(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 206506540 U
(45)授权公告日 2017.09.19

(21)申请号 201620830744.0

(22)申请日 2016.08.02

(73)专利权人 天地融科技股份有限公司
地址 100083 北京市海淀区学清路38号B座1810

(72)发明人 李东声

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 29/06(2006.01)

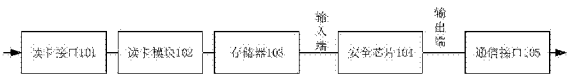
权利要求书3页 说明书8页 附图1页

(54)实用新型名称

一种智能密钥设备及业务办理系统

(57)摘要

本实用新型提供了一种智能密钥设备和业务办理系统，其中，智能密钥设备包括：读卡接口，读卡模块，存储器，安全芯片和通信接口，其中：读卡模块电连接在存储器与读卡接口之间，读卡模块，用于向读卡接口发送读卡指令，读卡接口，用于接收与读卡指令对应的第一数据，并将第一数据发送至读卡模块；读卡模块，还用于向存储器发送第一数据；存储器电连接在读卡模块与安全芯片的输入端之间，存储器，用于存储第一数据；安全芯片的输出端与通信接口电连接；安全芯片，用于接收存储器发送的第一数据，利用智能密钥设备的私钥对接收到的数据进行签名生成第二数据并向通信接口发送，其中，接收到的数据至少包括第一数据；通信接口，用于将第二数据外发。



CN 206506540 U

1.一种智能密钥设备，其特征在于，所述智能密钥设备包括：读卡接口，读卡模块，存储器，安全芯片和通信接口，其中：

所述读卡模块电连接在所述存储器与所述读卡接口之间，所述读卡模块，用于向所述读卡接口发送读卡指令，所述读卡接口，用于接收与所述读卡指令对应的第一数据，并将所述第一数据发送至所述读卡模块；所述读卡模块，还用于接收所述第一数据，并向所述存储器发送所述第一数据；

所述存储器电连接在所述读卡模块与所述安全芯片的输入端之间，所述存储器，用于接收所述第一数据，并存储所述第一数据；

所述安全芯片的输出端与所述通信接口电连接；所述安全芯片，用于接收所述存储器发送的所述第一数据，利用所述智能密钥设备的私钥对接收到的数据进行签名生成第二数据，并向所述通信接口发送所述第二数据，其中，所述接收到的数据至少包括所述第一数据；

所述通信接口，用于接收所述第二数据，并将所述第二数据外发。

2.根据权利要求1所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：二维码生成器和显示屏；

所述安全芯片的输出端还与所述二维码生成器的输入端电连接；所述安全芯片，还用于向所述二维码生成器发送所述第二数据；

所述二维码生成器的输出端与所述显示屏的输入端电连接；所述二维码生成器，用于根据所述第二数据生成二维码，并向所述显示屏发送所述二维码；

所述显示屏，用于接收所述二维码，并显示所述二维码。

3.根据权利要求1所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：输入接口；

所述输入接口，与所述安全芯片的输入端电连接，用于接收第三数据，并向所述安全芯片发送所述第三数据；

所述安全芯片，还用于接收所述第三数据；

其中，所述接收到的数据至少还包括所述第三数据。

4.根据权利要求2所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：输入接口；

所述输入接口，与所述安全芯片的输入端电连接，用于接收第三数据，并向所述安全芯片发送所述第三数据；

所述安全芯片，还用于接收所述第三数据；

其中，所述接收到的数据至少还包括所述第三数据。

5.根据权利要求3所述的智能密钥设备，其特征在于，

所述通信接口还与所述安全芯片的输入端电连接；所述通信接口，还用于接收第四数据，向所述安全芯片发送所述第四数据；

所述安全芯片，还用于接收所述第四数据；

其中，所述接收到的数据至少还包括所述第四数据。

6.根据权利要求4所述的智能密钥设备，其特征在于，

所述通信接口还与所述安全芯片的输入端电连接；所述通信接口，还用于接收第四数

据，向所述安全芯片发送所述第四数据；

所述安全芯片，还用于接收所述第四数据；

其中，所述接收到的数据至少还包括所述第四数据。

7.根据权利要求3至6任一项所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：时钟；

所述时钟，与所述安全芯片的输入端电连接，用于计时得到第五数据，并向所述安全芯片发送所述第五数据；

所述安全芯片，还用于接收所述第五数据；

其中，所述接收到的数据至少还包括所述第五数据。

8.根据权利要求3至6任一项所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：计数器；

所述计数器，与所述安全芯片的输入端电连接，用于计数得到第六数据，并向所述安全芯片发送所述第六数据；

所述安全芯片，还用于接收所述第六数据；

其中，所述接收到的数据至少还包括所述第六数据。

9.根据权利要求1至6任一项所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：指纹采集器和摄像头；

所述指纹采集器，与所述通信接口电连接，用于采集第七数据，并向所述通信接口发送所述第七数据；所述通信接口，还用于接收所述第七数据，并将所述第七数据外发；

所述摄像头，与所述通信接口电连接，用于采集第八数据，并向所述通信接口发送所述第八数据；所述通信接口，还用于接收所述第八数据，并将所述第八数据外发。

10.根据权利要求7所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：指纹采集器和摄像头；

所述指纹采集器，与所述通信接口电连接，用于采集第七数据，并向所述通信接口发送所述第七数据；所述通信接口，还用于接收所述第七数据，并将所述第七数据外发；

所述摄像头，与所述通信接口电连接，用于采集第八数据，并向所述通信接口发送所述第八数据；所述通信接口，还用于接收所述第八数据，并将所述第八数据外发。

11.根据权利要求8所述的智能密钥设备，其特征在于，所述智能密钥设备还包括：指纹采集器和摄像头；

所述指纹采集器，与所述通信接口电连接，用于采集第七数据，并向所述通信接口发送所述第七数据；所述通信接口，还用于接收所述第七数据，并将所述第七数据外发；

所述摄像头，与所述通信接口电连接，用于采集第八数据，并向所述通信接口发送所述第八数据；所述通信接口，还用于接收所述第八数据，并将所述第八数据外发。

12.根据权利要求1至6、10、11任一项所述的智能密钥设备，其特征在于，

所述读卡接口包括非接触式接口，所述通信接口包括有线接口或无线接口。

13.根据权利要求7所述的智能密钥设备，其特征在于，

所述读卡接口包括非接触式接口，所述通信接口包括有线接口或无线接口。

14.根据权利要求8所述的智能密钥设备，其特征在于，

所述读卡接口包括非接触式接口，所述通信接口包括有线接口或无线接口。

15.根据权利要求9所述的智能密钥设备，其特征在于，

所述读卡接口包括非接触式接口，所述通信接口包括有线接口或无线接口。

16.一种业务办理系统，其特征在于，包括：业务受理终端以及根据权利要求1至15任一项所述的智能密钥设备，其中：所述智能密钥设备通过其通信接口与所述业务受理终端有线或无线连接。

17.一种业务办理系统，其特征在于，包括：移动终端、业务受理终端以及根据权利要求1至15任一项所述的智能密钥设备，其中：所述智能密钥设备通过其通信接口与所述移动终端有线或无线连接，所述移动终端与所述业务受理终端有线或无线连接。

一种智能密钥设备及业务办理系统

技术领域

[0001] 本实用新型涉及一种电子技术领域，尤其涉及一种智能密钥设备及业务办理系统。

背景技术

[0002] 在现有技术中，智能密钥设备主要用来保证网上交易中数据传输的安全。智能密钥设备中的安全芯片可以执行如下安全操作，计算签名、对数据进行加解密、对签名进行校验等。为了随时能够进行网上交易，一般需要随身携带智能密钥设备。此外，随着智能卡、集成电路卡等在日常生活中应用越来越广泛，为了随时对智能卡、集成电路卡等进行操作，也需要携带读卡器。然而现有的智能密钥设备不具有读卡功能，因此用户需要随身携带两种不同的设备，给用户造成了极大的不便。

实用新型内容

[0003] 本实用新型旨在解决至少上述问题之一。

[0004] 本实用新型的主要目的在于提供一种智能密钥设备。

[0005] 本实用新型的另一目的在于提供一种业务办理系统。

[0006] 本实用新型的又一目的在于提供一种业务办理系统。为达到上述目的，本实用新型的技术方案具体是这样实现的：

[0007] 本实用新型一方面提供了一种智能密钥设备，智能密钥设备包括：读卡接口，读卡模块，存储器，安全芯片和通信接口，其中：读卡模块电连接在存储器与读卡接口之间，读卡模块，用于向读卡接口发送读卡指令，读卡接口，用于接收与读卡指令对应的第一数据，并将第一数据发送至读卡模块；读卡模块，还用于接收第一数据，并向存储器发送第一数据；存储器电连接在读卡模块与安全芯片的输入端之间，存储器，用于接收第一数据，并向安全芯片发送第一数据；安全芯片的输出端与通信接口电连接；安全芯片，用于接收第一数据，利用智能密钥设备的私钥对接收到的数据进行签名生成第二数据，并向通信接口发送第二数据，其中，接收到的数据至少包括第一数据；通信接口，用于接收第二数据，并将第二数据外发。

[0008] 可选的，智能密钥设备还包括：二维码生成器和显示屏；安全芯片的输出端还与二维码生成器的输入端电连接；安全芯片，还用于向二维码生成器发送第二数据；二维码生成器的输出端与显示屏的输入端电连接；二维码生成器，用于根据第二数据生成二维码，并向显示屏发送二维码；显示屏，用于接收二维码，并显示二维码。

[0009] 可选的，智能密钥设备还包括：输入接口；输入接口，与安全芯片的输入端电连接，用于接收第三数据，并向安全芯片发送第三数据；安全芯片，还用于接收第三数据；其中，接收到的数据至少还包括第三数据。

[0010] 可选的，通信接口还与安全芯片的输入端电连接；通信接口，还用于接收第四数据，向安全芯片发送第四数据；安全芯片，还用于接收第四数据；其中，接收到的数据至少还

包括第四数据。

[0011] 可选的，智能密钥设备还包括：时钟；时钟，与安全芯片的输入端电连接，用于计时得到第五数据，并向安全芯片发送第五数据；安全芯片，还用于接收第五数据；其中，接收到的数据至少还包括第五数据。

[0012] 可选的，智能密钥设备还包括：计数器；计数器，与安全芯片的输入端电连接，用于计数得到第六数据，并向安全芯片发送第六数据；安全芯片，还用于接收第六数据；其中，接收到的数据至少还包括第六数据。

[0013] 可选的，智能密钥设备还包括：指纹采集器和摄像头；指纹采集器，与通信接口电连接，用于采集第七数据，并向通信接口发送第七数据；通信接口，还用于接收第七数据，并将第七数据外发；摄像头，与通信接口电连接，用于采集第八数据，并向通信接口发送第八数据；通信接口，还用于接收第八数据，并将第八数据外发。

[0014] 可选的，读卡接口包括非接触式接口，通信接口包括有线接口或无线接口。

[0015] 本实用新型另一方面提供了一种业务办理系统，包括：业务受理终端以及智能密钥设备，其中：智能密钥设备通过其通信接口与业务受理终端有线或无线连接。

[0016] 本实用新型的有一方面提供了一种业务办理系统，包括：移动终端、业务受理终端以及智能密钥设备，其中：智能密钥设备通过其通信接口与移动终端有线或无线连接，移动终端与业务受理终端有线或无线连接。

[0017] 由上述本实用新型提供的技术方案可以看出，本实用新型提供的智能密钥设备，能够实现对卡片的读取功能，以及对卡片中读取的数据进行签名处理，从而输出安全不易被解密的数据，特别是当读卡模块读取的是身份证数据时，本实施例提供的智能密钥设备还可以输出身份证电子凭条作为办理相应业务的凭据，从而方便用户办理业务。

附图说明

[0018] 为了更清楚地说明本实用新型实施例的技术方案，下面将对实施例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实用新型的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他附图。

[0019] 图1为本实用新型实施例1提供的一种智能密钥设备的结构示意图；

[0020] 图2为本实用新型实施例1提供的另一种智能密钥设备的结构示意图；

[0021] 图3为本实用新型实施例2提供的业务办理系统的结构示意图；

[0022] 图4为本实用新型实施例3提供的业务办理系统的结构示意图。

具体实施方式

[0023] 下面结合本实用新型实施例中的附图，对本实用新型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实用新型一部分实施例，而不是全部的实施例。基于本实用新型的实施例，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，都属于本实用新型的保护范围。

[0024] 在本实用新型的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为

基于附图所示的方位或位置关系，仅是为了便于描述本实用新型和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本实用新型的限制。此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或数量或位置。

[0025] 在本实用新型的描述中，需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本实用新型中的具体含义。

[0026] 下面将结合附图对本实用新型实施例作进一步地详细描述。

[0027] 实施例1

[0028] 本实施例提供了一种智能密钥设备。图1为本实施例提供的智能密钥设备的结构示意图，如图1所示，智能密钥设备包括：读卡接口101，读卡模块102，存储器103，安全芯片104和通信接口105，其中：读卡模块102电连接在存储器103与读卡接口101之间，读卡模块102，用于向读卡接口101发送读卡指令，读卡接口101，用于接收与读卡指令对应的第一数据，并将第一数据发送至读卡模块102；读卡模块102，还用于接收第一数据，并向存储器103发送第一数据；存储器103电连接在读卡模块102与安全芯片104的输入端之间，存储器103，用于接收第一数据，并存储第一数据；安全芯片104的输出端与通信接口105电连接；安全芯片104，用于接收存储器103发送的第一数据，利用智能密钥设备的私钥对接收到的数据进行签名生成第二数据，并向通信接口105发送第二数据，其中，接收到的数据至少包括第一数据；通信接口105，用于接收第二数据，并将第二数据外发。

[0029] 通过本实施例提供的智能密钥设备，能够实现对卡片的读取功能，以及利用安全芯片对卡片中读取的数据进行签名处理，从而输出安全不易被解密的数据，特别是当读卡模块读取的是身份证数据时，本实施例提供的智能密钥设备还可以输出身份证电子凭条作为办理相应业务的凭据。

[0030] 在本实施例中，读卡接口101，用于接收外部卡片发送的数据以及向外部卡片发送数据。读卡模块102可以用于读取智能卡、IC卡，也可以用于读取身份证信息。存储器103可以是一个独立的存储器，存储器103也可以与安全芯片104集成在一起。安全芯片104可以是国民技术股份有限公司的Z8D64U(国密批号SSX43)、Z32(国密批号SSX20)等，安全芯片104内部拥有独立的处理器对数据进行加解密运算，为用户提供数据加密和身份安全认证服务，保护商业隐私和数据安全。安全芯片104的输入端用于接收输入安全芯片104的数据，安全芯片104的输出端用于将经过安全芯片104处理后的数据外发。通信接口105，用于接收安全芯片104输出的数据以及向外部发送数据。在本实施例中，读卡指令可以是智能密钥设备通过其自带的按键、触摸屏等接收到用户输入的指令后，发送至读卡模块102的。与读卡指令对应的第一数据可以是身份证信息，即身份证中的有效内容，例如，姓名、性别、身份证号码、住址等。读卡接口101和读卡模块102可以分别独立设置，也可以集成为一个身份证读卡机芯片，例如，FM1715芯片。读卡模块102中可以包含微处理器和居民身份证验证安全控制(Secure Access Module，简称SAM)模块，微处理器接收到用户通过按键或触摸屏输入的读卡指令后，将读卡指令发送至读卡接口101，读卡接口101将读卡指令发送至身份证，并接收

身份证返回的身份证信息密文，并将身份证信息密文发送至SAM模块，SAM模块对身份证信息密文解密得到身份证信息明文，身份证信息明文即是第一数据。读卡模块102接收第一数据后，可以将第一数据发送至存储器103，存储器103将该第一数据存储，在安全芯片104需要第一数据时(例如，安全芯片接收到签名指令)，存储器103再将第一数据发送至安全芯片104，例如，存储器103接收到安全芯片104发送的获取第一数据的指令后，向安全芯片104发送所述第一数据；当然，作为另一种可选的方式，读卡模块104的一端与读卡接口连接，另一端也可以与安全芯片104电连接(图上未示出)，读卡模块104还用于在接收第一数据后，将第一数据直接发送至安全芯片104。安全芯片104，用于利用智能密钥设备的私钥至少对第一数据进行签名生成第二数据。安全芯片104对接收到的数据进行签名生成第二数据的具体方式如下：安全芯片104利用哈希算法计算接收到的数据得到接收到的数据的摘要，并利用智能密钥设备的私钥对接收到的数据的摘要进行加密，得到第二数据。本实施例中，在第一数据为身份证信息时，第二数据可以作为用户办理业务的身份证电子凭条，首先，由于哈希算法为不可逆算法，因此，安全芯片利用哈希算法计算得到的第二数据无法被恢复出第一数据，即身份证电子凭条不可逆，因此身份证电子凭条不能被还原为身份证信息，保证了身份证信息的安全；其次，本实施例中，由于在智能密钥设备中预先存储了身份证信息，因此，在办理实名认证业务时，无需身份证原件即可实现实名认证；再次，身份证电子凭条可以作为办理业务的备案信息，实现电子化的备案。

[0031] 作为本实用新型实施例的一个可选实施方式，读卡接口101包括非接触式接口，通信接口105包括有线接口或无线接口。

[0032] 在本实施例中，读卡接口101可以为符合ISO14443A、ISO14443B、ISO15693等非接触标准协议的接口。采用非接触式接口作为读卡接口，无需插拔卡片即可实现读卡，使得读卡操作更加方便。通信接口105可以为USB接口、音频接口等有线接口，也可以为远程网络接口(例如，GSM、GPRS、3G、4G通信接口等)、近距离无线传输接口(例如，蓝牙、NFC、WIFI、UWB、RFID、红外传输接口等)等无线接口。采用有线接口作为通信接口，使得智能密钥设备能够兼容具有有线接口的外部设备，例如，PC，此外，在智能密钥上设置有线接口实现简单，成本低。采用无线接口作为通信接口，智能密钥设备无需与外部设备有线连接，即可实现数据的收发，提高了智能密钥设备使用的便利性。

[0033] 作为本实用新型实施例的一个可选实施方式，如图2所示，智能密钥设备还包括：二维码生成器106和显示屏107；安全芯片104的输出端还与二维码生成器106的输入端电连接；安全芯片104，还用于向二维码生成器106发送第二数据；二维码生成器106的输出端与显示屏107的输入端电连接；二维码生成器106，用于根据第二数据生成二维码，并向显示屏107发送二维码；显示屏107，用于接收二维码，并显示二维码。

[0034] 在本实施例中，二维码生成器106能够将输入的数据生成相应的二维码，二维码生成器106可以是由软件单独实现的，也可以是由软件和硬件结合实现的。显示屏107可以为LED显示屏、液晶显示屏等，在本实施例中不作具体限定。显示屏107显示第二数据对应的二维码后，外部设备扫描二维码并对二维码解码后，能够获得第二数据。通过本可选实施方式，能够以二维码的形式传输第二数据，实现了更加灵活的数据传输，且二维码不能被随意解码，保证了第二数据的安全。

[0035] 作为本实用新型实施例的一个可选实施方式，如图2所示，智能密钥设备还包括：

输入接口108;输入接口108,与安全芯片104的输入端电连接,用于接收第三数据,并向安全芯片104发送第三数据;安全芯片104,还用于接收第三数据;其中,接收到的数据至少还包括第三数据。

[0036] 在本实施例中,输入接口108可以为按键、触摸屏等可以用于输入信息的接口。用户通过输入接口108输入第三数据,第三数据可以为当前请求办理的业务的业务相关信息,业务相关信息可以用来表明当前办理的是何种业务,例如,XX银行的银行卡开户业务、XX电信营业厅的开卡业务等信息。输入接口108将第三数据发送至安全芯片104之后,安全芯片104利用智能密钥设备的私钥至少对第一数据和第三数据进行签名生成第二数据,智能密钥设备将第二数据发送至业务受理终端,业务受理终端将第二数据发送至后台。通过本可选实施方式,第二数据中包含的第三数据能够表征办理的业务,以便于后台对第二数据进行验证,防止第二数据被再次非法使用办理其他业务。

[0037] 作为本实用新型实施例的一个可选实施方式,如图2所示,通信接口105还与安全芯片104的输入端电连接;通信接口105,还用于接收第四数据,向安全芯片104发送第四数据;安全芯片104,还用于接收第四数据;其中,接收到的数据至少还包括第四数据。

[0038] 在本实施例中,通信接口105与安全芯片104的输入端电连接,方便通信接口105向安全芯片104发送数据。第四数据可以是外部设备生成的单次凭证因子,第四数据的具体形式可以为随机数、随机字符、流水号等信息的任意组合。安全芯片104利用智能密钥设备的私钥至少对第一数据和第四数据进行签名生成第二数据,智能密钥设备将第二数据发送至业务受理终端,业务受理终端将第二数据发送至后台。通过本可选实施方式,第二数据中包含的第四数据(随机数等单次凭证因子)以便于后台能够用于对第二数据进行有效性认证,防止重放攻击。

[0039] 作为本实用新型实施例的一个可选实施方式,如图2所示,智能密钥设备还包括:时钟109;时钟109,与安全芯片104的输入端电连接,用于计时得到第五数据,并向安全芯片104发送第五数据;安全芯片104,还用于接收第五数据;其中,接收到的数据至少还包括第五数据。

[0040] 在本实施例中,时钟109可以是有源晶振、无源晶振等。第五数据可以为时钟109在安全芯片104生成第二数据的时刻计时得到的。安全芯片104利用智能密钥设备的私钥至少对第一数据和第五数据进行签名生成第二数据,智能密钥设备将该第二数据发送至业务受理终端,业务受理终端将第二数据发送至后台。第五数据可以仅精确到日期,也可以精确到时间的小时、分钟以及秒,例如,当前生成第二数据的时间为xxxx年xx月xx日xx时xx分xx秒,本实施例可以通过第五数据精确到的时间单位确定使用第二数据的有效时间。例如,时间因子为xxxx年12月,则该第二数据可以在xxxx年12月这一个月的任何时间有效,又例如,第五数据为xxxx年xx月07日,则该第二数据可以在xxxx年xx月07日这一天的任何时间有效,又例如,第五数据为xxxx年xx月xx日11时,则该第二数据可以在xxxx年xx月07日11时这一小时的任何时间有效。通过本实施方式,以便于后台通过第二数据中包含的第五数据的精确度可以便于后台验证第二数据的时间有效性,即便于后台验证身份证电子凭条在某段时间内有效。

[0041] 作为本实用新型实施例的一个可选实施方式,如图2所示,智能密钥设备还包括:计数器110;计数器110,与安全芯片104的输入端电连接,用于计数得到第六数据,并向安全

芯片104发送第六数据；安全芯片104，还用于接收第六数据；其中，接收到的数据至少还包括第六数据。

[0042] 在本实施例中，第六数据可以为计数器110对生成第二数据的累计次数进行计数得到的。计数器110的初始值可以为0，安全芯片104每生成一次第二数据，计数器110的计数增加1。安全芯片104利用智能密钥设备的私钥至少对第一数据和第六数据进行签名生成第二数据，智能密钥设备将该第二数据发送至业务受理终端，业务受理终端将第二数据发送至后台。通过本实施例，通过第二数据中包含的第六数据可以便于后台验证使用第二数据的有效性，即便于后台验证使用身份证电子凭条最多可以办理相应业务的次数。

[0043] 作为本实用新型实施例的一个可选实施方式，如图2所示，智能密钥设备还包括：指纹采集器111和摄像头112；指纹采集器111，与通信接口105电连接，用于采集第七数据，并向通信接口105发送第七数据；通信接口105，还用于接收第七数据，并将第七数据外发；摄像头112，与通信接口105电连接，用于采集第八数据，并向通信接口105发送第八数据；通信接口105，还用于接收第八数据，并将第八数据外发。

[0044] 在本实施例中，第七数据可以为用户的指纹信息，第七数据可以便于后台对使用智能密钥设备的用户进行身份认证。指纹信息能够唯一的表征用户的身份，且指纹信息相对固定，不会随着时间变化而发生改变，因此，利用指纹信息对用户的身份进行认证，实现成本低，认证效果好。在本实施例中，第八数据可以为用户的脸部图像信息，便于后台从脸部图像信息中提取出脸部特征信息，根据脸部特征信息对用户的身份进行认证具有准确度高的优点。

[0045] 实施例2

[0046] 本实施例提供了一种业务办理系统。图3为本实施例提供的业务办理系统的结构示意图。如图3所示，该系统包括：业务受理终端31以及实施例1中的智能密钥设备32，其中：智能密钥设备32通过其通信接口与业务受理终端31有线或无线连接。

[0047] 在本实施例中，业务受理终端31可以为银行的远程视频柜员机(Video Teller Machine，简称VTM)、电信营业厅的自助业务办理机或者办理业务的工作人员使用的终端等，前两种终端都属于自助办理终端，便于用户自行办理业务，提高用户体验，在本实施例不作具体限定，只要是能够用于办理需要身份证电子凭条的业务的终端，均属于本实施例的保护范围之内。智能密钥设备32的通信接口与实施例1中的通信接口105相同，在此不再具体赘述，特别地，在通信接口为远程网络接口时，所述智能密钥设备具有远程联网功能，可以实现与业务受理终端的远程通信。

[0048] 通过本实施例提供的业务办理系统，智能密钥设备32与业务受理终端31能够进行有线或无线通信，智能密钥设备32可以通过通信接口向业务受理终端31发送数据(即第二数据)或者接收业务受理终端31发送的数据(如办理业务信息)，业务受理终端31可以接收通信接口发送的数据(即第二数据)以及向通信接口发送数据(如办理业务信息)。

[0049] 下面以第一数据为身份证信息，即智能密钥设备利用从身份证读取的身份证信息进行签名得到身份证电子凭条办理相应业务为例对本实施例的业务办理系统进行详细说明。

[0050] 以办理银行卡开户业务为例说明本实施例提供的业务办理系统，智能密钥设备32，接收身份证发送的身份证信息(第一数据)，接收业务受理终端31(例如，VTM)发送的此

次办理银行卡开户业务的流水号(第四数据)，至少根据身份证信息和流水号生成身份证电子凭条(第二数据)，通过通信接口将身份证电子凭条发送至业务受理终端31，其中，智能密钥设备32也可以只根据身份证信息生成身份证电子凭条；业务受理终端31，接收身份证电子凭条，根据接收的身份证电子凭条办理银行卡开户业务，其中，在业务受理终端办理银行卡开户业务的过程中可以将身份证电子凭条发送至后台以便于后台对该身份证电子凭条的有效性进行验证。

[0051] 以电信营业厅的开卡业务为例说明本实施例提供的业务办理系统，智能密钥设备32，接收身份证发送的身份证信息(第一数据)，接收业务受理终端31(例如，电信营业厅的自助业务办理机)发送的此次办理电信营业厅开卡业务的流水号(第四数据)，至少根据身份证信息和流水号生成身份证电子凭条(第二数据)，通过通信接口将身份证电子凭条发送至业务受理终端31，其中，智能密钥设备32也可以只根据身份证信息生成身份证电子凭条；业务受理终端31，接收身份证电子凭条，根据接收的身份证电子凭条办理电信营业厅开卡业务，其中，在业务受理终端办理电信营业厅开卡业务的过程中可以将身份证电子凭条发送至后台以便于后台对其进行验证。

[0052] 在本实施例中，根据办理业务的不同，智能密钥设备32接收业务受理终端31发送的业务办理信息的具体内容也会发生变化，智能密钥设备32生成的身份证电子凭条也仅限于办理相应的业务，其具体内容也会发生变化，在此不再一一列举。

[0053] 实施例3

[0054] 本实施例提供了一种业务办理系统。图4为本实施例提供的业务办理系统的结构示意图。如图4所示，该系统包括：移动终端41、业务受理终端42以及实施例1中的智能密钥设备43，其中：智能密钥设备43通过其通信接口与移动终端有线或无线连接，移动终端41与业务受理终端42有线或无线连接。

[0055] 在本实施例中，移动终端41可以为手机、平板电脑等便携式终端。业务受理终端42与实施例2中的业务受理终端31相同，在此不再赘述。

[0056] 通过本实施例提供的业务办理系统，移动终端41将智能密钥设备43与业务受理终端42之间的数据进行转发，从而实现智能密钥设备43与业务受理终端42之间的通信。

[0057] 下面以第一数据为身份证信息，即智能密钥设备利用从身份证读取的身份证信息进行签名得到身份证电子凭条办理相应业务为例对本实施例的业务办理系统进行详细说明。

[0058] 以办理银行卡开户业务为例说明本实施例提供的业务办理系统，智能密钥设备43，接收身份证发送的身份证信息(第一数据)，接收移动终端41转发的业务受理终端42(例如，VTM)发送的此次办理银行卡开户业务的流水号(第四数据)，至少根据身份证信息和流水号生成身份证电子凭条(第二数据)，通过通信接口将身份证电子凭条发送至移动终端41，其中，智能密钥设备43也可以只根据身份证信息生成身份证电子凭条；移动终端41接收身份证电子凭条，将身份证电子凭条发送至业务受理终端42；业务受理终端42，接收身份证电子凭条，根据接收的身份证电子凭条办理银行卡开户业务，其中，在业务受理终端办理银行卡开户业务的过程中可以将身份证电子凭条发送至后台以便于后台对其进行验证。

[0059] 以电信营业厅的开卡业务为例说明本实施例提供的业务办理系统，智能密钥设备43，接收身份证发送的身份证信息(第一数据)，接收移动终端41转发的业务受理终端42(例

如，电信营业厅的自助业务办理机)发送的此次办理电信营业厅开卡业务的流水号(第四数据)，至少根据身份证信息和流水号生成身份证电子凭条(第二数据)，通过通信接口将身份证电子凭条发送至移动终端41，其中，智能密钥设备43也可以只根据身份证信息生成身份证电子凭条；移动终端41接收身份证电子凭条，将身份证电子凭条发送至业务受理终端42；业务受理终端42，接收身份证电子凭条，根据接收的身份证电子凭条办理电信营业厅开卡业务，其中，在业务受理终端办理电信营业厅开卡业务的过程中可以将身份证电子凭条发送至后台以便于后台对其进行验证。

[0060] 在本实施例中，根据办理业务的不同，业务受理终端42向移动终端41和智能密钥设备43发送业务办理信息的具体内容也会发生变化，智能密钥设备43生成的身份证电子凭条也仅限于办理相应的业务，其具体内容也会发生变化，在此不再一一列举。

[0061] 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0062] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本实用新型的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0063] 尽管上面已经示出和描述了本实用新型的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本实用新型的限制，本领域的普通技术人员在不脱离本实用新型的原理和宗旨的情况下在本实用新型的范围内可以对上述实施例进行变化、修改、替换和变型。本实用新型的范围由所附权利要求及其等同限定。


读卡接口101
读卡模块102
存储器103
输入端
安全芯片104
输出端
通信接口105

图1

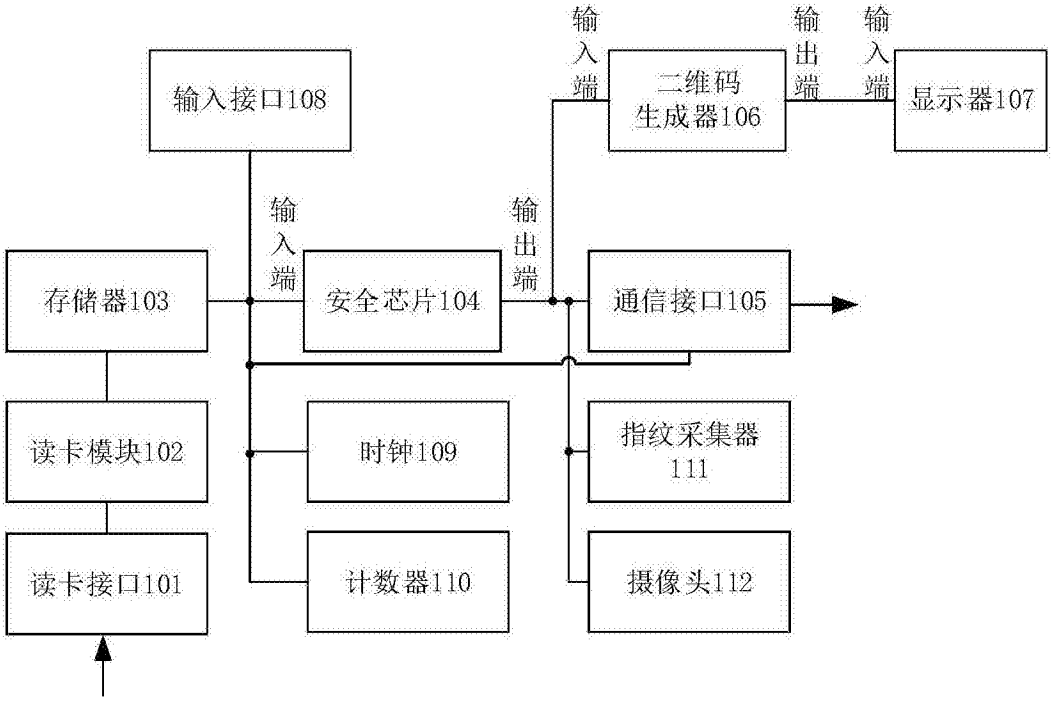

输入接口108
输入端
二维码生成器106
输出端
输入端
显示器107
输入端
输出端
存储器103
安全芯片104
通信接口105
读卡模块102
时钟109
指纹采集器111
读卡接口101
计数器110
摄像头112

图2

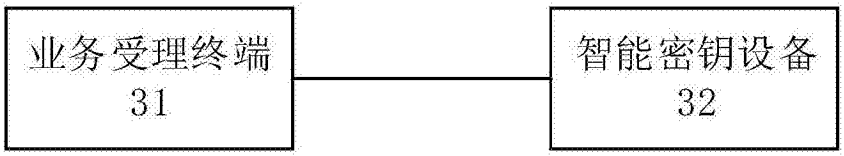

业务受理终端31
智能密钥设备32

图3


业务受理终端42
移动终端41
智能密钥设备43

图4