(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104363589 A
(43)申请公布日 2015.02.18

(21)申请号 201410751075.3

(22)申请日 2014.12.09

(71)申请人 北京大唐智能卡技术有限公司
地址 100094 北京市海淀区永嘉北路 6 号

(72)发明人 石春光 郑辉 张靖

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 李红爽 栗若木

(51)Int.Cl.
H04W 12/06(2009.01)
H04L 29/06(2006.01)

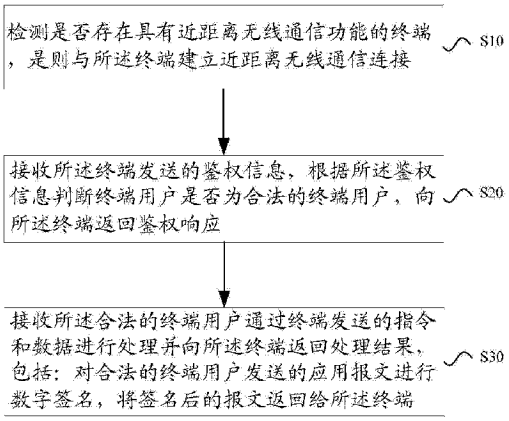
权利要求书3页 说明书7页 附图2页

(54)发明名称

一种身份认证的方法、装置和终端

(57)摘要

本发明公开了一种身份认证的方法，应用于内置有存储器的身份认证装置，包括：检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接；接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，向所述终端返回鉴权响应；接收所述合法的终端用户通过所述终端发送的指令和数据进行处理并向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端。本发明能够通过保存有合法用户身份信息的身份认证装置辅助终端上的应用进行用户身份认证，提高了终端应用的安全性。本发明还公开了一种身份认证的装置和具有身份认证功能的终端。



CN 104363589 A

1. 一种身份认证的方法，应用于内置有存储器的身份认证装置，包括：

检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接；

接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，向所述终端返回鉴权响应；

接收所述合法的终端用户通过所述终端发送的指令和数据进行处理并向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端。

2. 如权利要求 1 所述的方法，其特征在于：

所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

3. 如权利要求 1 所述的方法，其特征在于：

接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，包括：

接收终端用户通过所述终端发送的口令密码，将接收到的所述口令密码与所述存储器中预先保存的口令密码进行比对，如果一致则判断所述终端用户为合法的终端用户。

4. 如权利要求 1 所述的方法，其特征在于：

对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端，包括：

从存储器中读取所述合法的终端用户的密钥信息，根据所述密钥信息对所述应用报文进行数字签名，将签名后的报文返回给所述终端。

5. 如权利要求 1 所述的方法，其特征在于：

所述应用报文包括以下任意一种或多种：网上银行应用报文、网络运营商的电子支付应用报文、或需要实名认证的互联网应用报文。

6. 一种身份认证的方法，应用于具有近距离无线通信功能的终端，包括：

应用启动后，检测是否存在具有近距离无线通信功能的身份认证装置，是则与所述身份认证装置建立近距离无线通信连接；

将终端用户的鉴权信息发送给所述身份认证装置，接收所述身份认证装置返回的鉴权响应；

如鉴权通过，则向所述身份认证装置发送指令和数据，接收所述身份认证装置返回的处理结果，认证终端用户的身份。

7. 如权利要求 6 所述的方法，其特征在于：

所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

8. 如权利要求 6 所述的方法，其特征在于：

将终端用户的鉴权信息发送给所述身份认证装置，包括：接收终端用户输入的口令密码并将其发送给所述身份认证装置。

9. 如权利要求 6 所述的方法，其特征在于：

向所述身份认证装置发送指令和数据，接收所述身份认证装置返回的处理结果，认证终端用户的身份，包括：

向所述身份认证装置发送应用报文；

接收所述身份认证装置返回的经过数字签名后的应用报文，对所述数字签名进行验签，根据验签结果认证终端用户的身份。

10. 如权利要求 6 所述的方法，其特征在于：

所述应用包括以下任意一种或多种：网上银行应用、网络运营商的电子支付应用、或需要实名认证的互联网应用。

11. 一种身份认证装置，内置有存储器，包括：

近距离无线通信模块，用于检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接；接收所述终端发送的鉴权信息并转发给安全主控模块，接收所述安全主控模块返回的鉴权响应并转发给所述终端；接收所述合法的终端用户通过所述终端发送的指令和数据并转发给安全主控模块，接收所述安全主控模块返回的处理结果并转发给所述终端；

安全主控模块，用于接收所述鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，返回鉴权响应；接收来自终端的指令和数据进行处理并通过所述近距离无线通信模块向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端。

12. 如权利要求 11 所述的身份认证装置，其特征在于：

所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

13. 如权利要求 11 所述的身份认证装置，其特征在于：

所述安全主控模块，用于接收所述鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，包括：

接收终端用户通过所述终端发送的口令密码，将接收到的口令密码与存储器中预先保存的口令密码进行比对，如果一致则判断所述终端用户为合法的终端用户。

14. 如权利要求 11 所述的身份认证装置，其特征在于：

所述安全主控模块，用于对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端，包括：

从存储器中读取所述合法的终端用户的密钥信息，根据所述密钥信息对所述应用报文进行数字签名，将签名后的报文返回给所述终端。

15. 如权利要求 11 所述的身份认证装置，其特征在于：

所述安全主控模块，还用于对所述合法的终端用户的密钥信息进行管理，根据所述密钥信息对接收到的来自终端的数据进行解密、对发送给终端的数据进行加密。

16. 一种具有身份认证功能的终端，包括：

应用模块，用于应用启动后通知安全管理模块；如终端用户通过了身份认证装置的鉴权，则向安全管理模块发送指令和数据；

近距离无线通信模块，用于根据安全管理模块的指示检测是否存在具有近距离无线通信功能的身份认证装置，是则与所述身份认证装置建立近距离无线通信连接；在终端与身份认证装置之间传输数据；

安全管理模块，用于指示近距离无线通信模块与身份认证装置建立连接，如连接建立成功，则将终端用户的鉴权信息通过所述近距离无线通信模块发送给所述身份认证装置，接收所述身份认证装置返回的鉴权响应，将鉴权结果通知给所述应用模块；接收所述应用

模块发送的指令和数据并通过所述近距离无线通信模块转发给所述身份认证装置，接收所述身份认证装置返回的处理结果，认证终端用户的身份。

17. 如权利要求 16 所述的终端，其特征在于：

所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

18. 如权利要求 16 所述的终端，其特征在于：

安全管理模块，用于将终端用户的鉴权信息通过所述近距离无线通信模块发送给所述身份认证装置，包括：

接收终端用户输入的口令密码并将其通过所述近距离无线通信模块发送给所述身份认证装置。

19. 如权利要求 16 所述的终端，其特征在于：

安全管理模块，用于接收所述应用模块发送的指令和数据并通过所述近距离无线通信模块转发给所述身份认证装置，接收所述身份认证装置返回的处理结果，认证终端用户的身份，包括：

接收所述应用模块发送的应用报文，并通过所述近距离无线通信模块转发给所述身份认证装置；

接收所述身份认证装置返回的经过数字签名后的应用报文，对所述数字签名进行验签，根据验签结果认证终端用户的身份。

20. 如权利要求 16 所述的终端，其特征在于：

所述应用包括以下任意一种或多种：网上银行应用、网络运营商的电子支付应用、或需要实名认证的互联网应用。

一种身份认证的方法、装置和终端

技术领域

[0001] 本发明涉及通信领域，尤其涉及的是一种身份认证的方法、装置和终端。

背景技术

[0002] 随着全球信息化普及程度的提高，移动互联网已经成为与人们日常生活密不可分的重要一部分，而智能手机的日益普及又大大提升了接入互联网的方便程度。随着互联网的发展，用户在进行网上通信和交易时，其信息安全日益受到了网上黑客、网络监控设备、病毒及其它形式的威胁。这些威胁带来的各种损失已经成为使用成本的重要组成部分。

[0003] 为了保证移动互联网上通信和交易的安全性，需要加强对用户身份的验证。

发明内容

[0004] 本发明所要解决的技术问题是提供一种身份认证的方法、装置和终端，能够通过保存有合法用户身份信息的身份认证装置辅助终端上的应用进行用户身份认证，提高了终端应用的安全性。

[0005] 为了解决上述技术问题，本发明提供了一种身份认证的方法，应用于内置有存储器的身份认证装置，包括：

[0006] 检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接；

[0007] 接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，向所述终端返回鉴权响应；

[0008] 接收所述合法的终端用户通过所述终端发送的指令和数据进行处理并向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端。

[0009] 进一步地，该方法还包括下述特点：

[0010] 所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

[0011] 进一步地，该方法还包括下述特点：

[0012] 接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，包括：

[0013] 接收终端用户通过所述终端发送的口令密码，将接收到的所述口令密码与所述存储器中预先保存的口令密码进行比对，如果一致则判断所述终端用户为合法的终端用户。

[0014] 进一步地，该方法还包括下述特点：

[0015] 对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端，包括：

[0016] 从存储器中读取所述合法的终端用户的密钥信息，根据所述密钥信息对所述应用报文进行数字签名，将签名后的报文返回给所述终端。

[0017] 进一步地，该方法还包括下述特点：

[0018] 所述应用报文包括以下任意一种或多种：网上银行应用报文、网络运营商的电子支付应用报文、或需要实名认证的互联网应用报文。

[0019] 为了解决上述技术问题，本发明还提供了一种身份认证的方法，应用于具有近距离无线通信功能的终端，包括：

[0020] 应用启动后，检测是否存在具有近距离无线通信功能的身份认证装置，是则与所述身份认证装置建立近距离无线通信连接；

[0021] 将终端用户的鉴权信息发送给所述身份认证装置，接收所述身份认证装置返回的鉴权响应；

[0022] 如鉴权通过，则向所述身份认证装置发送指令和数据，接收所述身份认证装置返回的处理结果，认证终端用户的身份。

[0023] 进一步地，该方法还包括下述特点：

[0024] 所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

[0025] 进一步地，该方法还包括下述特点：

[0026] 将终端用户的鉴权信息发送给所述身份认证装置，包括：接收终端用户输入的口令密码并将其发送给所述身份认证装置。

[0027] 进一步地，该方法还包括下述特点：

[0028] 向所述身份认证装置发送指令和数据，接收所述身份认证装置返回的处理结果，认证终端用户的身份，包括：

[0029] 向所述身份认证装置发送应用报文；

[0030] 接收所述身份认证装置返回的经过数字签名后的应用报文，对所述数字签名进行验签，根据验签结果认证终端用户的身份。

[0031] 进一步地，该方法还包括下述特点：

[0032] 所述应用包括以下任意一种或多种：网上银行应用、网络运营商的电子支付应用、或需要实名认证的互联网应用。

[0033] 为了解决上述技术问题，本发明还提供了一种身份认证装置，内置有存储器，包括：

[0034] 近距离无线通信模块，用于检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接；接收所述终端发送的鉴权信息并转发给安全主控模块，接收所述安全主控模块返回的鉴权响应并转发给所述终端；接收所述合法的终端用户通过所述终端发送的指令和数据并转发给安全主控模块，接收所述安全主控模块返回的处理结果并转发给所述终端；

[0035] 安全主控模块，用于接收所述鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，返回鉴权响应；接收来自终端的指令和数据进行处理并通过所述近距离无线通信模块向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端。

[0036] 进一步地，该身份认证装置还包括下述特点：

[0037] 所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

[0038] 进一步地，该身份认证装置还包括下述特点：

[0039] 所述安全主控模块，用于接收所述鉴权信息，根据所述鉴权信息判断终端用户是

否为合法的终端用户，包括：

[0040] 接收终端用户通过所述终端发送的口令密码，将接收到的口令密码与存储器中预先保存的口令密码进行比对，如果一致则判断所述终端用户为合法的终端用户。

[0041] 进一步地，该身份认证装置还包括下述特点：

[0042] 所述安全主控模块，用于对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端，包括：

[0043] 从存储器中读取所述合法的终端用户的密钥信息，根据所述密钥信息对所述应用报文进行数字签名，将签名后的报文返回给所述终端。

[0044] 进一步地，该身份认证装置还包括下述特点：

[0045] 所述安全主控模块，还用于对所述合法的终端用户的密钥信息进行管理，根据所述密钥信息对接收到的来自终端的数据进行解密、对发送给终端的数据进行加密。

[0046] 为了解决上述技术问题，本发明还提供了一种具有身份认证功能的终端，包括：

[0047] 应用模块，用于应用启动后通知安全管理模块；如终端用户通过了身份认证装置的鉴权，则向安全管理模块发送指令和数据；

[0048] 近距离无线通信模块，用于根据安全管理模块的指示检测是否存在具有近距离无线通信功能的身份认证装置，是则与所述身份认证装置建立近距离无线通信连接；在终端与身份认证装置之间传输数据；

[0049] 安全管理模块，用于指示近距离无线通信模块与身份认证装置建立连接，如连接建立成功，则将终端用户的鉴权信息通过所述近距离无线通信模块发送给所述身份认证装置，接收所述身份认证装置返回的鉴权响应，将鉴权结果通知给所述应用模块；接收所述应用模块发送的指令和数据并通过所述近距离无线通信模块转发给所述身份认证装置，接收所述身份认证装置返回的处理结果，认证终端用户的身份。

[0050] 进一步地，该终端还包括下述特点：

[0051] 所述近距离无线通信连接，包括：近场通信连接或蓝牙连接。

[0052] 进一步地，该终端还包括下述特点：

[0053] 安全管理模块，用于将终端用户的鉴权信息通过所述近距离无线通信模块发送给所述身份认证装置，包括：

[0054] 接收终端用户输入的口令密码并将其通过所述近距离无线通信模块发送给所述身份认证装置。

[0055] 进一步地，该终端还包括下述特点：

[0056] 安全管理模块，用于接收所述应用模块发送的指令和数据并通过所述近距离无线通信模块转发给所述身份认证装置，接收所述身份认证装置返回的处理结果，认证终端用户的身份，包括：

[0057] 接收所述应用模块发送的应用报文，并通过所述近距离无线通信模块转发给所述身份认证装置；

[0058] 接收所述身份认证装置返回的经过数字签名后的应用报文，对所述数字签名进行验签，根据验签结果认证终端用户的身份。

[0059] 进一步地，该终端还包括下述特点：

[0060] 所述应用包括以下任意一种：网上银行应用、网络运营商的电子支付应用、或需要

实名认证的互联网应用。

[0061] 与现有技术相比，本发明提供的一种身份认证的方法、装置和终端，通过保存有合法用户身份信息的身份认证装置辅助终端上的应用进行用户身份认证，提高了终端应用的安全性。

附图说明

[0062] 图 1 为本发明实施例的一种身份认证的方法（装置侧）的流程图。

[0063] 图 2 为本发明实施例的一种身份认证的方法（终端侧）的流程图。

[0064] 图 3 为本发明实施例的一种身份认证装置的结构示意图。

[0065] 图 4 为本发明实施例的一种具有身份认证功能的终端的结构示意图。

具体实施方式

[0066] 为使本发明的目的、技术方案和优点更加清楚明白，下文中将结合附图对本发明的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0067] 如图 1 所示，本发明实施例提供了一种身份认证的方法，应用于内置有存储器的身份认证装置，包括：

[0068] S10，检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接；

[0069] S20，接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，向所述终端返回鉴权响应；

[0070] S30，接收所述合法的终端用户通过所述终端发送的指令和数据进行处理并向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端。

[0071] 该方法进一步包括下述特点：

[0072] 优选地，所述近距离无线通信连接，包括：近场通信 (Near Field Communication，NFC) 连接或蓝牙连接。

[0073] 其中，NFC 是一种短距高频的无线电技术，在 13.56MHz 频率运行于 20 厘米距离内。NFC 接口包括了索尼公司的 FeliCaTM 标准，以及 ISO 14443A，B，和飞利浦的 MIFARE 标准，即在业界简称为 TypeA，TypeB 和 TypeF，其中 A、B 为 Mifare 标准，F 为 Felica 标准。

[0074] 优选地，接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，包括：

[0075] 接收终端用户通过所述终端发送的口令密码，将接收到的所述口令密码与所述存储器中预先保存的口令密码进行比对，如果一致则判断所述终端用户为合法的终端用户。

[0076] 其中，所述口令密码为所述身份认证装置的个人识别码 (Personal Identification Number，PIN)。

[0077] 优选地，向终端返回鉴权响应，包括：将接收到的所述口令密码与所述存储器中预先保存的口令密码进行比对，如果一致则判断所述终端用户为合法的终端用户，向终端返回鉴权通过的响应，如果不一致则判断所述终端用户为非法的终端用户，向终端返回鉴权

失败的响应。

[0078] 优选地，对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端，包括：

[0079] 从存储器中读取所述合法的终端用户的密钥信息，根据所述密钥信息对所述应用报文进行数字签名，将签名后的报文返回给所述终端。

[0080] 优选地，所述应用报文包括以下任意一种或多种：网上银行应用报文、网络运营商的电子支付应用报文、或需要实名认证的互联网应用报文。

[0081] 其中，网络运营商的电子支付应用，比如：支付宝、微信等。需要实名认证的互联网应用，比如，网络购票应用等。

[0082] 所述具有近距离无线通信功能的终端为：具有近距离无线通信功能的移动终端、或 PC。

[0083] 如图 2 所示，本发明实施例提供了一种身份认证的方法，应用于具有近距离无线通信功能的终端，包括：

[0084] S10，应用启动后，检测是否存在具有近距离无线通信功能的身份认证装置，是则与所述身份认证装置建立近距离无线通信连接；

[0085] S20，将终端用户的鉴权信息发送给所述身份认证装置，接收所述身份认证装置返回的鉴权响应；

[0086] S30，如鉴权通过，则向所述身份认证装置发送指令和数据，接收所述身份认证装置返回的处理结果，认证终端用户的身份。

[0087] 所述方法还包括下述特点：

[0088] 优选地，所述近距离无线通信连接，包括：近场通信 (Near Field Communication，NFC) 连接或蓝牙连接。

[0089] 优选地，所述应用包括以下任意一种或多种：网上银行应用、网络运营商的电子支付应用、或需要实名认证的互联网应用。

[0090] 优选地，将终端用户的鉴权信息发送给所述身份认证装置，包括：接收终端用户输入的口令密码并将其发送给所述身份认证装置。

[0091] 其中，所述口令密码为所述身份认证装置的个人识别码 (Personal Identification Number，PIN)。

[0092] 优选地，向所述身份认证装置发送指令和数据，接收所述身份认证装置返回的处理结果，认证终端用户的身份，包括：

[0093] 向所述身份认证装置发送应用报文；

[0094] 接收所述身份认证装置返回的经过数字签名后的应用报文，对所述数字签名进行验签，根据验签结果认证终端用户的身份。

[0095] 比如，终端用户（比如，张三）在终端上启动网上银行应用，在确认支付前，需要使用身份认证装置为该支付请求进行数字签名，远程服务器端收到携带数字签名的支付请求后，通过验签获知终端用户为“张三”，从而实现了对终端用户的身份认证。

[0096] 优选地，具有近距离无线通信功能的终端为：具有近距离无线通信功能的移动终端，或者 PC。

[0097] 如图 3 所示，本发明实施例提供了一种身份认证装置，内置有存储器，包括：

[0098] 近距离无线通信模块，用于检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接；接收所述终端发送的鉴权信息并转发给安全主控模块，接收所述安全主控模块返回的鉴权响应并转发给所述终端；接收所述合法的终端用户通过所述终端发送的指令和数据并转发给安全主控模块，接收所述安全主控模块返回的处理结果并转发给所述终端；

[0099] 安全主控模块，用于接收所述鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，返回鉴权响应；接收来自终端的指令和数据进行处理并通过所述近距离无线通信模块向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端。

[0100] 所述身份认证装置还包括下述特点：

[0101] 优选地，所述近距离无线通信连接，包括：近场通信(Near Field Communication，NFC)连接或蓝牙连接。

[0102] 优选地，所述安全主控模块，用于接收所述鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，包括：

[0103] 接收终端用户通过所述终端发送的口令密码，将接收到的口令密码与存储器中预先保存的口令密码进行比对，如果一致则判断所述终端用户为合法的终端用户。

[0104] 其中，所述口令密码为所述身份认证装置的个人识别码(Personal Identification Number，PIN)。

[0105] 优选地，所述安全主控模块，用于对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端，包括：

[0106] 从存储器中读取所述合法的终端用户的密钥信息，根据所述密钥信息对所述应用报文进行数字签名，将签名后的报文返回给所述终端。

[0107] 优选地，所述安全主控模块，还用于对所述合法的终端用户的密钥信息进行管理，根据所述密钥信息对接收到的来自终端的数据进行解密、对发送给终端的数据进行加密。

[0108] 优选地，所述应用报文包括以下任意一种或多种：网上银行应用报文、网络运营商的电子支付应用报文、或需要实名认证的互联网应用报文。

[0109] 所述具有近距离无线通信功能的终端为：具有近距离无线通信功能的移动终端、或PC。

[0110] 所述身份认证装置内嵌存储器（存储单元），存储单元内部的数据存储介质可以是Nand Flash存储器、Nor Flash存储器或者其他任意适合嵌入式应用的存储器。所述安全主控模块全权控制存储单元的读写操作，没有旁路机制。

[0111] 如图4所示，本发明实施例提供了一种具有身份认证功能的终端，包括：

[0112] 应用模块，用于应用启动后通知安全管理模块；如终端用户通过了身份认证装置的鉴权，则向安全管理模块发送指令和数据；

[0113] 近距离无线通信模块，用于根据安全管理模块的指示检测是否存在具有近距离无线通信功能的身份认证装置，是则与所述身份认证装置建立近距离无线通信连接；在终端与身份认证装置之间传输数据；

[0114] 安全管理模块，用于指示近距离无线通信模块与身份认证装置建立连接，如连接建立成功，则将终端用户的鉴权信息通过所述近距离无线通信模块发送给所述身份认证装

置，接收所述身份认证装置返回的鉴权响应，将鉴权结果通知给所述应用模块；接收所述应用模块发送的指令和数据并通过所述近距离无线通信模块转发给所述身份认证装置，接收所述身份认证装置返回的处理结果，认证终端用户的身份。

[0115] 所述终端还包括下述特点：

[0116] 优选地，所述近距离无线通信连接，包括：近场通信(Near Field Communication，NFC)连接或蓝牙连接。

[0117] 安全管理模块，用于将终端用户的鉴权信息通过所述近距离无线通信模块发送给所述身份认证装置，包括：

[0118] 接收终端用户输入的口令密码并将其通过所述近距离无线通信模块发送给所述身份认证装置；

[0119] 其中，所述口令密码为所述身份认证装置的个人识别码(Personal Identification Number，PIN)。

[0120] 优选地，安全管理模块，用于接收所述应用模块发送的指令和数据并通过所述近距离无线通信模块转发给所述身份认证装置，通过所述近距离无线通信模块接收所述身份认证装置返回的处理结果，认证终端用户的身份，包括：

[0121] 接收所述应用模块发送的应用报文，并通过所述近距离无线通信模块转发给所述身份认证装置；

[0122] 通过所述近距离无线通信模块接收所述身份认证装置返回的经过数字签名后的应用报文，对所述数字签名进行验签，根据验签结果认证终端用户的身份。

[0123] 优选地，所述应用包括以下任意一种或多种：网上银行应用、网络运营商的电子支付应用、或需要实名认证的互联网应用。

[0124] 上述实施例提供的一种身份认证的方法、装置和终端，通过保存有合法用户身份信息的身份认证装置辅助终端上的应用进行用户身份认证，提高了终端应用的安全性。

[0125] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现，相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

[0126] 需要说明的是，本发明还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员可根据本发明作出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

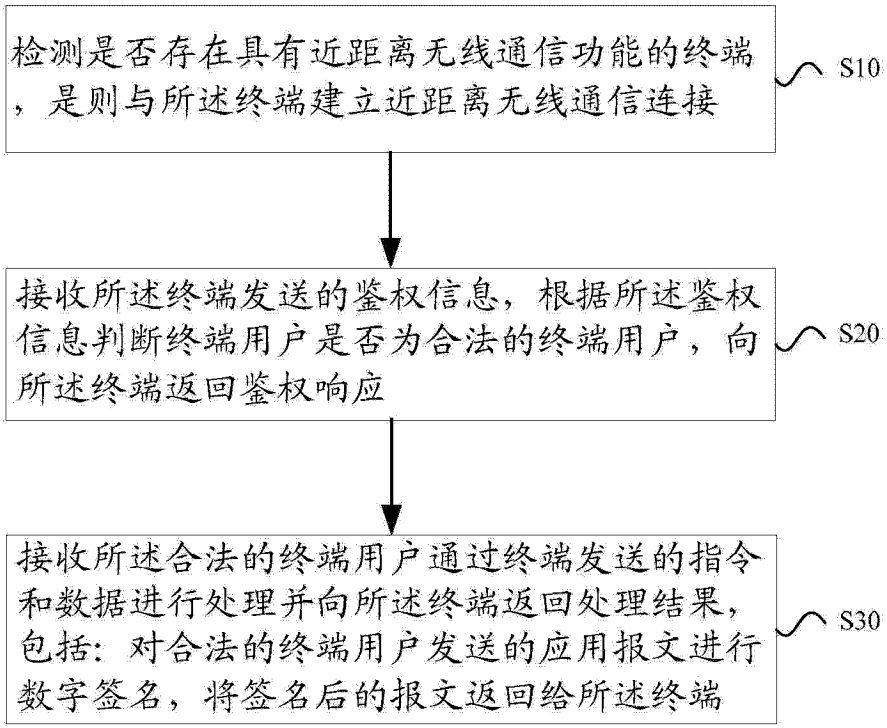

检测是否存在具有近距离无线通信功能的终端，是则与所述终端建立近距离无线通信连接
S10
接收所述终端发送的鉴权信息，根据所述鉴权信息判断终端用户是否为合法的终端用户，向所述终端返回鉴权响应
S20
接收所述合法的终端用户通过终端发送的指令和数据进行处理并向所述终端返回处理结果，包括：对合法的终端用户发送的应用报文进行数字签名，将签名后的报文返回给所述终端
S30

图 1

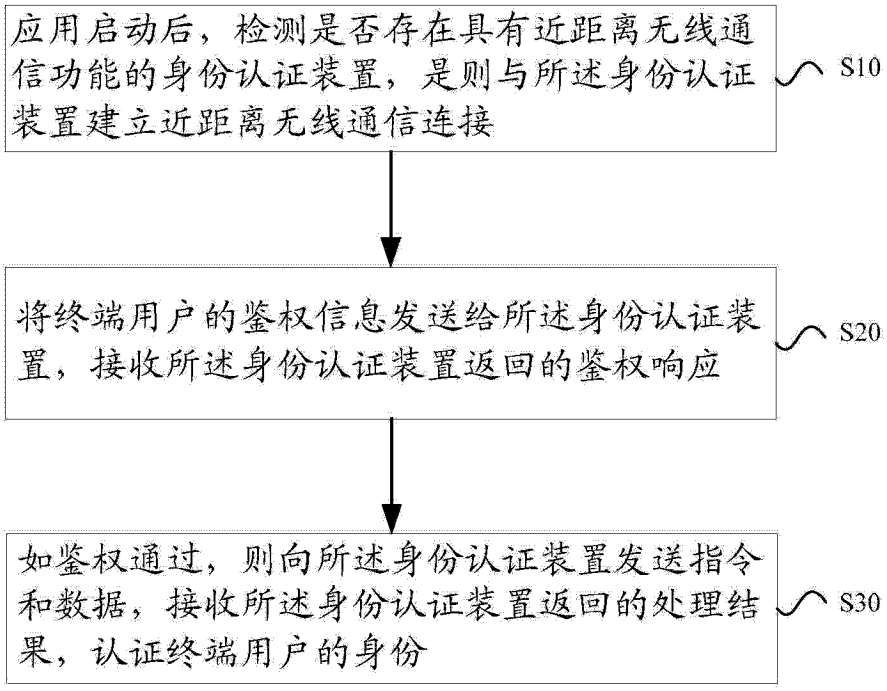

应用启动后，检测是否存在具有近距离无线通信功能的身份认证装置，是则与所述身份认证装置建立近距离无线通信连接
S10
将终端用户的鉴权信息发送给所述身份认证装置，接收所述身份认证装置返回的鉴权响应
S20
如鉴权通过，则向所述身份认证装置发送指令和数据，接收所述身份认证装置返回的处理结果，认证终端用户的身份
S30

图 2

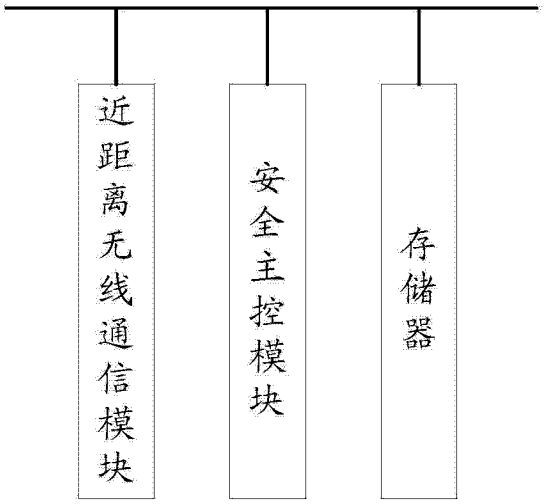


图 3

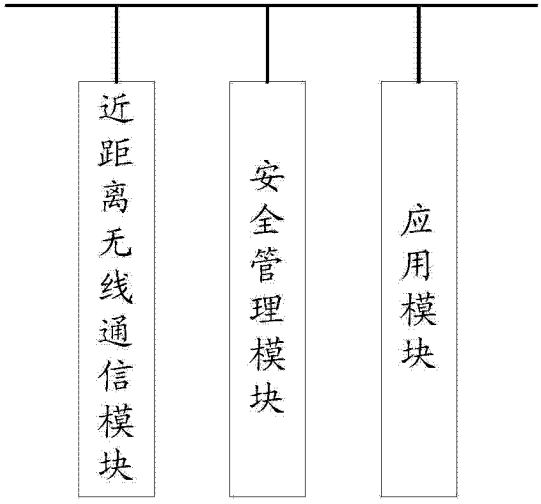


图 4