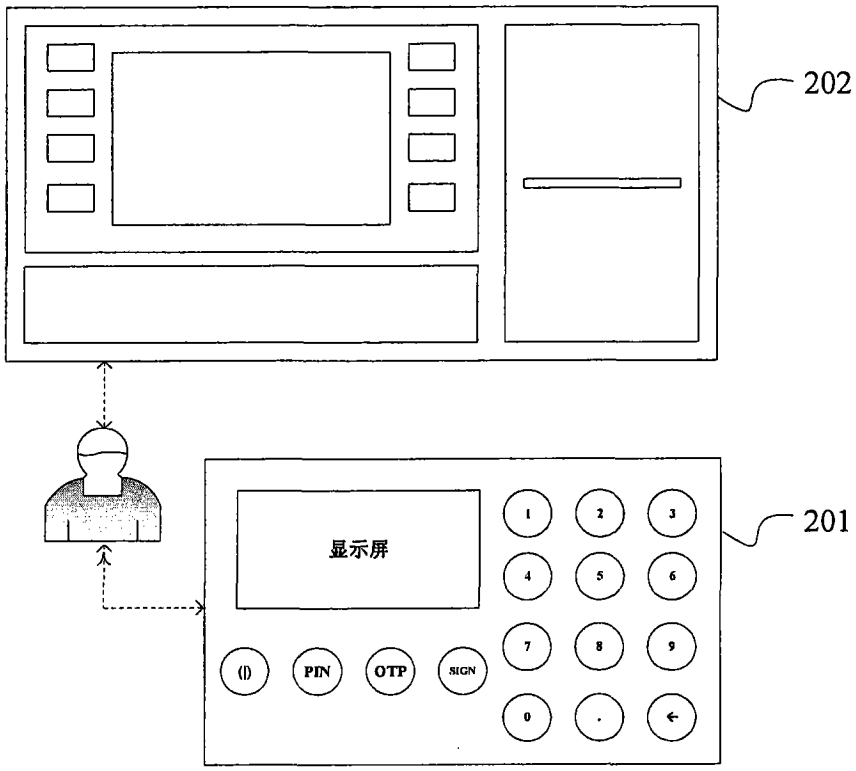

202
201
显示屏
PIN
OTP
SIGN

图 5

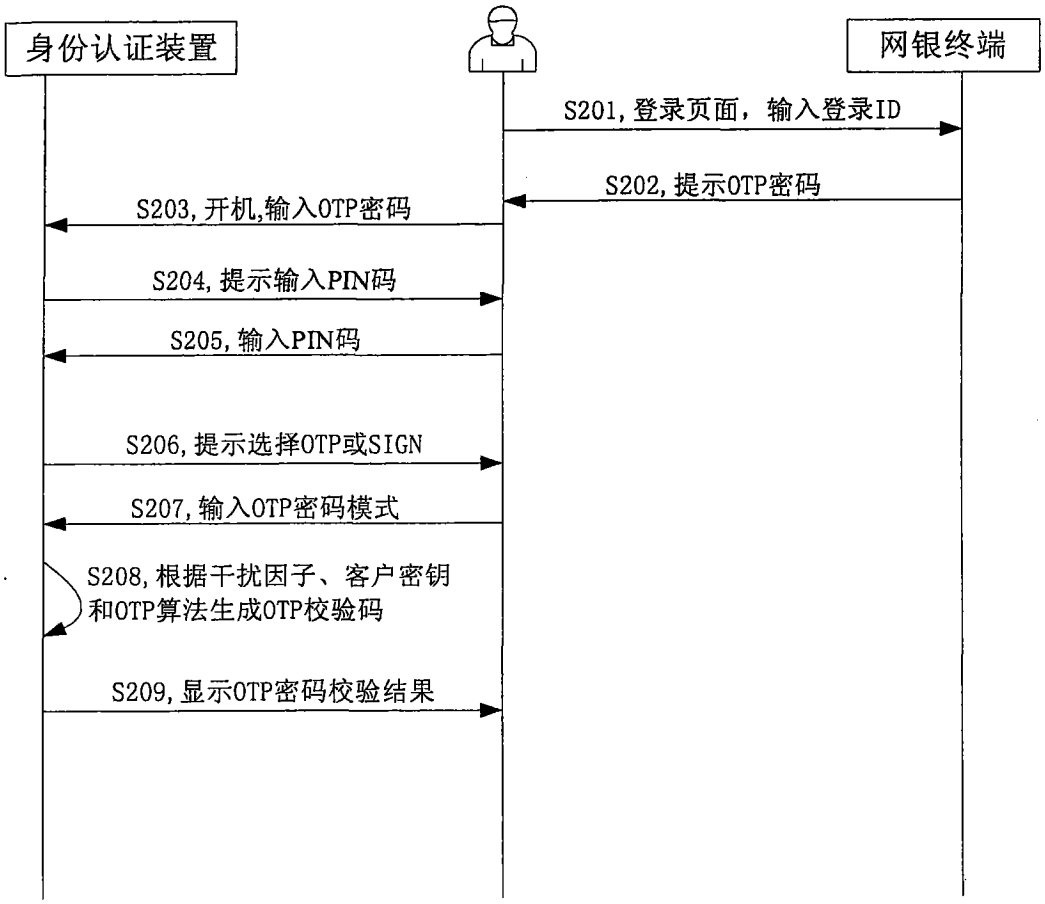

身份认证装置
网银终端
S201, 登录页面，输入登录ID
S202, 提示OTP密码
S203, 开机,输入OTP密码
S204, 提示输入PIN码
S205, 输入PIN码
S206, 提示选择OTP或SIGN
S207, 输入OTP密码模式
S208, 根据干扰因子、客户密钥
和OTP算法生成OTP校验码
S209, 显示OTP密码校验结果

图 6

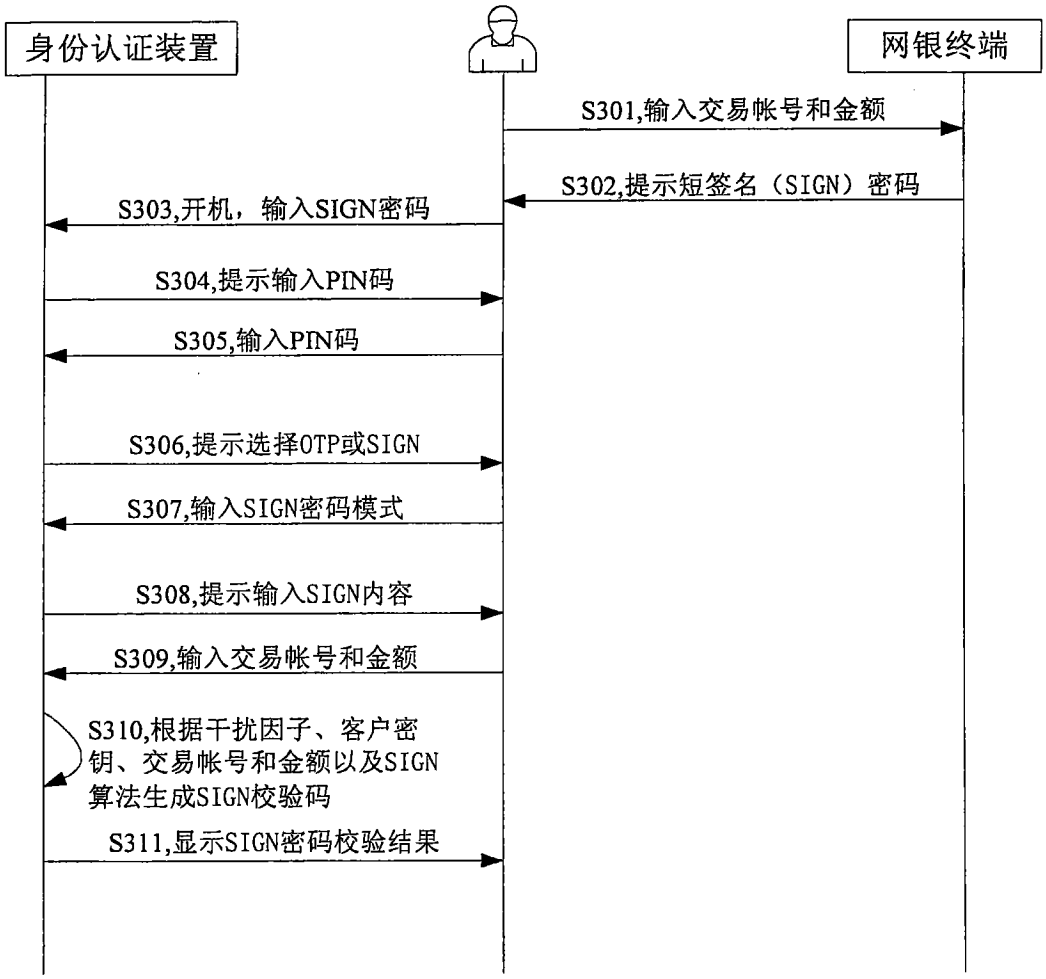

身份认证装置
网银终端
S301,输入交易帐号和金额
S302,提示短签名（SIGN）密码
S303,开机，输入SIGN密码
S304,提示输入PIN码
S305,输入PIN码
S306,提示选择OTP或SIGN
S307,输入SIGN密码模式
S308,提示输入SIGN内容
S309,输入交易帐号和金额
S310,根据干扰因子、客户密钥、交易帐号和金额以及SIGN算法生成SIGN校验码
S311,显示SIGN密码校验结果

图 7