

数据安全交互方法和系统

技术领域

本发明涉及一种信息安全领域，尤其涉及一种数据安全交互方法和系统。

5

背景技术

移动支付就是允许用户使用其移动终端（例如智能手机、PDA、平板电脑、笔记本电脑等终端）对所消费的商品或服务进行账务支付的一种服务方式。单位或个人通过移动终端、互联网或者近距离传感直接或间接向银行金融机构发送支付指令产生货币支付与资金
10 流转的行为，从而实现移动支付功能。移动支付将移动终端、互联网、应用提供商以及金融机构相融合，为用户提供货币支付、缴费等金融业务。

移动支付主要包括远程支付和近场支付两种。远程支付指用户通过移动终端登录银行网页进行支付、账户操作等，主要应用于线上电子商务网站的购物与消费；近场支付是指消费者在购买商品或服务时，即时通过移动终端向商家进行支付，支付的处理在现场进行，
15 并且是不需要使用移动网络的线下操作，通过使用移动终端的射频（NFC）、红外、蓝牙等通道，实现与自动售货机以及 POS 机的本地通讯。

在整个移动支付的过程中，涉及到支付的参与者包括：消费用户、商户、移动运营商、第三方服务提供商、银行。消费用户和商户是系统的服务对象，移动运营商提供网络支持，银行方提供银行相关服务，第三方服务提供商提供支付平台服务，通过各方的结合以实现
20 业务。支付手段的电子化和移动化已经成为了不可避免的发展趋势，而移动支付系统的安全性问题又是移动电子商务安全的核心问题。

如何在移动支付的过程中保证数据交互的安全性是亟待解决的问题。

发明内容

25 本发明旨在解决上述问题之一。

本发明的一个主要目的在于提供一种数据安全交互方法。

本发明的另一个主要目的在于提供一种数据安全交互系统。

为达到上述目的，本发明的技术方案具体是这样实现的：

本发明一方面提供了一种数据安全交互方法，包括：终端在信号覆盖范围内扫描智能
30 密码设备，并获得扫描到的所述智能密码设备的标识信息；所述终端与后台系统服务器进行相互认证，和/或所述终端与所述智能密码设备进行相互认证；所述终端根据扫描到的所

述智能密码设备的标识信息获取所述智能密码设备对应的用户信息；所述终端将所述用户信息存储到预先建立的当前用户列表中。

此外，所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息包括：所述终端向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求；所述后台系统服务器接收到所述智能密码设备的标识信息以及所述用户信息读取请求后，根据所述智能密码设备的标识信息获取与所述智能密码设备对应的用户信息；所述后台系统服务器根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息；所述终端接收到所述用户信息读取请求的响应信息后，根据所述用户信息读取请求的响应信息获得所述用户信息。

此外，所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息包括：所述终端根据扫描到的所述智能密码设备的标识信息向所述智能密码设备发送用户信息读取请求；所述智能密码设备获得预先存储的用户信息，并根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息；所述终端接收到所述用户信息读取请求的响应信息后，根据所述用户信息读取请求的响应信息获得所述用户信息。

此外，所述终端与后台系统服务器进行相互认证包括：所述终端生成第一待签名信息；所述终端向后台系统服务器发送所述第一待签名信息以及第一认证请求信息；所述后台系统服务器接收到所述第一待签名信息以及所述第一认证请求信息后，生成第二待签名信息；所述后台系统服务器向所述终端发送所述第二待签名信息以及后台系统服务器证书；所述终端接收到所述第二待签名信息以及所述后台系统服务器证书后，利用预存的后台系统服务器证书对应的根证书验证所述后台系统服务器证书是否合法；所述终端在验证所述后台系统服务器证书合法后，利用所述终端的私钥对所述第一待签名信息和所述第二待签名信息进行签名生成第一签名信息；所述终端向所述后台系统服务器发送所述第一签名信息以及终端证书；所述后台系统服务器利用预存的终端证书对应的根证书验证所述终端证书是否合法；所述后台系统服务器在验证所述终端证书合法后，利用所述终端证书中的公钥验证所述第一签名信息；所述后台系统服务器在验证所述第一签名信息通过后，生成后台认证完成消息，并向所述终端发送所述后台认证完成消息；所述终端接收到所述后台认证完成消息后，验证所述后台认证完成消息；所述终端在验证所述后台认证完成消息通过后，生成终端认证第一完成消息，向所述后台系统服务器发送所述终端认证第一完成消息；所述后台系统服务器接收到所述终端认证第一完成消息后，验证所述终端认证第一完成消息；所述后台系统服务器在验证所述终端认证第一完成消息通过后，所述终端与所述后台系统

服务器完成相互认证。

此外，所述终端与所述智能密码设备进行相互认证包括：所述终端生成第三待签名信息；所述终端向所述智能密码设备发送所述第三待签名信息以及第二认证请求信息；所述智能密码设备接收到所述第三待签名信息以及所述第二认证请求信息后，生成第四待签名信息；所述智能密码设备利用所述智能密码设备的私钥对所述第三待签名信息进行签名获得第二签名信息，并向所述终端发送所述第四待签名信息、所述第二签名信息以及智能密码设备证书；所述终端接收到所述第四待签名信息、所述第二签名信息以及所述智能密码设备证书后，利用预存的智能密码设备证书对应的根证书验证所述智能密码设备证书是否合法；所述终端在验证所述智能密码设备证书合法后，利用所述智能密码设备证书中的公钥对所述第二签名信息进行验证；所述终端在验证所述第二签名信息通过后，利用所述终端的私钥对所述第三待签名信息和所述第四待签名信息进行签名获得第三签名信息；所述终端向所述智能密码设备发送所述第三签名信息以及所述终端证书；所述智能密码设备接收到所述第三签名信息以及所述终端证书后，利用预存的所述终端证书对应的根证书验证所述终端证书是否合法；所述智能密码设备在验证所述终端证书合法后，利用所述终端证书中的公钥对所述第三签名信息进行验证；所述智能密码设备在验证所述第三签名信息通过后，生成智能密码设备认证完成消息；所述智能密码设备向所述终端发送所述智能密码设备认证完成消息；所述终端接收到所述智能密码设备认证完成消息后，验证所述智能密码设备认证完成消息；所述终端在验证所述智能密码设备认证完成消息通过后，生成终端认证第二完成消息，向所述智能密码设备发送所述终端认证第二完成消息；所述智能密码设备接收到所述终端认证第二完成消息后，验证所述终端认证第二完成消息；所述智能密码设备验证所述终端认证第二完成消息后，所述终端与所述智能密码设备完成相互认证。

此外，所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息的步骤之后，所述方法还包括：所述终端获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；所述终端根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比较；如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则执行所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息的步骤；且如果所述当前用户列表中的智能密码设备的标识信息不在所述实时标识列表中，则删除所述当前用户列表中不在所述实时标识列表中的智能密码设备的用户信息。

此外，所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码

设备的标识信息的步骤之后，所述方法还包括：所述终端获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；所述终端根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比对；如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则执行所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息的步骤，并在所述终端获得所述用户信息后，将所述用户信息存储至所述实时标识列表中；且如果所述实时标识列表中的智能密码设备的标识信息在所述当前用户列表中，则将所述在所述当前用户列表中的智能密码设备的用户信息存储至所述实时标识列表中；将所述实时标识列表作为更新后的所述当前用户列表。

此外，所述第一认证请求信息包括所述终端的标识信息；所述后台系统服务器接收到所述第一待签名信息以及所述第一认证请求信息后，判断所述终端的标识信息是否包含在所述后台系统服务器中预存的终端异常名单中；所述后台系统服务器在判断出所述终端的标识信息在所述终端异常名单中后，获取锁定终端指令，以及利用所述后台系统服务器的私钥对锁定终端指令进行签名获得第四签名信息，并向所述终端发送所述锁定终端指令以及所述第四签名信息；所述终端接收到所述锁定终端指令以及所述第四签名信息后，利用预存的所述后台系统服务器证书中的公钥对所述第四签名信息进行验证；所述终端在验证所述第四签名信息通过后，根据所述锁定终端指令执行锁定操作。

此外，所述终端向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求的步骤之后，所述方法还包括：所述后台系统服务器判断所述智能密码设备的标识信息是否包含在所述后台系统服务器中预存的智能密码设备异常名单中；所述后台系统服务器在判断出所述智能密码设备的标识信息在所述智能密码设备异常名单中后，获取锁定智能密码设备指令，以及利用所述后台系统服务器的私钥对锁定智能密码设备指令进行签名获得第五签名信息，并通过所述终端向所述智能密码设备发送所述锁定智能密码设备指令以及所述第五签名信息；所述智能密码设备接收到所述锁定智能密码设备指令以及所述第五签名信息后，利用预存的所述后台系统服务器证书中的公钥对所述第五签名信息进行验证；所述智能密码设备在验证所述第五签名信息通过后，根据所述锁定智能密码设备指令执行锁定操作。

此外，所述方法还包括：所述后台系统服务器接收终端注册申请，并对所述终端注册申请进行审核；所述后台系统服务器在审核所述终端注册申请通过后，向所述终端发送终端密钥对生成指令；所述终端接收到所述终端密钥对生成指令后，生成终端密钥对；所述终端向所述后台系统服务器发送所述终端密钥对中的公钥；所述后台系统服务器接收到所

述终端密钥对中的公钥后，生成所述终端证书，并向所述终端发送所述终端证书；所述终端存储所述终端证书；以及所述后台系统服务器接收智能密码设备注册申请，并对所述智能密码设备注册申请进行审核；所述后台系统服务器在审核所述智能密码设备注册申请通过后，向所述智能密码设备发送智能密码设备密钥对生成指令；所述智能密码设备接收到所述智能密码设备密钥对生成指令后，生成智能密码设备密钥对；所述智能密码设备向所述后台系统服务器发送所述智能密码设备密钥对中的公钥；所述后台系统服务器接收到所述智能密码设备密钥对中的公钥后，生成所述智能密码设备证书，并向所述智能密码设备发送所述智能密码设备证书；所述智能密码设备存储所述智能密码设备证书。

此外，所述方法还包括：所述终端获取终端销户申请，利用所述终端的私钥对所述销户申请进行签名获得第六签名信息，并向所述后台系统服务器发送所述终端销户申请以及所述第六签名信息；所述后台系统服务器接收到所述终端销户申请以及所述第六签名信息后，利用预存的所述终端证书中的公钥对所述第六签名信息进行验证；所述后台系统服务器在验证所述第六签名信息通过后，删除预存的所述终端证书，并生成终端销户完成信息，向所述终端发送所述终端销户完成信息；所述终端接收到所述终端销户完成信息后，删除所述终端的私钥；和/或 所述智能密码设备获取智能密码设备销户申请，利用所述智能密码设备的私钥对所述销户申请进行签名获得第七签名信息，并向所述后台系统服务器发送所述智能密码设备销户申请以及所述第七签名信息；所述后台系统服务器接收到所述智能密码设备销户申请以及所述第七签名信息后，利用预存的所述智能密码设备证书中的公钥对所述第七签名信息进行验证；所述后台系统服务器在验证所述第七签名信息通过后，删除预存的所述智能密码设备证书，并生成智能密码设备销户完成信息，向所述智能密码设备发送所述智能密码设备销户完成信息；所述智能密码设备接收到所述智能密码设备销户完成信息后，删除所述智能密码设备的私钥。

此外，所述后台系统服务器接收到所述智能密码设备的标识信息以及所述用户信息读取请求的步骤之后，所述后台系统服务器向所述终端发送所述用户信息读取请求的响应信息的步骤之前，所述方法还包括：所述后台系统服务器通过所述终端向所述智能密码设备发送用户授权请求信息；所述智能密码设备接收到所述用户授权请求信息后，生成授权信息，并通过所述终端向所述后台系统服务器发送所述授权信息；所述后台系统服务器接收到所述授权信息后，执行所述后台系统服务器向所述终端发送所述用户信息读取请求的响应信息的步骤。

此外，所述智能密码设备接收到所述用户授权请求信息后，生成授权信息的步骤包括：所述智能密码设备在接收到所述用户授权请求信息后，由休眠状态转换为唤醒状态；所述

智能密码设备在唤醒状态下生成授权信息。

此外，所述智能密码设备接收到所述第三待签名信息以及所述第二认证请求信息后，生成第四待签名信息的步骤包括：所述智能密码设备在接收到所述第二认证请求信息后，由休眠状态转换为唤醒状态；所述智能密码设备在唤醒状态下生成第四待签名信息。

5 此外，所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息之前，所述方法还包括：所述智能密码设备进入可被扫描状态。

此外，所述后台系统服务器与所述终端之间传输的信息均通过第一会话密钥加密计算和/或校验计算后传输，其中，所述第一会话密钥预存在所述后台系统服务器和所述终端中或者所述第一会话密钥通过所述后台系统服务器和所述终端协商生成；和/或所述终端与所
10 述智能密码设备之间传输的信息均通过第二会话密钥加密计算和/或校验计算后传输，其中，所述第二会话密钥预存在所述终端和所述智能密码设备中或者所述第二会话密钥通过所述终端和所述智能密码设备协商生成。

本发明另一方面提供了一种数据安全交互系统，包括：终端、后台系统服务器以及智能密码设备；所述终端，配置为在信号覆盖范围内扫描所述智能密码设备，并获得扫描到的
15 的所述智能密码设备的标识信息；与所述后台系统服务器进行相互认证和/或与所述智能密码设备进行相互认证；根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息；将所述用户信息存储到预先建立的当前用户列表中。

此外，所述终端，还配置为向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求；接收所述后台系统服务器发送的所述用户信息读取请求的响应信息，根据所述用户信息读取请求的响应信息获得所述用户信息；所述后台系统服务器，配
20 置为接收所述终端发送的所述智能密码设备的标识信息以及所述用户信息读取请求，根据所述智能密码设备的标识信息获取与所述智能密码设备对应的用户信息；根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息。

25 此外，所述终端，还配置为根据扫描到的所述智能密码设备的标识信息向所述智能密码设备发送用户信息读取请求；接收所述智能密码设备发送的所述用户信息读取请求的响应信息，根据所述用户信息读取请求的响应信息获得所述用户信息；所述智能密码设备，配置为获得预先存储的用户信息，并根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息。

30 此外，所述终端，还配置为生成第一待签名信息；向后台系统服务器发送所述第一待签名信息以及第一认证请求信息；接收所述后台系统服务器发送的所述第二待签名信息以

及所述后台系统服务器证书，利用预存的后台系统服务器证书对应的根证书验证所述后台系统服务器证书是否合法；在验证所述后台系统服务器证书合法后，利用所述终端的私钥对所述第一待签名信息和所述第二待签名信息进行签名生成第一签名信息；向所述后台系统服务器发送所述第一签名信息以及终端证书；接收所述后台系统服务器发送的所述后台认证完成消息，验证所述后台认证完成消息；在验证所述后台认证完成消息通过后，生成终端认证第一完成消息，向所述后台系统服务器发送所述终端认证第一完成消息；所述后台系统服务器，还配置为接收所述终端发送的所述第一待签名信息以及所述第一认证请求信息，生成第二待签名信息；向所述终端发送所述第二待签名信息以及后台系统服务器证书；利用预存的终端证书对应的根证书验证所述终端证书是否合法；在验证所述终端证书合法后，利用所述终端证书中的公钥验证所述第一签名信息；在验证所述第一签名信息通过后，生成后台认证完成消息，并向所述终端发送所述后台认证完成消息；接收所述终端发送的所述终端认证第一完成消息，验证所述终端认证第一完成消息；在验证所述终端认证第一完成消息通过后，所述终端与所述后台系统服务器完成相互认证。

此外，所述终端，还配置为生成第三待签名信息；向所述智能密码设备发送所述第三待签名信息以及第二认证请求信息；接收所述智能密码设备发送的所述第四待签名信息、所述第二签名信息以及所述智能密码设备证书，利用预存的智能密码设备证书对应的根证书验证所述智能密码设备证书是否合法；在验证所述智能密码设备证书合法后，利用所述智能密码设备证书中的公钥对所述第二签名信息进行验证；在验证所述第二签名信息通过后，利用所述终端的私钥对所述第三待签名信息和所述第四待签名信息进行签名获得第三签名信息；向所述智能密码设备发送所述第三签名信息以及所述终端证书；接收所述智能密码设备发送的所述智能密码设备认证完成消息，验证所述智能密码设备认证完成消息；在验证所述智能密码设备认证完成消息通过后，生成终端认证第二完成消息，向所述智能密码设备发送所述终端认证第二完成消息；所述智能密码设备，还配置为接收所述终端发送的所述第三待签名信息以及所述第二认证请求信息，生成第四待签名信息；利用所述智能密码设备的私钥对所述第三待签名信息进行签名获得第二签名信息，并向所述终端发送所述第四待签名信息、所述第二签名信息以及智能密码设备证书；接收所述终端发送的所述第三签名信息以及所述终端证书，利用预存的所述终端证书对应的根证书验证所述终端证书是否合法；在验证所述终端证书合法后，利用所述终端证书中的公钥对所述第三签名信息进行验证；在验证所述第三签名信息通过后，生成智能密码设备认证完成消息；向所述终端发送所述智能密码设备认证完成消息；接收所述终端发送的所述终端认证第二完成消息，验证所述终端认证第二完成消息；验证所述终端认证第二完成消息后，所述终端与

所述智能密码设备完成相互认证。

此外，所述终端，还配置为在所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息之后，获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比对；如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息；且如果所述当前用户列表中的智能密码设备的标识信息不在所述实时标识列表中，则删除所述当前用户列表中不在所述实时标识列表中的智能密码设备的用户信息。

此外，所述终端，还配置为在所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息之后，获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比对；如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息，并在所述终端获得所述用户信息后，将所述用户信息存储至所述实时标识列表中；且如果所述实时标识列表中的智能密码设备的标识信息在所述当前用户列表中，则将所述在所述当前用户列表中的智能密码设备的用户信息存储至所述实时标识列表中；将所述实时标识列表作为更新后的所述当前用户列表。

此外，所述后台系统服务器，还配置为接收所述终端发送的所述第一待签名信息以及所述第一认证请求信息，其中，所述第一认证请求信息包括所述终端的标识信息；判断所述终端的标识信息是否包含在所述后台系统服务器中预存的终端异常名单中；在判断出所述终端的标识信息在所述终端异常名单中后，获取锁定终端指令，以及利用所述后台系统服务器的私钥对锁定终端指令进行签名获得第四签名信息，并向所述终端发送所述锁定终端指令以及所述第四签名信息；所述终端，还配置为接收所述后台系统服务器发送的所述锁定终端指令以及所述第四签名信息，利用预存的所述后台系统服务器证书中的公钥对所述第四签名信息进行验证；在验证所述第四签名信息通过后，根据所述锁定终端指令执行锁定操作。

此外，所述后台系统服务器，还配置为在所述终端向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求之后，判断所述智能密码设备的标识信息是否包含在所述后台系统服务器中预存的智能密码设备异常名单中；在判断出所述智能密码

设备的标识信息在所述智能密码设备异常名单中后，获取锁定智能密码设备指令，以及利用所述后台系统服务器的私钥对锁定智能密码设备指令进行签名获得第五签名信息，并通过所述终端向所述智能密码设备发送所述锁定智能密码设备指令以及所述第五签名信息；所述智能密码设备，还配置为接收所述锁定智能密码设备指令以及所述第五签名信息，利用预存的所述后台系统服务器证书中的公钥对所述第五签名信息进行验证；在验证所述第五签名信息通过后，根据所述锁定智能密码设备指令执行锁定操作。

此外，所述后台系统服务器，还配置为接收终端注册申请，并对所述终端注册申请进行审核；在审核所述终端注册申请通过后，向所述终端发送终端密钥对生成指令；接收所述终端发送的所述终端密钥对中的公钥，生成所述终端证书，并向所述终端发送所述终端证书；所述终端，还配置为接收所述后台系统服务器发送的所述终端密钥对生成指令，生成终端密钥对；向所述后台系统服务器发送所述终端密钥对中的公钥；存储所述终端证书；以及所述后台系统服务器，还配置为接收智能密码设备注册申请，并对所述智能密码设备注册申请进行审核；在审核所述智能密码设备注册申请通过后，向所述智能密码设备发送智能密码设备密钥对生成指令；接收所述智能密码设备发送的所述智能密码设备密钥对中的公钥，生成所述智能密码设备证书，并向所述智能密码设备发送所述智能密码设备证书；所述智能密码设备，还配置为接收所述后台系统服务器发送的所述智能密码设备密钥对生成指令，生成智能密码设备密钥对；向所述后台系统服务器发送所述智能密码设备密钥对中的公钥；存储所述智能密码设备证书。

此外，所述终端，还配置为获取终端销户申请，利用所述终端的私钥对所述销户申请进行签名获得第六签名信息，并向所述后台系统服务器发送所述终端销户申请以及所述第六签名信息；接收所述后台系统服务器发送的所述终端销户完成信息，删除所述终端的私钥；所述后台系统服务器，还配置为接收所述终端发送的所述终端销户申请以及所述第六签名信息，利用预存的所述终端证书中的公钥对所述第六签名信息进行验证；在验证所述第六签名信息通过后，删除预存的所述终端证书，并生成终端销户完成信息，向所述终端发送所述终端销户完成信息；和/或 所述智能密码设备，还配置为获取智能密码设备销户申请，利用所述智能密码设备的私钥对所述销户申请进行签名获得第七签名信息，并向所述后台系统服务器发送所述智能密码设备销户申请以及所述第七签名信息；接收所述后台系统服务器发送的所述智能密码设备销户完成信息，删除所述智能密码设备的私钥；所述后台系统服务器，还配置为接收所述智能密码设备发送的所述智能密码设备销户申请以及所述第七签名信息，利用预存的所述智能密码设备证书中的公钥对所述第七签名信息进行验证；在验证所述第七签名信息通过后，删除预存的所述智能密码设备证书，并生成智能

密码设备销户完成信息，向所述智能密码设备发送所述智能密码设备销户完成信息。

此外，所述后台系统服务器，还配置为通过所述终端向所述智能密码设备发送用户授权请求信息；接收所述智能密码设备通过所述终端发送的所述授权信息，向所述终端发送所述用户信息读取请求的响应信息；所述智能密码设备，还配置为接收所述后台系统服务器通过所述终端发送的所述用户授权请求信息，生成授权信息，并通过所述终端向所述后台系统服务器发送所述授权信息。

此外，所述智能密码设备，还配置为在接收到所述用户授权请求信息后，由休眠状态转换为唤醒状态；在唤醒状态下生成授权信息。

此外，所述智能密码设备，还配置为在接收到所述第二认证请求信息后，由休眠状态转换为唤醒状态；在唤醒状态下生成第四待签名信息。

此外，所述智能密码设备，还配置为在被所述终端扫描之前，进入可被扫描状态。

此外，所述后台系统服务器与所述终端之间传输的信息均通过第一会话密钥加密计算和/或校验计算后传输，其中，所述第一会话密钥预存在所述后台系统服务器和所述终端中或者所述第一会话密钥通过所述后台系统服务器和所述终端协商生成；和/或所述终端与所述智能密码设备之间传输的信息均通过第二会话密钥加密计算和/或校验计算后传输，其中，所述第二会话密钥预存在所述终端和所述智能密码设备中或者所述第二会话密钥通过所述终端和所述智能密码设备协商生成。

由上述本发明提供的技术方案可以看出，本发明可以仅构建后台系统服务器与终端之间进行相互认证的体系，建立二者之间的安全通道；也可以仅构建终端与智能密码设备之间进行相互认证的体系，建立二者之间的安全通道；还可以构建后台系统服务器、终端、智能密码设备三者之间进行相互认证的体系，建立三者之间的安全通道。基于上述三种中的任一种相互认证的体系，可以防范钓鱼风险，防止交易信息篡改、远程劫持和中间人攻击等交易风险，从而有效保障持有智能密码设备的用户与持有终端的商户的账户资金安全。

附图说明

为了更清楚地说明本发明实施例的技术方案，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发明的一些实施例，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。

图 1 为本发明提供的数据安全交互系统结构示意图；

图 2 为本发明提供的数据安全交互方法的流程图。

具体实施方式

下面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
5 明的实施例，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，都属于本发明的保护范围。

在本发明的描述中，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
10 是两个元件内部的连通。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。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。

下面将结合附图对本发明实施例作进一步地详细描述。

15 本发明提供的数据安全交互方法，可适用的系统架构如图 1 所示，包括：后台系统服务器、终端以及智能密码设备。

其中，后台系统服务器可以完成对终端和智能密码设备的管理以及对用户信息的存储和下发管理，例如包括对终端和智能密码设备的注册、销户、锁定、认证等管理，其可以提供银行相关服务、支付平台服务等金融服务；可以包括支付服务器、认证服务器、管理
20 服务器等一个或多个服务器的组合。

终端可以为商户端的终端，以完成移动支付的发起，对智能密码设备和后台系统服务器的认证，用户信息的维护等，该终端可以自动扫描到其信号覆盖范围内的智能密码设备，并建立与智能密码设备的通信连接，获取智能密码设备对应的用户信息。

智能密码设备具备安全支付（例如：电子签名、动态口令生成）功能，以及对终端的
25 认证。该智能密码设备具备无线通信模块（例如：蓝牙、红外线、RFID、NFC、光、声波、热能、振动、WIFI 等），可以与终端之间通过该无线通信模块进行通信。当然，该智能密码设备还可以包括有线接口（例如：音频接口、USB 接口、串口等），并通过有线接口与终端进行通信。另外，智能密码设备还可以具备连接选项功能，如果用户不开启该功能，则终端无法获取智能密码设备的标识信息和对应的用户信息。例如：智能密码设备可以进入
30 可被扫描的状态，以便终端扫描到该智能密码设备。智能密码设备具备的连接选项功能，可以为在智能密码设备上设置的硬件开关开启实现的，也可以为智能密码设备通过软件开

启实现的。

如图 2 所示，本发明提供的数据安全交互方法，包括下述步骤一至步骤七。

步骤一：终端和智能密码设备向后台系统服务器进行注册。

5 包括以下两个方面：终端向后台系统服务器进行注册和智能密码设备向后台系统服务器进行注册。

1、终端向后台系统服务器进行注册。

后台系统服务器接收终端注册申请，并对终端注册申请进行审核；具体的，商户可以到银行柜台办理该终端的注册申请，也可以通过互联网办理该终端的注册申请，后台系统
10 服务器接收到该注册申请后，对该商户的身份的合法性进行审核。

后台系统服务器在审核终端注册申请通过后，向终端发送终端密钥对生成指令；具体的，后台系统服务器审核商户身份的合法性等通过后，予以同意对商户的终端进行注册，同时向终端发送密钥对生成指令，用于指示终端生成终端密钥对，该终端密钥对包括一对公私钥。

15 终端接收到终端密钥对生成指令后，生成终端密钥对。具体的，在终端中可以预设一个密钥对的生成方式，在终端接收到终端密钥对生成指令后，根据预设的密钥对生成方式生成终端密钥对，即生成一对公私钥。

终端向后台系统服务器发送终端密钥对中的公钥。具体的，终端可以通过可信的通信链路将其生成的终端密钥对中的公钥向后台系统服务器进行发送，以保证终端的公钥发送
20 的安全性；也可以通过互联网将其生成的终端密钥对中的公钥向后台系统服务器进行发送，以提高终端的公钥传输的便捷性。

后台系统服务器接收到终端密钥对中的公钥后，生成终端证书，并向终端发送终端证书。具体的，后台系统服务器可以以后台系统服务器的私钥对商户的信息以及终端的公钥进行计算生成终端证书；后台系统服务器中还可以包含 CA 服务器，通过该 CA 服务器的
25 私钥对商户的信息以及终端的公钥进行计算生成终端证书；后台系统服务器还可以将商户的信息以及终端的公钥发送至 CA，CA 根据 CA 的私钥对商户的信息以及终端的公钥进行计算生成终端证书，并通过后台系统服务器发送给终端。

终端存储终端证书。具体的，终端在接收到后台系统服务器发送的终端证书后，将该终端证书存储在执行安全功能的存储区中。当然，针对不同的后台系统服务器，终端还可
30 以存储不同的后台系统服务器发送的不同的终端证书。

2、智能密码设备向后台系统服务器进行注册。

后台系统服务器接收智能密码设备注册申请，并对智能密码设备注册申请进行审核。具体的，持有智能密码设备的用户可以到银行柜台办理该智能密码设备的注册申请，也可以通过互联网办理该智能密码设备的注册申请，后台系统服务器接收到该注册申请后，对该用户的身份的合法性进行审核。

- 5 后台系统服务器在审核智能密码设备注册申请通过后，向智能密码设备发送智能密码设备密钥对生成指令。具体的，后台系统服务器审核用户身份的合法性等通过后，予以同意对用户的智能密码设备进行注册，同时向智能密码设备发送密钥对生成指令，用于指示智能密码设备生成智能密码设备密钥对，该智能密码设备密钥对包括一对公私钥。

- 10 智能密码设备接收到智能密码设备密钥对生成指令后，生成智能密码设备密钥对。具体的，在智能密码设备中可以预设一个密钥对的生成方式，在智能密码设备接收到智能密码设备密钥对生成指令后，根据预设的密钥对生成方式生成智能密码设备密钥对，即生成一对公私钥。

- 15 智能密码设备向后台系统服务器发送智能密码设备密钥对中的公钥。具体的，智能密码设备可以通过可信的通信链路将其生成的智能密码设备密钥对中的公钥向后台系统服务器进行发送，以保证智能密码设备的公钥发送的安全性；也可以通过互联网将其生成的智能密码设备密钥对中的公钥向后台系统服务器进行发送，以提高智能密码设备的公钥传输的便捷性。

- 20 后台系统服务器接收到智能密码设备密钥对中的公钥后，生成智能密码设备证书，并向智能密码设备发送智能密码设备证书。具体的，后台系统服务器可以以后台系统服务器的私钥对用户的信息以及智能密码设备的公钥进行计算生成智能密码设备证书。后台系统服务器中还可以包含 CA 服务器，通过该 CA 服务器的私钥对用户的信息以及智能密码设备的公钥进行计算生成智能密码设备证书。后台系统服务器还可以将用户的信息以及智能密码设备的公钥发送至 CA，CA 根据 CA 的私钥对用户的信息以及智能密码设备的公钥进行计算生成智能密码设备证书，并通过后台系统服务器发送给智能密码设备。

- 25 智能密码设备存储智能密码设备证书。具体的，智能密码设备在接收到后台系统服务器发送的智能密码设备证书后，将该智能密码设备证书存储在执行安全功能的存储区中。当然，针对不同的后台系统服务器，智能密码设备还可以存储不同的后台系统服务器发送的不同的智能密码设备证书。

- 30 步骤二：终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的智能密码设备的标识信息。

具体的，终端可以按照一定的时间间隔发送查询信号（例如终端的序列号）查询一定

无线信号覆盖范围内的智能密码设备。

智能密码设备对终端的查询进行侦听（查询扫描），当智能密码设备进入终端的信号覆盖范围内后，向终端发送智能密码设备的标识信息，由此，终端扫描到了智能密码设备的标识信息。

5 以下，提供两种实现终端扫描得到智能密码设备的标识信息的方法。

（1）终端可以使用 IAC（Inquiry Access Code，查询访问码）查询一定无线信号覆盖范围内的智能密码设备。

智能密码设备对终端的查询进行侦听（查询扫描），当智能密码设备进入终端的信号覆盖范围内后，向终端发送智能密码设备的地址和时钟信息；

10 智能密码设备侦听来自终端的寻呼信息，进行寻呼扫描；

终端寻呼已经查询到的智能密码设备；

智能密码设备接收到寻呼信息后，向终端发送智能密码设备的 DAC（Device Access Code，设备访问码）。

（2）终端发送查询信号查询一定无线信号覆盖范围内的智能密码设备。

15 智能密码设备对终端的查询信号进行侦听（查询扫描），当智能密码设备进入终端的信号覆盖范围内后，向终端发送智能密码设备的地址。

当然，本发明仅以以上两个示例说明终端如何获得智能密码设备的标识信息，但本发明并不局限于此，基于上述两个获得智能密码设备的标识信息的方法，智能密码设备可以在接收到终端发送的任何信息时，均可以将终端发送的信息作为休眠唤醒信号，智能密码设备根据休眠唤醒信号，将休眠状态切换为唤醒状态（即正常工作模式）。同时，智能密码设备在任何命令执行结束以后，均可以自动回复休眠状态。智能密码设备进入休眠状态以节省智能密码设备的电能，延长使用寿命。

在本步骤终端扫描智能密码设备之前，智能密码设备还需要进入可被扫描的状态，以便终端可以扫描到该智能密码设备，其中，智能密码设备进入可被扫描的状态可以通过在智能密码设备上设置的硬件开关开启实现，也可以通过智能密码设备软件开启实现。

25 **步骤三：终端与后台系统服务器进行相互认证，和/或终端与智能密码设备进行相互认证。**

1、终端与后台系统服务器进行相互认证。

终端生成第一待签名信息。具体的，终端可以通过随机数生成器生成随机数作为第一待签名信息，也可以采用自身的序列号、MAC 地址或者其他的标识信息作为第一待签名信息，也可以是随机数和标识信息的组合作为第一待签名信息。其中，只要可以被后台系统

服务器进行签名的信息均可以作为第一待签名信息，以便后台系统服务器返回签名信息后对后台系统服务器进行认证。随机数可以为数字、字母、特殊字符等字符中的一种或任意几种的组合。

终端向后台系统服务器发送第一待签名信息以及第一认证请求信息。具体的，终端可以通过可信的通信链路将第一待签名信息以及第一认证请求信息向后台系统服务器进行发送，以保证信息发送的安全性；也可以通过互联网将第一待签名信息以及第一认证请求信息向后台系统服务器进行发送，以提高信息传输的便捷性。

此外，后台系统服务器为了确保数据交互的安全性以及终端的合法性，后台系统服务器还可以在接收到第一待签名信息以及第一认证请求信息后，判断终端的标识信息是否包含在后台系统服务器中预存的终端异常名单中，其中，第一认证请求信息包括终端的标识信息。后台系统服务器在判断出终端的标识信息在终端异常名单中后，获取锁定终端指令，以及利用后台系统服务器的私钥对锁定终端指令进行签名获得第四签名信息，并向终端发送锁定终端指令以及第四签名信息。终端接收到锁定终端指令以及第四签名信息后，利用预存的后台系统服务器证书中的公钥对第四签名信息进行验证。终端在验证第四签名信息通过后，根据锁定终端指令执行锁定操作。

具体的，终端异常名单可以为黑名单、挂失名单、失效名单等任意表示终端身份非法的名单。如果终端的标识信息在终端异常名单中，则说明该终端是非法的终端，此时，为了确保安全性，后台系统服务器向该非法终端发送锁定指令以锁定该非法终端，同时，后台系统服务器还对该锁定指令进行签名，以确保锁定指令的合法来源，避免非法锁定终端的恶意操作。

当然，本发明并不局限于此，对于实际应用来说，只要可以合法锁定非法终端即可。

另外，后台系统服务器也可以不对锁定指令进行签名，仅发送锁定指令至非法终端以锁定该非法终端。

终端根据锁定终端指令执行锁定操作可以包括：终端拒绝执行任何请求，销毁自身存储的证书等任意方式。

当然，后台系统服务器在发送锁定指令后，还可以执行拒绝该非法终端的任何请求。

由此可见，当终端出现遗失或遭到非法举报等异常情况时，该终端的标识信息将被录入到后台系统服务器的挂失名单或黑名单等异常名单中。此后，若再有人企图使用该终端进行交易以非法转账盗取资金时，在终端与后台系统服务器进行认证时，后台系统服务器会将终端标识信息在异常名单进行比对，若发现该终端的标识信息在异常名单中，后台系统服务器就会对终端进行锁定，从而保护用户账户安全。

后台系统服务器接收到第一待签名信息以及第一认证请求信息后，生成第二待签名信息。具体的，后台系统服务器可以在接收到第一认证请求信息后，生成第二待签名信息，可以通过随机数生成器生成随机数作为第二待签名信息，也可以采用自身的序列号、MAC地址或者其他的标识信息作为第二待签名信息，也可以是随机数和标识信息的组合作为第二待签名信息。其中，只要可以被终端进行签名的信息均可以作为第二待签名信息，以便终端返回签名信息后对终端进行认证。随机数可以为数字、字母、特殊字符等字符中的一种或任意几种的组合。

后台系统服务器向终端发送第二待签名信息以及后台系统服务器证书。具体的，后台系统服务器可以通过可信的通信链路将第二待签名信息以及后台系统服务器证书向终端进行发送，以保证信息发送的安全性。也可以通过互联网将第二待签名信息以及后台系统服务器证书向终端进行发送，以提高信息传输的便捷性。

终端接收到第二待签名信息以及后台系统服务器证书后，利用预存的后台系统服务器证书对应的根证书验证后台系统服务器证书是否合法。具体的，终端在注册过程中还需获取到后台系统服务器证书对应的根证书，以便对后台系统服务器证书进行合法性验证。

终端在验证后台系统服务器证书合法后，利用终端的私钥对第一待签名信息和第二待签名信息进行签名生成第一签名信息。具体的，终端对第一待签名信息和第二待签名信息进行签名，由此，终端将签名信息传输至后台系统服务器，即可以保证该数据的合法来源，也保证了数据中重要信息的安全性。本发明中的第一签名信息可以是将第一待签名信息和第二待签名信息连接后的信息进行签名获得的，也可以是将第一待签名信息和第二待签名信息按照预先协商的调整方案进行调整后的信息进行签名获得的。当然，终端在验证后台系统服务器证书合法后，还可以生成共享主密钥，该共享主密钥具体可以用于生成第一会话密钥，此时，终端还利用后台系统服务器证书中的公钥对共享主密钥进行加密生成第一加密信息；由此可以安全传输共享主密钥。

终端向后台系统服务器发送第一签名信息以及终端证书。当然，如果终端还生成了共享主密钥，并对共享主密钥进行加密获得第一加密信息，则在本步骤中，终端除了向后台系统服务器发送第一签名信息以及终端证书外，还向后台系统服务器发送第一加密信息。

后台系统服务器利用预存的终端证书对应的根证书验证终端证书是否合法。具体的，后台系统服务器在终端的注册过程中还获取到终端证书对应的根证书，以便对终端证书进行合法性验证。

后台系统服务器在验证终端证书合法后，利用终端证书中的公钥验证第一签名信息。

后台系统服务器在验证第一签名信息通过后，生成后台认证完成消息，并向终端发送

后台认证完成消息；当然，如果后台系统服务器还接收到第一加密信息，则本步骤中，后台系统服务器还利用后台系统服务器的私钥解密第一加密信息，获得共享主密钥。

终端接收到后台认证完成消息后，验证后台认证完成消息。具体的，终端对后台认证完成消息进行合法性验证。

- 5 终端在验证后台认证完成消息通过后，生成终端认证第一完成消息，向后台系统服务器发送终端认证第一完成消息。当然，如果终端生成了共享主密钥，则本步骤中，终端还可以根据共享主密钥计算第一会话密钥。

后台系统服务器接收到终端认证第一完成消息后，验证终端认证第一完成消息；具体的后台系统服务器对终端认证第一完成消息进行合法性验证。

- 10 后台系统服务器在验证终端认证第一完成消息通过后，终端与后台系统服务器完成相互认证。当然，如果后台系统服务器还解密获得了共享主密钥，则本步骤中，后台系统服务器还可以根据共享主密钥计算第一会话密钥。

基于上述终端与后台系统服务器之间的双向认证，可以确保双方合法性，提高后续处理的安全性。

- 15 另外，后台系统服务器在验证终端认证第一完成消息通过后，还对终端开放相应的权限，例如：终端可以从后台系统服务器获取智能密码设备对应的用户信息，以便实现后台系统服务器对终端的管理。

- 20 当然，如果终端与后台系统服务器之间还生成第一会话密钥，则可以保证后台系统服务器与终端之间数据传输的安全性和/或完整性，以便后台系统服务器与终端进行后续数据传输时，利用第一会话密钥对待传输数据进行加密计算和/或校验计算。该第一会话密钥可以包括加密密钥和/或校验密钥，校验密钥可以为 MAC 校验计算密钥或 HASH 校验计算密钥，加密密钥为对称加密计算密钥，该第一会话密钥所包括的加密密钥和/或校验密钥可以为通过共享主密钥进行分解得到的。

- 25 当然，本发明并不局限于此种由终端发起的第一会话密钥生成过程，还可以由后台系统服务器发起该第一会话密钥生成过程。此时对于终端的锁定，只要在后台系统服务器接收到终端的标识信息后即可由后台系统服务器进行判断即可。

此外，第一会话密钥可以由终端或者后台系统服务器中的任一方生成后，并以对方的公钥进行加密后发送给对方，减少一方的计算复杂度。

- 30 终端与后台系统服务器之间生成第一会话密钥的过程可以与下述终端与智能密码设备之间生成第二会话密钥的过程相同。

以下，给出一个具体的终端与后台系统服务器之间认证并结合第一会话密钥生成的方

式，当然本发明并不局限于此。

1) 商户端的终端产生随机数 R1。

2) 商户端的终端将随机数 R1 发送给后台系统服务器，并向后台系统服务器发送认证请求。

5 3) 后台系统服务器接收到来自终端的认证请求，产生随机数 R2。

4) 后台系统服务器向终端发送随机数 R2 和后台系统服务器证书。

5) 终端使用终端中预存的后台系统服务器证书对应的根证书验证收到的后台系统服务器证书。

如果验证不通过，则结束。

10 如果验证通过，终端产生共享主密钥 MKey，用后台系统服务器证书中的公钥对 MKey 加密得到 E1。

6) 终端连接 R1 和 R2 得到 R3，对 R3 进行摘要计算得到 H1，然后使用终端的私钥对 H1 进行签名计算得到 S1。

7) 终端将 S1、E1 和终端证书发送至后台系统服务器。

15 8) 后台系统服务器使用终端证书对应的根证书验证终端证书合法性。

如果验证终端证书不通过，则结束。

如果验证终端证书通过，则使用终端证书验证 S1。

如果验证 S1 不通过，则结束。

如果验证 S1 通过，则从 E1 中解密得到共享主密钥 MKey。

20 9) 后台系统服务器对后台系统服务器证书进行摘要计算得到 H2，对终端证书进行摘要计算得到 H3，将 R1、R2、H2、H3、S1、E1 连接后得到 T1，对 T1 进行摘要计算后再经过 HMAC 计算得到“后台系统服务器认证完成消息”。

10) 后台系统服务器发送“后台系统服务器认证完成消息”到终端。

11) 终端验证接收到的后台系统服务器发来的“后台系统服务器认证完成消息”。

25 如果验证不通过，则结束。

如果验证通过，则生成“终端认证完成消息”(参见上述生成“后台系统服务器认证完成消息”的方式)。

12) 终端发送“终端认证完成消息”到后台系统服务器。

13) 后台系统服务器验证接收到的“终端认证完成消息”。

30 如果验证不通过，则结束。

如果验证通过，则表示双向认证过程成功，双方计算会话密钥，并从会话密钥中分解

出的加密密钥 **K1**，用于后台系统服务器与终端之间进行数据传输的加密解密，和/或校验计算的校验密钥 **MACKEY**，用于校验值的生成与校验。

如此商户的终端与后台系统服务器之间就进行了双向的身份认证，确保了对方是合法的，并协商出了公共的会话密钥（包括加密密钥和/或校验密钥），可用于终端与后台系统服务器之间数据互传时的数据加密和/或校验值的生成。该商户的终端也完成了在后台系统服务器处的“签到”，即可以进行后续的用户信息读取和交易请求的操作请求。

需要说明的是，本例中后台系统服务器与终端之间的传输数据的时候生成的校验值是 **MAC** 形式的。在具体实现时，所述的校验值并不一定只是用 **MAC** 密钥生成的 **MAC** 值，也可以通过生成摘要再签名的方式生成校验值。

在本步骤中，通过终端与后台系统服务器相互认证建立安全通道，认证通过以后即完成了持有该终端的商户在后台系统服务器的“签到”，即后台系统服务器认定了持有该终端的商户的合法性并与终端协商出第一会话密钥，以便利用该第一会话密钥实现了后台系统服务器与终端的交易数据交互时的加密传输，做好后续对智能密码设备对应的用户信息传输以及交易数据传输等操作的准备工作。之后该经过后台系统服务器认证的终端可以通过后台系统服务器对智能密码设备的合法性进行验证，并获取合法智能密码设备的相关用户信息。

2、终端与智能密码设备进行相互认证。

终端生成第三待签名信息。具体的，终端可以通过随机数生成器生成随机数作为第三待签名信息，也可以采用自身的序列号、**MAC** 地址或者其他的标识信息作为第三待签名信息，也可以是随机数和标识信息的组合作为第三待签名信息。其中，只要可以被智能密码设备进行签名的信息均可以作为第三待签名信息，以便智能密码设备返回签名信息后对智能密码设备进行认证。随机数可以为数字、字母、特殊字符等字符中的一种或任意几种的组合。

终端向智能密码设备发送第三待签名信息以及第二认证请求信息。具体的，终端可以通过无线通信链路将第三待签名信息以及第二认证请求信息向智能密码设备进行发送，以保证信息发送的便捷性；也可以通过有线接口将第三待签名信息以及第二认证请求信息向智能密码设备进行发送，以提高信息传输的安全性。

智能密码设备接收到第三待签名信息以及第二认证请求信息后，生成第四待签名信息。具体的，智能密码设备可以在接收到第二认证请求信息后，生成第四待签名信息，可以通过随机数生成器生成随机数作为第四待签名信息，也可以采用自身的序列号、**MAC** 地址或者其他的标识信息（例如设备访问码 **DAC**）作为第四待签名信息，也可以是随机数和标识

信息的组合作为第四待签名信息。其中，只要可以被终端进行签名的信息均可以作为第四待签名信息，以便终端返回签名信息后对终端进行认证。随机数可以为数字、字母、特殊字符等字符中的一种或任意几种的组合。

另外，智能密码设备在接收到第三待签名信息以及第二认证请求信息后，生成第四待签名信息的步骤中，智能密码设备还可以在接收到第二认证请求信息后，由休眠状态转换为唤醒状态。智能密码设备在唤醒状态下生成第四待签名信息。由休眠状态转换为唤醒状态以完成正常工作，并在智能密码设备完成工作后，再次切换为休眠状态，以减少电能损耗，延长使用寿命。

智能密码设备利用智能密码设备的私钥对第三待签名信息进行签名获得第二签名信息，并向终端发送第四待签名信息、第二签名信息以及智能密码设备证书。

终端接收到第四待签名信息、第二签名信息以及智能密码设备证书后，利用预存的智能密码设备证书对应的根证书验证智能密码设备证书是否合法。具体的，终端还需要获取智能密码设备证书对应的根证书，以便对智能密码设备证书进行合法性验证。

终端在验证智能密码设备证书合法后，利用智能密码设备证书中的公钥对第二签名信息进行验证。

终端在验证第二签名信息通过后，利用终端的私钥对第三待签名信息和第四待签名信息进行签名获得第三签名信息。具体的，终端在验证第二签名信息通过后，还对第三待签名信息和第四待签名信息进行签名，以保证第三待签名信息和第四待签名信息传输的安全性以及不可抵赖性，保证信息传输的合法来源。当然，终端还可以生成第一会话密钥生成因子，利用智能密码设备证书中的公钥对第一会话密钥生成因子进行加密获得第二加密信息，终端在验证智能密码设备证书以及智能密码设备的签名均通过后，生成终端与智能密码设备之间数据交互的会话密钥的生成因子（即第一会话密钥生成因子，该第一会话密钥生成因子用于生成终端与智能密码设备之间数据交互的会话密钥），同时，利用智能密码设备证书中的公钥对该第一会话密钥生成因子进行加密，以便保证第一会话密钥生成因子传输的安全性。

终端向智能密码设备发送第三签名信息以及终端证书。当然，如果终端还生成了第一会话密钥生成因子，并利用智能密码设备证书中的公钥对第一会话密钥生成因子进行加密获得第二加密信息，则在本步骤中，终端除了向后台系统服务器发送第三签名信息以及终端证书外，还向后台系统服务器发送第二加密信息。

智能密码设备接收到第三签名信息以及终端证书后，利用预存的终端证书对应的根证书验证终端证书是否合法。具体的，智能密码设备还需要获取到终端证书对应的根证书，

以便对终端证书进行合法性验证。当然，如果终端还向智能密码设备发送第二加密信息，则本步骤中，智能密码设备还接收终端发送的第二加密信息。

智能密码设备在验证终端证书合法后，利用终端证书中的公钥对第三签名信息进行验证。

- 5 智能密码设备在验证第三签名信息通过后，生成智能密码设备认证完成消息。具体的，智能密码设备在验证终端证书以及终端的签名信息均通过后，还生成智能密码设备认证完成消息，以便告知终端智能密码设备认证完成。当然，如果智能密码设备还接收到第二加密信息，则本步骤中，智能密码设备还生成第二会话密钥生成因子，利用终端证书中的公钥对第二会话密钥生成因子进行加密获得第三加密信息，其中，智能密码设备在验证终端
- 10 证书以及终端的签名信息均通过后，还生成终端与智能密码设备之间数据交互的会话密钥的生成因子（即第二会话密钥生成因子，该第二会话密钥生成因子用于生成终端与智能密码设备之间数据交互的会话密钥），同时，利用终端证书中的公钥对该第二会话密钥生成因子进行加密，以便保证第二会话密钥生成因子传输的安全性。

- 智能密码设备向终端发送智能密码设备认证完成消息。当然，如果智能密码设备还生
- 15 成了第二会话密钥生成因子，并对第二会话密钥生成因子进行加密获得第三加密信息，则本步骤中，智能密码设备除了向终端发送智能密码设备认证完成消息外，还向终端发送第三加密信息。

- 终端接收到智能密码设备认证完成消息后，验证智能密码设备认证完成消息。具体的，终端还认证智能密码设备认证完成消息，以确保认证完成消息的合法来源。当然，如果智
- 20 能密码设备还向终端发送了第三加密信息，则本步骤中，终端还接收第三加密信息。

- 终端在验证智能密码设备认证完成消息通过后，生成终端认证第二完成消息，向智能密码设备发送终端认证第二完成消息。具体的，终端在认证智能密码设备认证完成消息通过后，生成终端认证第二完成消息，以告知智能密码设备终端认证完成。当然，如果终端还接收到第三加密信息，则本步骤中，终端还根据第一会话密钥生成因子以及解密第三加
- 25 密信息获得的第二会话密钥生成因子生成第二会话密钥，以便与智能密码设备之间通过该第二会话密钥进行数据交互。

智能密码设备接收到终端认证第二完成消息后，验证终端认证第二完成消息。具体的，智能密码设备还认证终端认证第二完成消息，以确保认证完成消息的合法来源。

- 智能密码设备验证终端认证第二完成消息后，终端与智能密码设备完成相互认证。当
- 30 然，如果智能密码设备还生成了第二会话密钥生成因子且接收到了第二加密信息，则本步骤中，智能密码设备还根据第二会话密钥生成因子以及解密第二加密信息获得的第一会话

密钥生成因子生成第二会话密钥，以便与终端之间通过该第二会话密钥进行数据交互。

基于上述终端与智能密码设备之间的双向认证，可以确保双方合法性，提高后续处理的安全性。

当然，本发明并不局限于此种由终端发起的第二会话密钥生成过程，还可以由智能密码设备发起该第二会话密钥生成过程。

此外，第二会话密钥可以由终端或者智能密码设备中的任一方生成后，并以对方的公钥进行加密后发送给对方，减少一方的计算复杂度。

当然，本发明的终端与智能密码设备之间生成第二会话密钥的过程可以与上述终端与后台系统服务器之间生成第一会话密钥的过程相同。即第二会话密钥也可以通过分解共享主密钥的方式获得。

以下，给出一个具体的终端与智能密码设备之间认证并结合第二会话密钥生成的方式，当然本发明并不局限于此。

1) 终端向智能密码设备发送认证请求，并发送随机数 R01。

2) 处于休眠状态的智能密码设备在接收到终端发来的认证请求以后被唤醒。

3) 智能密码设备生成随机数 R02，并对 R01 进行摘要计算并用其私钥加密摘要生成签名 S01，智能密码设备将随机数 R02、签名 S01 以及智能密码设备证书发送给终端。

4) 终端使用终端内预存的智能密码设备证书对应的根证书验证智能密码设备证书的合法性。

如果验证智能密码设备证书不合法，则结束连接。

如果验证智能密码设备证书合法，则执行步骤 5)。

5) 终端验证签名 S01 是否正确，如果验证签名 S01 不正确，则结束连接；如果验证签名 S01 正确，则执行步骤 6)。

6) 终端将 R01、R02 连接起来组成 R01R02，对 R01R02 生成摘要并签名，得到签名 S02，生成随机数 R03，利用智能密码设备的公钥加密 R03 生成密文 E01。将 E01、终端证书和 S02 发送给智能密码设备。

7) 智能密码设备使用智能密码设备预存的终端证书对应的根证书验证终端证书的合法性。

如果验证终端证书不合法，则结束连接。

如果验证终端证书合法，则执行步骤 8)；

8) 智能密码设备验证签名 S02 是否正确；如果验证签名 S02 不正确，则结束连接；如果验证签名 S02 正确，则执行步骤 9)。

9) 智能密码设备生成随机数 R04, 利用终端的公钥对 R04 加密生成密文 E02, 将密文 E02 发给终端。

10) 终端生成认证完成消息, 终端对终端证书进行摘要运算得到 H01, 对智能密码设备证书进行摘要运算得到 H02, 将 R01、R02、E01, E02, H01、H02、S01、S02 连接后得到 T01, 然后对 T01 进行摘要并签名, 得到“后台认证完成消息” F01, 向智能密码设备发送 F01。

11) 智能密码设备收到 F01, 对 F01 进行验证。

如果验证 F01 不通过, 则返回错误信息结束连接。

如果验证 F01 通过, 则执行步骤 12)。

12) 智能密码设备以同样方式生成认证完成消息 F02, 并将生成的认证完成信息发送给终端。

13) 终端验证 F02。

如果验证 F02 不通过, 则返回错误信息结束连接。

如果验证 F02 通过, 则执行步骤 14)。

14) 智能密码设备与终端分别连接 R03、R04, 得到 R03|R04, 利用 R03|R04 生成第二会话密钥 K2 (该密钥可以仅为加密密钥), 配置为两者之后数据的安全传输。

由此可见, 终端与智能密码设备的相互认证过程 (过程二) 与后台和终端相互认证 (过程一) 不同之处在于:

过程一生成了加密密钥以及校验密钥 (例如 MACKEY), 过程二只生成了加密密钥, 没有生成校验密钥 (当然也可以生成校验密钥)。

校验密钥的作用是用来生成校验值, 校验值是用来校验数据传输过程中是否被篡改的。数据发送方采用特定算法利用校验密钥将传输的数据生成校验值, 数据接收方利用校验值和校验密钥来校验接收的数据是否被篡改。而针对于本发明终端与智能密码设备后续的流程, 终端与智能密码设备之间传输交易数据时, 用户可以通过智能密码设备上显示的信息进行人为判断数据是否正确, 所以无须再引入校验值; 对于终端也可以通过校验智能密码设备发来的签名来判断信息是否被篡改, 也无需引入校验值, 因此为了简化处理流程, 提高通信效率, 在生成第二会话密钥时, 可以不需要生成校验密钥。当然, 为了进一步提高安全性, 也可以生成校验密钥。

对于后台系统服务器和终端之间, 因为后台系统服务器并不知晓交易具体内容, 为保证安全, 则需通过引入校验值的方式来判断数据是否被篡改。

由此可见, 过程一是通过一方产生共享主密钥, 再采用特殊的算法对共享主密钥进行

处理，而分解得到加密密钥和校验密钥；过程二是认证双方各产生一个加密密钥的组成因子，最后合成加密密钥。当然，过程一中采用的会话密钥生成方式与过程二中采用的会话密钥生成方式既可以用于终端与后台系统服务器之间会话密钥的生成，也可以用于终端与智能密码设备之间会话密钥的生成。

- 5 由此，在终端与智能密码设备进行了双向认证后，可以防范钓鱼风险，防止传输信息的篡改、远程劫持和中间人攻击等交易风险，从而有效的保障终端与智能密码设备的资金安全。

在本步骤中，可以仅构建后台系统服务器与终端之间进行相互认证的方法体系，建立二者之间的安全通道。也可以仅构建终端与智能密码设备之间进行相互认证的方法体系，
10 建立二者之间的安全通道。还可以构建后台系统服务器、终端、智能密码设备三者之间进行相互认证的方法体系，建立三者之间的安全通道。基于上述三种中的任一种相互认证的方法体系，可以防范钓鱼风险，防止交易信息篡改、远程劫持和中间人攻击等交易风险，从而有效保障持有智能密码设备的用户与持有终端的商户的账户资金安全。

- 此外，本发明并不局限于本步骤三在步骤二之后完成，也可以在步骤二之前完成或者
15 与步骤二同时完成，只要在步骤四之前完成认证即可。

当然，本发明中的第一会话密钥可以预存在后台系统服务器和终端中，也可以通过后台系统服务器和终端协商生成，在协商生成第一会话密钥时，可以在终端与后台系统服务器进行认证的过程中协商生成（参见上述终端与后台系统服务器进行相互认证的流程）。

- 当然，本发明中后台系统服务器与终端之间传输的所有信息均可以通过第一会话密钥
20 加密计算和/或校验计算后传输。

本发明中的第二会话密钥可以预存在终端和智能密码设备中，也可以通过终端和智能密码设备协商生成，在协商生成第二会话密钥时，可以在终端与智能密码设备进行认证的过程中协商生成（参见上述终端与智能密码设备进行相互认证的流程）。

- 当然，本发明中终端与智能密码设备之间传输的所有信息也均可以通过第二会话密钥
25 加密计算和/或校验计算后传输。

步骤四：终端获取用户信息。

具体的，本步骤中，终端根据扫描到的智能密码设备的标识信息获取智能密码设备对应的用户信息（例如，可以是用户的照片、姓名、账号等信息），具体可以通过但不限于以下方式一和方式二获取智能密码设备对应的用户信息。

- 30 方式一、终端从后台系统服务器获取智能密码设备对应的用户信息。

终端向后台系统服务器发送智能密码设备的标识信息以及用户信息读取请求。具体的，

在终端向后台系统服务器发送智能密码设备的标识信息以及用户信息读取请求时，可以直接向后台系统服务器发送智能密码设备的标识信息以及用户信息读取请求，也可以利用第一会话密钥对智能密码设备的标识信息和/或用户信息读取请求进行加密计算和/或校验计算后再发送，以保证信息传输的安全性和完整性。

- 5 后台系统服务器接收到智能密码设备的标识信息以及用户信息读取请求后，根据智能密码设备的标识信息获取与智能密码设备对应的用户信息。具体的，后台系统服务器预存了已注册的每个智能密码设备对应的用户信息，以便根据接收到的智能密码设备的标识信息获得该智能密码设备对应的用户信息。当然，如果终端向后台系统服务器发送了加密计算和/或校验计算后的信息，那么本步骤中，后台系统服务器还需要利用第一会话密钥对接
- 10 收到的信息进行解密和/或校验验证计算无误后，获得完整的智能密码设备的标识信息和/或用户信息读取请求。

- 此外，为了确保数据交互的安全性以及智能密码设备的合法性，后台系统服务器在接收到智能密码设备的标识信息以及用户信息读取请求后，还判断智能密码设备的标识信息是否包含在后台系统服务器中预存的智能密码设备异常名单中；后台系统服务器在判断出
- 15 智能密码设备的标识信息在智能密码设备异常名单中后，获取锁定智能密码设备指令，以及利用后台系统服务器的私钥对锁定智能密码设备指令进行签名获得第五签名信息，并通过终端向智能密码设备发送锁定智能密码设备指令以及第五签名信息；智能密码设备接收到锁定智能密码设备指令以及第五签名信息后，利用预存的后台系统服务器证书中的公钥对第五签名信息进行验证；智能密码设备在验证第五签名信息通过后，根据锁定智能密码
- 20 设备指令执行锁定操作。

- 具体的，智能密码设备异常名单可以为黑名单、挂失名单、失效名单等任意表示智能密码设备身份非法的名单；如果智能密码设备的标识信息在智能密码设备异常名单中，则说明该智能密码设备是非法的智能密码设备，此时，为了确保安全性，后台系统服务器通过终端向该非法智能密码设备发送锁定指令以锁定该非法智能密码设备，同时，后台系统
- 25 服务器还对该锁定指令进行签名，以确保锁定指令的合法来源，避免非法锁定智能密码设备的恶意操作。

当然，本发明并不局限于此，对于实际应用来说，只要可以合法锁定非法智能密码设备即可。

- 另外，后台系统服务器也可以不对锁定指令进行签名，仅发送锁定指令至非法终端以
- 30 锁定该非法终端。

智能密码设备根据锁定智能密码设备指令执行锁定操作可以包括：智能密码设备拒绝

执行任何请求，销毁自身存储的证书等任意方式。

当然，后台系统服务器在发送锁定指令后，还可以执行拒绝该非法智能密码设备的任何请求。

可见，采用本发明实施例提供的方法，当用户遗失了智能密码设备后可以向后台系统服务器进行挂失，后台系统服务器将该智能密码设备的设备识别码登记到挂失名单上；或者出现账户异常遭到举报等情况，后台系统服务器也会将这些智能密码设备登记在黑名单中。这些异常名单中的设备都会作为异常设备登记在异常名单上。每次交易之前，后台系统服务器会对智能密码设备进行认证，认证过程中会将该设备标识与异常名单比对，若在名单上即对该智能密码设备进行锁定。应用该方法，若有人盗用他人的智能密码设备，并企图非法使用该智能密码设备进行转账盗取用户资金时，由于后台系统服务器每次交易之前都会对智能密码设备进行认证，后台系统服务器可以远程将这个智能密码设备锁定，因此即使该智能密码设备被别人被非法盗用也能保障用户账户不受损失。

此外，本发明中，后台系统服务器通过终端向智能密码设备发送锁定智能密码设备指令以及第五签名信息时，还可以利用第一会话密钥对锁定智能密码设备指令以及第五签名信息进行加密计算和/或校验计算，以便保证锁定智能密码设备指令以及第五签名信息传输的安全性和/或完整性，终端接收到经加密计算和/或校验计算后的信息后，利用第一会话密钥进行解密计算和/或校验验证计算后，获得锁定智能密码设备指令以及第五签名信息。当然，终端在获得锁定智能密码设备指令以及第五签名信息后，还可以利用第二会话密钥对锁定智能密码设备指令以及第五签名信息进行加密计算和/或校验计算后，将加密计算和/或校验计算后的信息发送至智能密码设备，以保证信息传输的安全性和/或完整性，智能密码设备在接收到终端发送的信息后，进行解密计算和/或校验验证计算，以获得锁定智能密码设备指令以及第五签名信息。

另外，为了保证用户信息的安全性，后台系统服务器还需要通过智能密码设备持有者的授权才能将该智能密码设备对应的用户信息发送给终端。后台系统服务器通过终端向智能密码设备发送用户授权请求信息（例如，该用户授权请求信息可以是随机数）。智能密码设备接收到用户授权请求信息后，生成授权信息（例如，该授权信息可以是对该随机数进行签名后得到的信息），并通过终端向后台系统服务器发送授权信息。后台系统服务器接收到授权信息后，执行后台系统服务器向终端发送用户信息读取请求的响应信息的步骤。当然，后台系统服务器还可以利用后台系统服务器的私钥将用户授权请求信息进行签名后，通过终端向智能密码设备进行发送，智能密码设备接收到签名的信息后，对签名进行验证，验证通过后则认为用户授权请求信息是来自于合法的后台系统服务器，并对该请求进行确

认以授权后台系统服务器。智能密码设备也可以利用智能密码设备的私钥对授权信息进行签名后通过终端发送给后台系统服务器，后台系统服务器接收到签名的信息后，对签名进行验证，验证通过后则认为授权信息是来自于正确的智能密码设备，以根据授权信息进行后续操作。后台系统服务器还可以利用第一会话密钥对用户授权请求信息进行加密计算和/或校验计算后发送给终端，终端利用第一会话密钥对接收到的信息进行解密计算和/或校验验证计算。终端利用第二会话密钥对用户授权请求信息进行加密计算和/或校验计算后发送给智能密码设备，智能密码设备利用第二会话密钥对接收到的信息进行解密计算和/或校验验证计算。后台系统服务器还可以利用后台系统服务器的私钥对用户授权请求信息进行签名后再利用第一会话密钥进行加密计算和/或校验计算，终端利用第一会话密钥对接收到的信息进行解密计算和/或校验验证计算。终端利用第二会话密钥对后台系统服务器签名后的信息进行加密计算和/或校验计算后发送至智能密码设备，智能密码设备利用第二会话密钥对接收到的信息进行解密计算和/或校验验证计算，并对签名进行验签。以上仅是后台系统服务器向智能密码设备请求授权的几种方式，本发明并不局限于此，以上的各类变形组合也应属于本发明的保护范围。

当然，在智能密码设备在接收到用户授权请求信息后，还可以由休眠状态转换为唤醒状态；智能密码设备在唤醒状态下生成授权信息。以便节省电能，延长智能密码设备的使用寿命。

后台系统服务器根据用户信息获得用户信息读取请求的响应信息，并向终端发送用户信息读取请求的响应信息；当然，还可以利用第一会话密钥对用户信息进行加密计算和/或校验计算，以保证用户信息传输的安全性和/或完整性。

终端接收到用户信息读取请求的响应信息后，根据用户信息读取请求的响应信息获得用户信息；当然，如果终端收到的是对用户信息进行加密计算和/或校验计算后得到的信息，在本步骤中终端还利用第一会话密钥对用户信息读取请求的响应信息进行解密计算和/或校验验证计算后获得用户信息。

方式二、终端从智能密码设备获取智能密码设备对应的用户信息。

终端根据扫描到的智能密码设备的标识信息向智能密码设备发送用户信息读取请求。具体的，终端可以直接向智能密码设备发送用户信息读取请求，也可以利用第二会话密钥对用户信息读取请求进行加密计算和/或校验计算后再发送，以保证信息传输的安全性和完整性。

智能密码设备获得预先存储的用户信息，并根据用户信息获得用户信息读取请求的响应信息，并向终端发送用户信息读取请求的响应信息。具体的，智能密码设备可以直接将

获取到的用户信息发送给终端，也可以利用第二会话密钥对获取到的用户信息进行加密计算和/或校验计算后获得用户信息读取请求的响应信息发送给终端。

- 终端接收到用户信息读取请求的响应信息后，根据用户信息读取请求的响应信息获得用户信息。当然，如果终端收到的是对用户信息进行加密计算和/或校验计算后得到的信息，
- 5 在本步骤中终端还利用第二会话密钥对用户信息读取请求的响应信息进行解密计算和/或校验验证计算后获得用户信息。

此外，如果智能密码设备的持有者拒绝发送用户信息，则可以通过智能密码设备上设置的按键或者通过软件控制向终端发送拒绝信息，以保证用户信息的安全。当然，该拒绝信息也可以通过第二会话密钥加密计算和/或校验计算后发送。

- 10 终端将用户信息存储到预先建立的当前用户列表中。具体的，由于终端所在店铺内容流量的变化、人员的流动，探测到的智能密码设备也是不断变化的，此时，该当前用户列表可以通过但不限于如下两种方式进行更新。

更新方式一：

- 15 终端获得在终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表。

终端根据预设的时间间隔将实时标识列表中的智能密码设备的标识信息与当前用户列表中的智能密码设备的标识信息进行比对。

- 如果实时标识列表中的智能密码设备的标识信息不在当前用户列表中，则执行终端根据扫描到的智能密码设备的标识信息获取智能密码设备对应的用户信息的步骤；且如果当前用户列表中的智能密码设备的标识信息不在实时标识列表中，则删除当前用户列表中不在实时标识列表中的智能密码设备的用户信息。
- 20

通过本方式对当前用户列表进行更新，可以保证在终端信号覆盖范围内的智能密码设备对应的用户信息可以及时更新到当前用户列表中，对于离开终端信号覆盖范围内的智能密码设备对应的用户信息可以及时从当前用户列表中删除，保证安全性。

- 25 更新方式二：

终端获得在终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表。

终端根据预设的时间间隔将实时标识列表中的智能密码设备的标识信息与当前用户列表中的智能密码设备的标识信息进行比对。

- 30 如果实时标识列表中的智能密码设备的标识信息不在当前用户列表中，则执行终端根据扫描到的智能密码设备的标识信息获取智能密码设备对应的用户信息的步骤，并在终端

获得用户信息后，将用户信息存储至实时标识列表中；且如果实时标识列表中的智能密码设备的标识信息在当前用户列表中，则将在当前用户列表中的智能密码设备的用户信息存储至实时标识列表中。

将实时标识列表作为更新后的当前用户列表。

5 通过本方式对当前用户列表进行更新，可以仅将在终端的信号覆盖范围内的智能密码设备对应的用户信息进行及时更新，提高更新效率。利用本方式，终端在获取用户信息时，可以将店内原有智能密码设备对应的用户信息直接从原有的当前用户列表中复制到实时标识列表中，新进店的顾客对应的用户信息可以通过向后台系统服务器或者智能密码设备提出用户信息读取请求来获得。

10 由此可见，当终端所在店铺客流量发生变化时，不需要商户进行任何操作，当前用户列表可以自动进行更新，方便了商户的店员对顾客的信息管理维护。

另外，终端可以将所存储的当前用户列表中用户对应的用户信息显示出来，以便智能密码设备的持有者查看该用户信息，确保交易的正确性。

现有技术中，交易过程均需要 SIM 卡或智能卡等具备账户存储功能的设备，用户需要
15 进行刷卡刷手机等操作，如此商户才能获得用户的账户信息。

区别于现有技术，商户的终端可以通过先读取智能密码设备的标识信息，再利用该智能密码设备的标识信息获取智能密码设备对应的用户信息。因此，顾客可以无需借助钱包、信用卡、手机等方式来支付商品，从而简化了顾客与商户的交互操作，提升了用户体验。

步骤五：交易信息处理。

20 终端根据待交易的智能密码设备对应的用户信息生成交易信息，并根据交易信息获得交易请求信息。具体的，交易信息可以包含交易金额、收付款双方的账号信息、收付款双方的标识信息等信息，交易信息中还可以包括电子对账单，用户可以根据电子对账单审核交易细节，例如，具体交易时间、交易单号，交易金额、购买的物品等。当然，终端还可以利用第二会话密钥对交易信息进行加密计算和/或校验计算以确保交易信息传输的安全
25 性和/或完整性。

终端向智能密码设备发送交易请求信息。具体的，终端可以通过但不限于如下方式发送交易请求信息：终端对交易请求信息进行编码后通过声波信号发送；或者终端对交易请求信息进行图形编码后并显示以便智能密码设备进行图像采集；或者终端通过终端与智能密码设备匹配的通信接口发送交易请求信息。

30 智能密码设备接收到交易请求信息后，根据交易请求信息获得交易信息。当然，如果智能密码设备接收到的是终端通过第二会话密钥对交易信息进行加密计算和/或校验计算

得到的交易请求信息，则在本步骤中，智能密码设备还利用第二会话密钥对交易请求信息进行解密计算和/或校验验证计算获得交易信息，以保证交易信息传输的安全性和/或完整性。

5 为了节约智能密码设备的电能，延长使用寿命，智能密码设备还可以在接收到交易请求信息后，由休眠状态转换为唤醒状态。智能密码设备在唤醒状态下根据交易请求信息获得交易信息，当然，智能密码设备还可以在唤醒状态下利用第二会话密钥对交易请求信息进行解密计算和/或校验验证计算获得交易信息。

智能密码设备提示交易信息。具体的，智能密码设备可以通过显示屏将交易信息显示出来，也可以通过扬声器等将交易信息以语音的方式播放出来。当然，智能密码设备还可以通过其他方式提示用户以获知真实的交易信息，确保交易的安全。此外，智能密码设备10 获取到交易信息后，还可以对交易信息进行关键信息的提取，智能密码设备仅对关键信息进行提示，具体提示方式可以参见智能密码设备对交易信息的提示方式。

智能密码设备接收确认指令，并生成交易确认信息。具体的，智能密码设备可以通过检测到设置在智能密码设备上的确认键被按下时发送的信息接收确认指令，也可以通过检测15 到触摸屏上显示的虚拟确认键被点击时发送的信息接收确认指令，还可以通过检测到的语音、指纹、虹膜等生物特征信息作为确认指令等任意方式。进一步，智能密码设备可以通过但不限于如下方式生成交易确认信息：智能密码设备利用智能密码设备的私钥对交易信息进行签名，生成交易签名信息作为交易确认信息；或者智能密码设备生成动态口令作为交易确认信息，当然上述交易确认信息还可以是利用第二会话密钥加密计算和/或校验计算20 后的信息。当然，为了防止重复交易，保证用户的账户安全，在智能密码设备每次生成交易确认信息时，智能密码设备还生成单次交易标识，并利用智能密码设备的私钥对交易信息以及单次交易标识进行签名，生成交易签名信息作为交易确认信息。或者智能密码设备生成单次交易标识，利用智能密码设备的私钥对单次交易标识进行签名获得单次交易标识的签名信息，并生成动态口令，将单次交易标识的签名信息以及动态口令作为交易确认25 信息，以保证一次交易仅被成功执行一次，其中单次交易标识可以为随机数等，当然上述交易确认信息也可以是利用第二会话密钥加密计算和/或校验计算后的信息。由于无线网络传输线路不稳定，可能出现智能密码设备收不到回执的情况，如果不设置单次交易标识，终端在没有收到智能密码设备的签名信息时，可能需要持有该智能密码设备的用户多次进行确认签名操作，也就是智能密码设备多次向终端发送签名信息，那么就有可能造成终端30 可以利用这多个签名值生成多个交易数据包发送给后台系统服务器，从而对智能密码设备对应的账户进行重复扣款。而如果设置了单次交易标识，当出现线路不稳定时，智能密码

设备就会继续再对交易信息和同一个单次交易标识进行签名再发送给终端，直到收到回执为止。终端用智能密码设备发来的签名值生成交易数据包，后台系统服务器收到交易数据包会对里面的单次交易标识进行判定，若此单次交易标识已经保存在交易日志中，也就是说已经交易过了，就不会再对这个交易数据包进行处理，不会造成多次或者重复扣款，从而保护了智能密码设备用户的账户资金安全。

终端接收交易确认信息。具体的，终端可以通过但不限于如下方式接收交易确认信息：终端接收智能密码设备发送的声波信号并对声波信号进行解码获得交易确认信息（例如，可以采用声波识别设备对声波信号进行识别，采用声波解码器对声波信号进行解码获得交易确认信息）；或者终端采集智能密码设备显示的图像信息并对图像信息（例如，二维码、条形码等）进行解码获得交易确认信息（例如采用图像采集设备对图像信息进行采集，采用解码器对图像信息进行解码后获得交易确认信息）；或者终端通过终端与智能密码设备匹配的通信接口接收交易确认信息；或者终端通过终端输入的信息获得交易确认信息。如果交易确认信息是利用第二会话密钥加密计算和/或校验计算得到的，那么本步骤中，还利用第二会话密钥对计算后的信息进行解密计算和/或校验验证计算。

终端根据交易确认信息获得交易数据包，并向后台系统服务器发送交易数据包。具体的，交易数据包中也可以包括交易信息等其他信息。交易信息可以包含交易金额、收付款双方的账号信息、收付款双方的标识信息等信息，交易信息中还可以包括电子对账单，用户可以根据电子对账单审核交易细节，例如，具体交易时间、交易单号，交易金额、购买的物品等。当然，终端还可以利用第一会话密钥对交易确认信息或者对交易确认信息解密后的信息进行加密计算和/或校验计算，以保证信息传输的安全性和/或完整性。

后台系统服务器接收到交易数据包后，根据交易数据包获得交易确认信息；当然，后台系统服务器还可以利用第一会话密钥对交易数据包进行解密计算和/或校验验证计算获得交易确认信息。

后台系统服务器对交易确认信息进行验证，并在验证通过后执行交易。具体的，后台系统服务器只有在验证交易确认信息验证通过后，才说明本次交易经过了合法的智能密码设备的确认，并根据确认后的结果执行交易。当然，为了保证智能密码设备的持有者知晓交易已经完成，后台系统服务器还可以通过终端向智能密码设备发送交易成功回执信息。智能密码设备接收到交易成功回执信息后，提示交易成功回执信息，交易成功回执信息中还可以包括电子对账单，用户可以根据电子对账单审核交易细节，例如，具体交易时间、交易单号，交易金额、购买的物品等。另外，后台系统服务器还可以向终端发送交易成功回执信息，以便终端获知交易完成。当然，交易成功回执信息可以利用第一会话密钥加密

计算和/或校验计算后发送给终端，终端解密计算和/或校验验证计算后利用第二会话密钥进行加密计算和/或校验计算后发送给智能密码设备，智能密码设备解密计算和/或校验验证计算后提示给用户知晓；交易成功回执信息也可以是后台系统服务器利用后台系统服务器的私钥进行签名后通过终端发送给智能密码设备，智能密码设备对签名的信息进行验签通过后提示给用户知晓；还可以是后台系统服务器签名后利用第一会话密钥加密计算和/或校验计算后发送给终端，终端解密计算和/或校验计算后利用第二会话密钥加密计算和/或校验计算后发送给智能密码设备，智能密码设备解密计算和/或校验验证计算后并验签通过后提示给用户知晓。

步骤六：退款。

当顾客需要退款时，可以执行但不限于如下几种方式以实现退款操作。

方式一、终端向智能密码设备发送退款信息。具体的，退款信息可以包括：退款双方的账号、退款金额、退款交易单号、退款双方的标识信息等任意组合。退款信息中还可以包括电子对账单，用户可以根据电子对账单审核退款细节，例如，具体退款时间、退款交易单号，退款金额、退换的物品等。当然，该退款信息还可以通过第二会话密钥进行加密计算和/或校验计算后发送至智能密码设备，以保证信息传输的安全性和/或完整性。终端还可以通过但不限于如下方式发送退款信息：终端对退款信息进行编码后通过声波信号发送；或者终端对退款信息进行图形编码后并显示以便智能密码设备进行图像采集；或者终端通过终端与智能密码设备匹配的通信接口发送退款信息。

智能密码设备接收到退款信息后，提示退款信息。具体的，智能密码设备在接收到退款信息后，将该退款信息通过语音播放或者显示屏显示等任意方式提示给用户知晓，以便用户确定该退款信息是真实的退款信息。当终端利用第二会话密钥对退款信息进行加密计算和/或校验计算后，本步骤还需利用第二会话密钥对接收到的信息进行解密计算和/或校验验证计算。

为了节约智能密码设备的电能，延长使用寿命，智能密码设备还可以在接收到退款信息后，由休眠状态转换为唤醒状态；智能密码设备在唤醒状态下提示退款信息。

智能密码设备接收退款确认指令，并利用智能密码设备的私钥对退款信息进行签名，生成退款确认信息。具体的，用户在确定了退款信息是真实的退款信息后，通过智能密码设备上设置的实体按键或者虚拟按键等方式进行确认。智能密码设备在向终端发送退款确认信息后（例如，发送退款确认信息对应的声波信号后，或者显示退款确认信息对应的图像信息达到预定的时间后），由唤醒状态转换为休眠状态。

终端接收退款确认信息，对退款确认信息进行验证，并在验证通过后，利用终端的私

钥对退款确认信息进行签名生成退款确认包。具体的，终端可以通过但不限于如下方式接收退款确认信息：终端接收智能密码设备发送的声波信号并对声波信号进行解码获得退款确认信息（例如，可以采用声波识别设备对声波信号进行识别，采用声波解码器对声波信号进行解码获得退款确认信息）；或者终端采集智能密码设备显示的图像信息并对图像信息（例如，二维码、条形码等）进行解码获得退款确认信息（例如采用图像采集设备对图像信息进行采集，采用解码器对图像信息进行解码后获得退款确认信息）；或者终端通过终端与智能密码设备匹配的通信接口接收退款确认信息。此外，终端利用智能密码设备的公钥对退款确认信息进行验证。

终端向后台系统服务器发送退款确认包和退款确认信息。具体的，终端可以向后台系统服务器直接发送退款确认包和退款确认信息，终端也可以利用第一会话密钥对退款确认包和退款确认信息进行加密计算和/或校验计算后发送至后台系统服务器，以保证信息传输的安全性和/或完整性。

后台系统服务器接收到退款确认包和退款确认信息后，分别对退款确认包和退款确认信息进行验证，并在全部验证通过后，执行退款操作。具体的，如果终端利用了第一会话密钥对退款确认包和退款确认信息进行了加密计算和/或校验计算，那么本步骤中，后台系统服务器还利用第一会话密钥对接收到的信息进行解密计算和/或校验验证计算。此外，后台系统服务器还利用终端的公钥对退款确认包进行验证，利用智能密码设备的公钥对退款确认信息进行验证。

以下针对方式一，提供一种退款的应用场景，但本发明并不局限于此。

店铺根据顾客的退款意向，由终端生成退款信息（该退款信息可以通过查找已记录的交易信息获得，也可以是重新生成的一个退款信息或其他形式的退款信息），并使用终端和智能密码设备之间的第二会话密钥加密退款信息，并发送给智能密码设备。

智能密码设备在接收到加密后的退款信息后，由休眠状态转换为唤醒状态，并利用第二会话密钥解密该加密退款信息，获得退款信息，并对退款信息进行显示，以供顾客进行确认。

顾客确认该退款信息正确，按下智能密码设备上的确认键进行确认，智能密码设备接收到该退款确认指令后，利用智能密码设备的私钥对退款信息进行签名得到退款确认信息，并利用第二会话密钥对退款确认信息进行加密，发送给终端。

终端接收到加密后的退款确认信息后，利用第二会话密钥解密此信息，获得退款确认信息，并利用智能密码设备的公钥验证退款确认信息的正确性，若正确，终端利用终端的私钥对退款确认信息再进行签名得到退款确认包，当然，终端还可以直接对退款信息进行

签名得到退款确认包。

终端利用第一会话密钥对退款确认包和退款确认信息进行加密后发送至后台系统服务器。

5 后台系统服务器接收到加密后的信息后，利用第一会话密钥对接收到的信息进行解密，并利用终端的公钥对退款确认包进行验证，利用智能密码设备的公钥对退款确认信息进行验证，并在二者验证均通过后，执行退款操作，并发送退款成功回执信息给终端和/或智能密码设备。

方式二、该方式二与方式一的区别在于：在终端向智能密码设备发送退款信息之前，该终端还接收该智能密码设备发送的退款请求，并根据退款请求生成退款信息。具体的，
10 顾客可以通过按下智能密码设备上的按键以生成退款请求，智能密码设备接收到该退款请求后，将该退款请求发送给该终端。退款信息中还可以包括电子对账单，用户可以根据电子对账单审核退款细节，例如，具体退款时间、退款交易单号，退款金额、退换的物品等。当然，任何可以触发智能密码设备生成退款请求的实现方式都属于本发明的保护范围内。

为了节约智能密码设备的电能，延长使用寿命，智能密码设备还可以在向终端发送退款请求前，由休眠状态转换为唤醒状态；智能密码设备在唤醒状态下向终端发送退款请求。
15 智能密码设备发送退款请求之后，由唤醒状态转换为休眠状态。当智能密码设备接收到终端发送的退款信息时，由休眠状态转换为唤醒状态，在唤醒状态下执行提示退款信息和生成退款确认信息的操作。智能密码设备在向终端发送退款确认信息后（例如，发送退款确认信息对应的声波信号后，或者显示退款确认信息对应的图像信息达到预定的时间后），由
20 唤醒状态转换为休眠状态。

方式三、智能密码设备向终端发送退款请求。具体的，顾客可以通过按下智能密码设备上的按键以生成退款请求，智能密码设备接收到该退款请求后，将该退款请求发送给该终端。当然，任何可以触发智能密码设备生成退款请求的实现方式都属于本发明的保护范围内。

25 为了节约智能密码设备的电能，延长使用寿命，智能密码设备还可以在向终端发送退款请求前，由休眠状态转换为唤醒状态；智能密码设备在唤醒状态下向终端发送退款请求。

终端生成退款请求标识，并向智能密码设备发送退款请求标识。具体的，终端可以生成随机数，将该随机数作为退款请求标识，该随机数用于提供给智能密码设备以生成退款信息。

30 智能密码设备接收到退款请求标识后，生成退款信息，并利用智能密码设备的私钥对退款信息进行签名，得到退款确认信息，并向终端发送退款确认信息。具体的，智能密码

设备利用该退款请求标识、退款金额、退款账户等信息生成退款信息，该退款信息还可以包括退款交易单号、退款双方的标识信息等任意组合。其中，退款金额可以通过智能密码设备上的按键进行输入，当然，也可以通过其他方式（例如，语音输入）输入。退款账户可以通过智能密码设备上的按键进行输入，还可以通过读取预先存储在智能密码设备中的退款账户来输入。当然，还可以在交易完成后，在智能密码设备上保存交易信息，通过查询交易信息以获得退款金额和退款账户等信息。当然，该退款信息还可以通过第二会话密钥进行加密计算和/或校验计算后发送至终端，以保证信息传输的安全性和/或完整性。智能密码设备还可以通过但不限于如下方式发送退款信息：智能密码设备对退款信息进行编码后通过声波信号发送；或者智能密码设备对退款信息进行图形编码后并显示以便终端进行图像采集；或者智能密码设备通过智能密码设备与终端匹配的通信接口发送退款信息。

为了节约智能密码设备的电能，延长使用寿命，智能密码设备还可以在向终端发送退款确认信息后（例如，发送退款确认信息对应的声波信号后，或者显示退款确认信息对应的图像信息达到预定的时间后），由唤醒状态转换为休眠状态。

终端接收退款确认信息，对退款确认信息进行验证，并在验证通过后，利用终端的私钥对退款确认信息进行签名生成退款确认包。具体的，当智能密码设备利用第二会话密钥对退款信息进行加密计算和/或校验计算后，本步骤还需利用第二会话密钥对接收到的信息进行解密计算和/或校验验证计算。终端可以通过但不限于如下方式接收退款确认信息：终端接收智能密码设备发送的声波信号并对声波信号进行解码获得退款确认信息（例如，可以采用声波识别设备对声波信号进行识别，采用声波解码器对声波信号进行解码获得退款确认信息）；或者终端采集智能密码设备显示的图像信息并对图像信息（例如，二维码、条形码等）进行解码获得退款确认信息（例如采用图像采集设备对图像信息进行采集，采用解码器对图像信息进行解码后获得退款确认信息）；或者终端通过终端与智能密码设备匹配的通信接口接收退款确认信息。此外，终端利用智能密码设备的公钥对退款确认信息进行验证。

终端向后台系统服务器发送退款确认包和退款确认信息。具体的，终端直接向后台系统服务器发送退款确认包和退款确认信息，终端也可以利用第一会话密钥对退款确认包和退款确认信息进行加密计算和/或校验计算后发送至后台系统服务器，以保证信息传输的安全性和/或完整性。

后台系统服务器接收到退款确认包和退款确认信息后，分别对退款确认包和退款确认信息进行验证，并在全部验证通过后，执行退款操作。具体的，如果终端利用了第一会话密钥对退款确认包和退款确认信息进行了加密计算和/或校验计算，那么本步骤中，后台系

统服务器还利用第一会话密钥对接收到的信息进行解密计算和/或校验验证计算。此外，后台系统服务器还利用终端的公钥对退款确认包进行验证，利用智能密码设备的公钥对退款确认信息进行验证。

以下针对方式三，提供一种退款的应用场景，但本发明并不局限于此。

- 5 智能密码设备由休眠状态转换为唤醒状态。例如，可以通过持有该智能密码设备的顾客的按键操作使得智能密码设备进入唤醒状态。

顾客可以通过按下智能密码设备上的按键以生成退款请求，智能密码设备接收到该退款请求后，将该退款请求发送给该终端。

- 10 终端可以生成随机数 R ，将该随机数作 R 为退款请求标识，并向智能密码设备发送退款请求标识。

- 智能密码设备生成退款信息，并利用智能密码设备的私钥对退款信息进行签名，得到退款确认信息，并向终端发送退款确认信息；其中，该退款信息至少包括：退款请求标识、退款金额、退款账户等信息。其中，退款金额、退款账户等信息可以由顾客通过智能密码设备上的按键进行输入，或者退款金额可以由顾客通过智能密码设备上的按键输入，退款
15 账户从智能密码设备预存的信息中读取获得，或者退款金额、退款账户等信息均可以从智能密码设备预存的信息中读取获得，智能密码设备使用终端和智能密码设备之间的第二会话密钥加密退款确认信息，并发送给终端。

- 终端接收到加密后的退款确认信息后，利用第二会话密钥解密此信息，获得退款确认信息，并利用智能密码设备的公钥验证退款确认信息的正确性，若正确，终端利用终端的
20 私钥对退款确认信息再进行签名得到退款确认包，当然，终端还可以直接对退款信息进行签名得到退款确认包。

终端利用第一会话密钥对退款确认包和退款确认信息进行加密后发送至后台系统服务器。

- 后台系统服务器接收到加密后的信息后，利用第一会话密钥对接收到的信息进行解密，
25 并利用终端的公钥对退款确认包进行验证，利用智能密码设备的公钥对退款确认信息进行验证，并在二者验证均通过后，执行退款操作，并发送退款成功回执信息给终端和/或智能密码设备。

- 以上三种退款方式中，退款确认包或者退款确认信息中还可以包含单次退款标识，该单次退款标识可以为随机数，以保证一次退款仅被成功执行一次。当然，该单次退款标识
30 可以由终端生成，也可以由智能密码设备生成，可以在退款确认包中被终端签名，也可以在退款确认信息中被智能密码设备签名。

当然，后台系统服务器在执行退款操作后，还可以向终端和/或智能密码设备发送退款成功回执信息，以便店铺和/或顾客可以得知退款成功。

由此可见，通过上述退款流程，可以大大简化顾客在退款过程中的操作，应用智能密码设备相关的安全功能保障顾客退款过程的安全性，为消费者带来无缝使用体验。

5 步骤七：销户。

本发明实施例听销户包括终端的销户和智能密码设备的销户，以下先对终端的销户进行说明。

终端获取终端销户申请，利用终端的私钥对销户申请进行签名获得第六签名信息，并向后台系统服务器发送终端销户申请以及第六签名信息。具体的，终端可以直接向后台系统服务器发送销户申请以及第六签名信息，终端也可以利用第一会话密钥对第六签名信息进行加密计算和/或校验计算，并将计算后的信息发送至后台系统服务器，以保证信息传输的安全性和/或完整性。

后台系统服务器接收到终端销户申请以及第六签名信息后，利用预存的终端证书中的公钥对第六签名信息进行验证。具体的，如果终端还利用第一会话密钥进行了加密计算和/或校验计算，在本步骤中，后台系统服务器还利用第一会话密钥对接收到的信息进行解密计算和/或校验验证计算。

后台系统服务器在验证第六签名信息通过后，删除预存的终端证书，并生成终端销户完成信息，向终端发送终端销户完成信息。具体的，后台系统服务器在进行销户时，除了删除预存的终端证书外，还可以将该终端对应的信息放到后台系统服务器预设的销户列表里等其他销户操作。另外，销户完成信息也可以是利用第一会话密钥进行加密计算和/或校验计算得到的，也可以是利用后台系统服务器的私钥进行签名得到的，或者利用后台系统服务器的私钥进行签名后再利用第一会话密钥进行加密计算和/或校验计算得到的。

终端接收到终端销户完成信息后，删除终端的私钥。具体的，终端接收到终端销户完成信息后，删除私钥，当然，还可以拒绝执行任何与发送该终端销户完成信息的后台系统服务器有关的交易操作。此外，终端还可以利用第一会话密钥进行解密计算和/或校验验证计算和/或验签操作等。

以下对智能密码设备的销户进行说明。

智能密码设备获取智能密码设备销户申请，利用智能密码设备的私钥对销户申请进行签名获得第七签名信息，并向后台系统服务器发送智能密码设备销户申请以及第七签名信息。具体的，该第七签名信息可以通过终端发送的，也可以是人工办理的，在通过终端发送时，可以利用第一会话密钥和第二会话密钥进行加密计算和/或校验计算等计算，以保证

信息传输的安全性。

后台系统服务器接收到智能密码设备销户申请以及第七签名信息后，利用预存的智能密码设备证书中的公钥对第七签名信息进行验证。具体的，如果终端还利用第一会话密钥进行加密计算和/或校验计算，在本步骤中，后台系统服务器还利用第一会话密钥对接收到的信息进行解密计算和/或校验验证计算。

后台系统服务器在验证第七签名信息通过后，删除预存的智能密码设备证书，并生成智能密码设备销户完成信息，向智能密码设备发送智能密码设备销户完成信息。具体的，后台系统服务器在进行销户时，除了删除预存的智能密码设备证书外，还可以将该智能密码设备对应的信息放到后台系统服务器预设的销户列表里等其他销户操作。另外，销户完成信息也可以通过终端发送至智能密码设备，此时可以利用第一会话密钥进行加密计算和/或校验计算得到的，也可以是利用后台系统服务器的私钥进行签名得到的，或者利用后台系统服务器的私钥进行签名后再利用第一会话密钥进行加密计算和/或校验计算得到的。

智能密码设备接收到智能密码设备销户完成信息后，删除智能密码设备的私钥。具体的，智能密码设备可以对签名信息进行验签，并在验签通过后，执行删除操作，也可以利用第二会话密钥解密和/或校验验证得到的信息，当然，还可以利用第二会话密钥解密和/或校验验证得到的信息后再对签名信息进行验签，只要保证信息传输的安全性和/或完整性均应包含在本发明的保护范围内。

后台系统服务器通过管理终端和智能密码设备的注册、销户、认证以及锁定几个方面，确保终端和智能密码设备的合法性，杜绝了由于终端或者智能密码设备被非法盗用时产生的财产损失。

值得说明的是，以上的步骤一至步骤七并非依次执行的，其可以仅完成其中几个步骤，另外，以上的步骤一至步骤七也不仅限于同一应用场景下完成，无论在何种应用场景下，只要使用本发明的任一步骤，并可以安全的执行完交易即应属于本发明的保护范围。

以下，给出本发明示例性的一种应用场景。

本应用场景中，在智能密码设备上集成无线通信模块，以及状态控制模块形成本发明的新型的可用于安全支付的智能密码设备。该智能密码设备包括无线通信模块，其可以是蓝牙通信模块或者 WIFI 通信模块等，该无线通信模块可以对其他设备进行查询扫描和寻呼扫描，并可以与其他无线设备进行信号和数据的交互。同时该智能密码设备上还包括一个状态控制模块，可以控制智能密码设备的无线通信模块和主机的工作状态。且本发明的智能密码设备具备两个状态：休眠状态以及唤醒状态，在休眠状态下只有收发器（无线通信

模块)和状态控制模块处于工作,CPU 将关闭,不能进行指令操作(例如:签名,接收、发送数据等功能),从而使智能密码设备处于一种低功耗的状态。当其他无线设备从外部发给该智能密码设备应用指令时,状态控制模块可以对这些信号进行识别,并生成唤醒信号,将 CPU 唤醒为唤醒状态,开始执行这个应用命令。当命令执行完毕以后,CPU 将再次进入
5 休眠状态。

以下,对于本发明的完整交易流程进行简单说明。

智能密码设备处于休眠状态,用户带着该智能密码设备进入终端的无线信号覆盖范围内,智能密码设备与终端完成无线设备的交互识别,即终端可以知道有智能密码设备进入终端所在店铺并与该智能密码设备建立连接。

10 终端与智能密码设备建立连接以后,终端会向智能密码设备发送认证设备的请求,智能密码设备接收到该请求,状态控制模块会发出唤醒信号,此时 CPU 就会被唤醒,智能密码设备进入唤醒状态,并执行相应的操作。

智能密码设备完成相应指令以后,恢复至休眠状态,并继续保持与终端的设备交互识别,以便终端能够判断智能密码设备的持有者是否离店。

15 终端与智能密码设备相互认证通过以后,终端会向后台系统服务器提出读取用户信息的请求,后台系统服务器提出输入用户授权信息的请求,此时终端会向智能密码设备发送用户授权请求。

休眠状态下的智能密码设备接收到来自终端发送的用户授权请求,进入唤醒状态。智能密码设备将显示终端的请求,提示用户进行判断是否授权。

20 用户根据显示的终端发送的请求判断是否授权,若授权,则按下智能密码设备上的确认键使智能密码设备产生授权信息并发送给终端,然后转入休眠状态,否则,智能密码设备结束执行命令,直接转入休眠状态。

在结算时,终端又会向休眠状态的智能密码设备发送用户交易确认请求指令,处于休眠状态下的智能密码设备接收到该指令进入唤醒状态,智能密码设备显示接收到的交易信息,用户进行确认,若交易信息正确,则按下确认键使智能密码设备对交易信息签名,并
25 返回给终端;否则,结束执行操作,智能密码设备转入休眠状态。

以下,给出本发明的另一种应用场景。

后台系统服务器与终端进行相互认证,建立安全通道协商共同的会话密钥 K1。

30 终端在本地服务器建立一个当前用户列表,该当前用户列表可以用来存储当前店内的顾客持有的智能密码设备对应的用户信息。

终端本地服务器通过无线方式（例如采用无线探测设备）对终端的无线信号覆盖范围内的智能密码设备进行监测。

顾客携带着具有无线通讯功能的智能密码设备（处于休眠状态）逛街购物，当该顾客进入终端的无线信号覆盖范围内，智能密码设备可以被终端搜索到，并与终端建立无线连接。

终端与智能密码设备进行相互认证，并建立安全通道协商出共同的会话密钥 K2。

终端向后台系统服务器发送读取智能密码设备对应的用户信息的请求。

后台系统服务器产生随机数（单次授权标识），作为生成用户授权信息的参数，后台系统服务器利用会话密钥 K1 加密该随机数。

10 后台系统服务器向终端发出用户授权请求信息，并将该随机数密文发送给终端。

终端解密密文，再利用终端与智能密码设备之间协商的会话密钥 K2 对该随机数加密。

终端向智能密码设备发送用户授权请求信息，并将该随机数密文发给智能密码设备。

智能密码设备接收到该用户授权请求信息后，转换成唤醒状态，并利用会话密钥 K2 对接收到的该随机数密文进行解密，然后在智能密码设备的显示屏上显示该用户授权请求信息，等待用户进行确认。

用户对该信息进行判断，如果不允许则拒绝，智能密码设备转入休眠状态。

如果允许，则按下智能密码设备上的确认键，智能密码设备对该随机数（单次授权标识）进行摘要并签名，并将签名值作为用户授权信息，利用会话密钥 K2 加密签名值发送至终端，然后转入休眠状态。

20 终端接到签名值利用会话密钥 K2 解密，再利用会话密钥 K1 加密，传送给后台系统服务器。

后台系统服务器利用会话密钥 K1 解密得到签名，再利用智能密码设备的公钥解密签名，将利用其自身生成的随机数生成的摘要与解密签名后得到的值进行对比，若不一致，则返回错误信息结束操作。

25 若一致，则后台系统服务器将用户信息利用会话密钥 K1 进行加密，并生成用户授权信息校验值（第一校验值），该校验值可以是 MAC 形式或者哈希函数加签名的形式等，将密文以及校验值发送给终端。

终端收到用户信息以后，将用户信息存储在当前用户列表中。

顾客购物结束以后到收银处进行结算。

30 终端结算金额，并在当前用户列表中选中该顾客持有的智能密码设备对应的账户。

终端将交易金额、收付款双方账号、收付款双方标识信息等生成交易信息，利用会话

密钥 K2 加密交易信息。

终端向智能密码设备发送交易请求信息，并将交易信息密文发送给智能密码设备。

智能密码设备接收到终端的交易请求信息，则转入唤醒状态，对交易信息解密成明文并在屏幕上显示出来。

- 5 顾客对交易信息进行确认，若有问题则按取消，交易中止，智能密码设备转入休眠状态。

若没有问题，则按下确认键，智能密码设备生成随机数，作为单次交易标识。

智能密码设备对交易信息以及该随机数进行摘要并签名，利用会话密钥 K2 加密签名，得到用户交易确认信息并发送给终端。

- 10 终端对用户交易确认信息进行解密，并生成交易数据包（包括交易金额，收付款双方账号以及各自的唯一识别信息等），利用会话密钥 K1 对交易数据包加密，并生成交易数据包校验值（第二校验值）。

终端向后台系统服务器发送转账申请并发送交易数据包密文以及第二校验值。

- 15 后台系统服务器进行转账处理，并向终端发送转账成功的支付完成信息，当然，后台系统服务器还可以将支付完成信息通过终端发送给智能密码设备，以便顾客得知交易完成。
终端收到该支付完成信息，向顾客交付商品，结账完成。

- 20 通过终端与后台系统服务器之间进行的认证，终端认定了后台系统服务器的合法性以后，可以利用可信的后台系统服务器对智能密码设备的合法性进行认证。在同时确定了后台系统服务器与智能密码设备是可信的情况下，这样就保证了终端的交易安全。同时利用后台系统服务器对终端的合法性认证以及交易时智能密码设备对显示信息手动确认的环节，也保证了智能密码设备持有者的交易安全。

- 25 基于本发明提供的数据安全交互方法，顾客在进入店铺进行交易时，无需配合手机、银行卡或金融 IC 卡等相关账户载体设备完成支付，而原有技术的支付过程均需要借助 SIM 卡或智能卡等具备账户存储功能的设备，用户还需要进行刷卡、刷手机等操作才能完成交易。采用本发明提供的方法，顾客可以无需借助钱包、信用卡、手机等方式来完成支付，从而简化了顾客与商户在支付过程中的交互操作，提高了支付效率，提升了顾客在近场支付过程中的体验；同时利用智能密码设备的安全性特点保证顾客支付过程的安全性。

- 30 顾客选购好商品以后在结账时，终端无需再通过让顾客手动刷卡或刷手机的方式获得用户信息，是因为该用户信息在刚进店时已经存储在终端的当前用户列表中了，结账时顾

客只需报出自己的姓名，终端即可直接将结算后的金额等交易信息发送至顾客的智能密码设备并显示，此时，顾客只需利用智能密码设备进行确认，并输出交易确认信息，终端生成交易数据包发送给后台系统服务器，后台系统服务器验证该交易数据包准确无误后进行转账处理，即可完成支付过程。

- 5 当顾客走出这家店铺的信号覆盖范围时，智能密码设备与终端之间的网络连接就会自动中断，用户信息从该店铺的当前用户列表中消失。若顾客又进入另一家店铺时，将会自动进入该家店铺的当前用户列表中，开始另一次购物。这样不需要顾客执行任何操作，只需要顾客在购物时将一个小巧的智能密码设备随身放入口袋，采用本发明就可以为顾客带来无缝使用体验。

10

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的
15 实施例所属技术领域的技术人员所理解。

- 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路
20 的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列（PGA），现场可编程门阵列（FPGA）等。

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。

- 25 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既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。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用，也可以存储在一个计算机可读存储介质中。

- 30 上述提到的存储介质可以是只读存储器，磁盘或光盘等。

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发明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一个或多个实施例或示例中以合适的方式结合。

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

权利要求书

1、一种数据安全交互方法，其特征在于，包括：

5 终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息；

所述终端与后台系统服务器进行相互认证，和/或所述终端与所述智能密码设备进行相互认证；

所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息；

10 所述终端将所述用户信息存储到预先建立的当前用户列表中。

2、根据权利要求1所述的方法，其特征在于，所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息包括：

所述终端向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求；

15 所述后台系统服务器接收到所述智能密码设备的标识信息以及所述用户信息读取请求后，根据所述智能密码设备的标识信息获取与所述智能密码设备对应的用户信息；

所述后台系统服务器根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息；

20 所述终端接收到所述用户信息读取请求的响应信息后，根据所述用户信息读取请求的响应信息获得所述用户信息。

3、根据权利要求1所述的方法，其特征在于，所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息包括：

所述终端根据扫描到的所述智能密码设备的标识信息向所述智能密码设备发送用户信息读取请求；

25 所述智能密码设备获得预先存储的用户信息，并根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息；

所述终端接收到所述用户信息读取请求的响应信息后，根据所述用户信息读取请求的响应信息获得所述用户信息。

30 4、根据权利要求1至3任一项所述的方法，其特征在于，所述终端与后台系统服务器进行相互认证包括：

所述终端生成第一待签名信息；

所述终端向后台系统服务器发送所述第一待签名信息以及第一认证请求信息；

所述后台系统服务器接收到所述第一待签名信息以及所述第一认证请求信息后，生成第二待签名信息；

所述后台系统服务器向所述终端发送所述第二待签名信息以及后台系统服务器证书；

5 所述终端接收到所述第二待签名信息以及所述后台系统服务器证书后，利用预存的后台系统服务器证书对应的根证书验证所述后台系统服务器证书是否合法；

所述终端在验证所述后台系统服务器证书合法后，利用所述终端的私钥对所述第一待签名信息和所述第二待签名信息进行签名生成第一签名信息；

所述终端向所述后台系统服务器发送所述第一签名信息以及终端证书；

10 所述后台系统服务器利用预存的终端证书对应的根证书验证所述终端证书是否合法；

所述后台系统服务器在验证所述终端证书合法后，利用所述终端证书中的公钥验证所述第一签名信息；

所述后台系统服务器在验证所述第一签名信息通过后，生成后台认证完成消息，并向所述终端发送所述后台认证完成消息；

15 所述终端接收到所述后台认证完成消息后，验证所述后台认证完成消息；

所述终端在验证所述后台认证完成消息通过后，生成终端认证第一完成消息，向所述后台系统服务器发送所述终端认证第一完成消息；

所述后台系统服务器接收到所述终端认证第一完成消息后，验证所述终端认证第一完成消息；

20 所述后台系统服务器在验证所述终端认证第一完成消息通过后，所述终端与所述后台系统服务器完成相互认证。

5、根据权利要求1至4任一项所述的方法，其特征在于，所述终端与所述智能密码设备进行相互认证包括：

所述终端生成第三待签名信息；

25 所述终端向所述智能密码设备发送所述第三待签名信息以及第二认证请求信息；

所述智能密码设备接收到所述第三待签名信息以及所述第二认证请求信息后，生成第四待签名信息；

所述智能密码设备利用所述智能密码设备的私钥对所述第三待签名信息进行签名获得第二签名信息，并向所述终端发送所述第四待签名信息、所述第二签名信息以及智能密码设备证书；

30

所述终端接收到所述第四待签名信息、所述第二签名信息以及所述智能密码设备证书

后，利用预存的智能密码设备证书对应的根证书验证所述智能密码设备证书是否合法；

所述终端在验证所述智能密码设备证书合法后，利用所述智能密码设备证书中的公钥对所述第二签名信息进行验证；

所述终端在验证所述第二签名信息通过后，利用所述终端的私钥对所述第三待签名信息
5 息和所述第四待签名信息进行签名获得第三签名信息；

所述终端向所述智能密码设备发送所述第三签名信息以及所述终端证书；

所述智能密码设备接收到所述第三签名信息以及所述终端证书后，利用预存的所述终端证书对应的根证书验证所述终端证书是否合法；

所述智能密码设备在验证所述终端证书合法后，利用所述终端证书中的公钥对所述第
10 三签名信息进行验证；

所述智能密码设备在验证所述第三签名信息通过后，生成智能密码设备认证完成消息；

所述智能密码设备向所述终端发送所述智能密码设备认证完成消息；

所述终端接收到所述智能密码设备认证完成消息后，验证所述智能密码设备认证完成消息；

所述终端在验证所述智能密码设备认证完成消息通过后，生成终端认证第二完成消息，
15 向所述智能密码设备发送所述终端认证第二完成消息；

所述智能密码设备接收到所述终端认证第二完成消息后，验证所述终端认证第二完成消息；

所述智能密码设备验证所述终端认证第二完成消息后，所述终端与所述智能密码设备
20 完成相互认证。

6、根据权利要求 1 至 5 任一项所述的方法，其特征在于，所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息的步骤之后，所述方法还包括：

所述终端获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；
25

所述终端根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比对；

如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则执行所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户
30 信息的步骤；且如果所述当前用户列表中的智能密码设备的标识信息不在所述实时标识列表中，则删除所述当前用户列表中不在所述实时标识列表中的智能密码设备的用户信息。

7、根据权利要求 1 至 5 任一项所述的方法，其特征在于，所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息的步骤之后，所述方法还包括：

所述终端获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；

所述终端根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比较；

如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则执行所述终端根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息的步骤，并在所述终端获得所述用户信息后，将所述用户信息存储至所述实时标识列表中；且如果所述实时标识列表中的智能密码设备的标识信息在所述当前用户列表中，则将所述在所述当前用户列表中的智能密码设备的用户信息存储至所述实时标识列表中；

将所述实时标识列表作为更新后的所述当前用户列表。

8、根据权利要求 4 所述的方法，其特征在于，所述第一认证请求信息包括所述终端的标识信息；

所述后台系统服务器接收到所述第一待签名信息以及所述第一认证请求信息后，判断所述终端的标识信息是否包含在所述后台系统服务器中预存的终端异常名单中；

所述后台系统服务器在判断出所述终端的标识信息在所述终端异常名单中后，获取锁定终端指令，以及利用所述后台系统服务器的私钥对锁定终端指令进行签名获得第四签名信息，并向所述终端发送所述锁定终端指令以及所述第四签名信息；

所述终端接收到所述锁定终端指令以及所述第四签名信息后，利用预存的所述后台系统服务器证书中的公钥对所述第四签名信息进行验证；

所述终端在验证所述第四签名信息通过后，根据所述锁定终端指令执行锁定操作。

9、根据权利要求 2 所述的方法，其特征在于，所述终端向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求的步骤之后，所述方法还包括：

所述后台系统服务器判断所述智能密码设备的标识信息是否包含在所述后台系统服务器中预存的智能密码设备异常名单中；

所述后台系统服务器在判断出所述智能密码设备的标识信息在所述智能密码设备异常名单中后，获取锁定智能密码设备指令，以及利用所述后台系统服务器的私钥对锁定智能密码设备指令进行签名获得第五签名信息，并通过所述终端向所述智能密码设备发送所述锁定智能密码设备指令以及所述第五签名信息；

所述智能密码设备接收到所述锁定智能密码设备指令以及所述第五签名信息后，利用预存的所述后台系统服务器证书中的公钥对所述第五签名信息进行验证；

所述智能密码设备在验证所述第五签名信息通过后，根据所述锁定智能密码设备指令执行锁定操作。

5 10、根据权利要求 1 至 9 任一项所述的方法，其特征在于，所述方法还包括：

所述后台系统服务器接收终端注册申请，并对所述终端注册申请进行审核；

所述后台系统服务器在审核所述终端注册申请通过后，向所述终端发送终端密钥对生成指令；

所述终端接收到所述终端密钥对生成指令后，生成终端密钥对；

10 所述终端向所述后台系统服务器发送所述终端密钥对中的公钥；

所述后台系统服务器接收到所述终端密钥对中的公钥后，生成所述终端证书，并向所述终端发送所述终端证书；

所述终端存储所述终端证书；

以及

15 所述后台系统服务器接收智能密码设备注册申请，并对所述智能密码设备注册申请进行审核；

所述后台系统服务器在审核所述智能密码设备注册申请通过后，向所述智能密码设备发送智能密码设备密钥对生成指令；

20 所述智能密码设备接收到所述智能密码设备密钥对生成指令后，生成智能密码设备密钥对；

所述智能密码设备向所述后台系统服务器发送所述智能密码设备密钥对中的公钥；

所述后台系统服务器接收到所述智能密码设备密钥对中的公钥后，生成所述智能密码设备证书，并向所述智能密码设备发送所述智能密码设备证书；

所述智能密码设备存储所述智能密码设备证书。

25 11、根据权利要求 10 所述的方法，其特征在于，所述方法还包括：

所述终端获取终端销户申请，利用所述终端的私钥对所述销户申请进行签名获得第六签名信息，并向所述后台系统服务器发送所述终端销户申请以及所述第六签名信息；所述后台系统服务器接收到所述终端销户申请以及所述第六签名信息后，利用预存的所述终端证书中的公钥对所述第六签名信息进行验证；所述后台系统服务器在验证所述第六签名信息通过后，删除预存的所述终端证书，并生成终端销户完成信息，向所述终端发送所述终端销户完成信息；所述终端接收到所述终端销户完成信息后，删除所述终端的私钥；和/或

30

所述智能密码设备获取智能密码设备销户申请，利用所述智能密码设备的私钥对所述销户申请进行签名获得第七签名信息，并向所述后台系统服务器发送所述智能密码设备销户申请以及所述第七签名信息；所述后台系统服务器接收到所述智能密码设备销户申请以及所述第七签名信息后，利用预存的所述智能密码设备证书中的公钥对所述第七签名信息进行验证；所述后台系统服务器在验证所述第七签名信息通过后，删除预存的所述智能密码设备证书，并生成智能密码设备销户完成信息，向所述智能密码设备发送所述智能密码设备销户完成信息；所述智能密码设备接收到所述智能密码设备销户完成信息后，删除所述智能密码设备的私钥。

12、根据权利要求 2 所述的方法，其特征在于，所述后台系统服务器接收到所述智能密码设备的标识信息以及所述用户信息读取请求的步骤之后，所述后台系统服务器向所述终端发送所述用户信息读取请求的响应信息的步骤之前，所述方法还包括：

所述后台系统服务器通过所述终端向所述智能密码设备发送用户授权请求信息；

所述智能密码设备接收到所述用户授权请求信息后，生成授权信息，并通过所述终端向所述后台系统服务器发送所述授权信息；

所述后台系统服务器接收到所述授权信息后，执行所述后台系统服务器向所述终端发送所述用户信息读取请求的响应信息的步骤。

13、根据权利要求 12 所述的方法，其特征在于，所述智能密码设备接收到所述用户授权请求信息后，生成授权信息的步骤包括：

所述智能密码设备在接收到所述用户授权请求信息后，由休眠状态转换为唤醒状态；

所述智能密码设备在唤醒状态下生成授权信息。

14、根据权利要求 5 所述的方法，其特征在于，所述智能密码设备接收到所述第三待签名信息以及所述第二认证请求信息后，生成第四待签名信息的步骤包括：

所述智能密码设备在接收到所述第二认证请求信息后，由休眠状态转换为唤醒状态；

所述智能密码设备在唤醒状态下生成第四待签名信息。

15、根据权利要求 1 至 14 任一项所述的方法，其特征在于，所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的所述智能密码设备的标识信息之前，所述方法还包括：

所述智能密码设备进入可被扫描状态。

16、根据权利要求 1 至 15 任一项所述的方法，其特征在于，

所述后台系统服务器与所述终端之间传输的信息均通过第一会话密钥加密计算和/或校验计算后传输，其中，所述第一会话密钥预存在所述后台系统服务器和所述终端中或者

所述第一会话密钥通过所述后台系统服务器和所述终端协商生成；和/或

所述终端与所述智能密码设备之间传输的信息均通过第二会话密钥加密计算和/或校验计算后传输，其中，所述第二会话密钥预存在所述终端和所述智能密码设备中或者所述第二会话密钥通过所述终端和所述智能密码设备协商生成。

- 5 17、一种数据安全交互系统，其特征在于，包括：终端、后台系统服务器以及智能密码设备；

所述终端，配置为在信号覆盖范围内扫描所述智能密码设备，并获得扫描到的所述智能密码设备的标识信息；与所述后台系统服务器进行相互认证和/或与所述智能密码设备进行相互认证；根据扫描到的所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息；将所述用户信息存储到预先建立的当前用户列表中。

10

- 18、根据权利要求 17 所述的系统，其特征在于，

所述终端，还配置为向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求；接收所述后台系统服务器发送的所述用户信息读取请求的响应信息，根据所述用户信息读取请求的响应信息获得所述用户信息；

- 15 所述后台系统服务器，配置为接收所述终端发送的所述智能密码设备的标识信息以及所述用户信息读取请求，根据所述智能密码设备的标识信息获取与所述智能密码设备对应的用户信息；根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息。

- 19、根据权利要求 17 所述的系统，其特征在于，

- 20 所述终端，还配置为根据扫描到的所述智能密码设备的标识信息向所述智能密码设备发送用户信息读取请求；接收所述智能密码设备发送的所述用户信息读取请求的响应信息，根据所述用户信息读取请求的响应信息获得所述用户信息；

所述智能密码设备，配置为获得预先存储的用户信息，并根据所述用户信息获得所述用户信息读取请求的响应信息，并向所述终端发送所述用户信息读取请求的响应信息。

- 25 20、根据权利要求 17 至 19 任一项所述的系统，其特征在于，

所述终端，还配置为生成第一待签名信息；向后台系统服务器发送所述第一待签名信息以及第一认证请求信息；接收所述后台系统服务器发送的所述第二待签名信息以及所述后台系统服务器证书，利用预存的后台系统服务器证书对应的根证书验证所述后台系统服务器证书是否合法；在验证所述后台系统服务器证书合法后，利用所述终端的私钥对所述第一待签名信息和所述第二待签名信息进行签名生成第一签名信息；向所述后台系统服务器发送所述第一签名信息以及终端证书；接收所述后台系统服务器发送的所述后台认证完

30

成消息，验证所述后台认证完成消息；在验证所述后台认证完成消息通过后，生成终端认证第一完成消息，向所述后台系统服务器发送所述终端认证第一完成消息；

所述后台系统服务器，还配置为接收所述终端发送的所述第一待签名信息以及所述第一认证请求信息，生成第二待签名信息；向所述终端发送所述第二待签名信息以及后台系统服务器证书；利用预存的终端证书对应的根证书验证所述终端证书是否合法；在验证所述终端证书合法后，利用所述终端证书中的公钥验证所述第一签名信息；在验证所述第一签名信息通过后，生成后台认证完成消息，并向所述终端发送所述后台认证完成消息；接收所述终端发送的所述终端认证第一完成消息，验证所述终端认证第一完成消息；在验证所述终端认证第一完成消息通过后，所述终端与所述后台系统服务器完成相互认证。

21、根据权利要求 17 至 20 任一项所述的系统，其特征在于，

所述终端，还配置为生成第三待签名信息；向所述智能密码设备发送所述第三待签名信息以及第二认证请求信息；接收所述智能密码设备发送的所述第四待签名信息、所述第二签名信息以及所述智能密码设备证书，利用预存的智能密码设备证书对应的根证书验证所述智能密码设备证书是否合法；在验证所述智能密码设备证书合法后，利用所述智能密码设备证书中的公钥对所述第二签名信息进行验证；在验证所述第二签名信息通过后，利用所述终端的私钥对所述第三待签名信息和所述第四待签名信息进行签名获得第三签名信息；向所述智能密码设备发送所述第三签名信息以及所述终端证书；接收所述智能密码设备发送的所述智能密码设备认证完成消息，验证所述智能密码设备认证完成消息；在验证所述智能密码设备认证完成消息通过后，生成终端认证第二完成消息，向所述智能密码设备发送所述终端认证第二完成消息；

所述智能密码设备，还配置为接收所述终端发送的所述第三待签名信息以及所述第二认证请求信息，生成第四待签名信息；利用所述智能密码设备的私钥对所述第三待签名信息进行签名获得第二签名信息，并向所述终端发送所述第四待签名信息、所述第二签名信息以及智能密码设备证书；接收所述终端发送的所述第三签名信息以及所述终端证书，利用预存的所述终端证书对应的根证书验证所述终端证书是否合法；在验证所述终端证书合法后，利用所述终端证书中的公钥对所述第三签名信息进行验证；在验证所述第三签名信息通过后，生成智能密码设备认证完成消息；向所述终端发送所述智能密码设备认证完成消息；接收所述终端发送的所述终端认证第二完成消息，验证所述终端认证第二完成消息；验证所述终端认证第二完成消息后，所述终端与所述智能密码设备完成相互认证。

22、根据权利要求 17 至 21 任一项所述的系统，其特征在于，

所述终端，还配置为在所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到

的所述智能密码设备的标识信息之后，获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比对；如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则根据扫描到的
5 所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息；且如果所述当前用户列表中的智能密码设备的标识信息不在所述实时标识列表中，则删除所述当前用户列表中不在所述实时标识列表中的智能密码设备的用户信息。

23、根据权利要求 17 至 21 任一项所述的系统，其特征在于，

所述终端，还配置为在所述终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的
10 的所述智能密码设备的标识信息之后，获得在所述终端的信号覆盖范围内的全部智能密码设备的标识信息，生成实时标识列表；根据预设的时间间隔将所述实时标识列表中的智能密码设备的标识信息与所述当前用户列表中的智能密码设备的标识信息进行比对；如果所述实时标识列表中的智能密码设备的标识信息不在所述当前用户列表中，则根据扫描到的
15 所述智能密码设备的标识信息获取所述智能密码设备对应的用户信息，并在所述终端获得所述用户信息后，将所述用户信息存储至所述实时标识列表中；且如果所述实时标识列表中的智能密码设备的标识信息在所述当前用户列表中，则将所述在所述当前用户列表中的智能密码设备的用户信息存储至所述实时标识列表中；将所述实时标识列表作为更新后的所述当前用户列表。

24、根据权利要求 20 所述的系统，其特征在于，

20 所述后台系统服务器，还配置为接收所述终端发送的所述第一待签名信息以及所述第一认证请求信息，其中，所述第一认证请求信息包括所述终端的标识信息；判断所述终端的标识信息是否包含在所述后台系统服务器中预存的终端异常名单中；在判断出所述终端的标识信息在所述终端异常名单中后，获取锁定终端指令，以及利用所述后台系统服务器的私钥对锁定终端指令进行签名获得第四签名信息，并向所述终端发送所述锁定终端指令
25 以及所述第四签名信息；

所述终端，还配置为接收所述后台系统服务器发送的所述锁定终端指令以及所述第四签名信息，利用预存的所述后台系统服务器证书中的公钥对所述第四签名信息进行验证；在验证所述第四签名信息通过后，根据所述锁定终端指令执行锁定操作。

25、根据权利要求 18 所述的系统，其特征在于，

30 所述后台系统服务器，还配置为在所述终端向所述后台系统服务器发送所述智能密码设备的标识信息以及用户信息读取请求之后，判断所述智能密码设备的标识信息是否包含

在所述后台系统服务器中预存的智能密码设备异常名单中；在判断出所述智能密码设备的标识信息在所述智能密码设备异常名单中后，获取锁定智能密码设备指令，以及利用所述后台系统服务器的私钥对锁定智能密码设备指令进行签名获得第五签名信息，并通过所述终端向所述智能密码设备发送所述锁定智能密码设备指令以及所述第五签名信息；

- 5 所述智能密码设备，还配置为接收所述锁定智能密码设备指令以及所述第五签名信息，利用预存的所述后台系统服务器证书中的公钥对所述第五签名信息进行验证；在验证所述第五签名信息通过后，根据所述锁定智能密码设备指令执行锁定操作。

26、根据权利要求 17 至 25 任一项所述的系统，其特征在于，

- 所述后台系统服务器，还配置为接收终端注册申请，并对所述终端注册申请进行审核；
10 在审核所述终端注册申请通过后，向所述终端发送终端密钥对生成指令；接收所述终端发送的所述终端密钥对中的公钥，生成所述终端证书，并向所述终端发送所述终端证书；

 所述终端，还配置为接收所述后台系统服务器发送的所述终端密钥对生成指令，生成终端密钥对；向所述后台系统服务器发送所述终端密钥对中的公钥；存储所述终端证书；

 以及

- 15 所述后台系统服务器，还配置为接收智能密码设备注册申请，并对所述智能密码设备注册申请进行审核；在审核所述智能密码设备注册申请通过后，向所述智能密码设备发送智能密码设备密钥对生成指令；接收所述智能密码设备发送的所述智能密码设备密钥对中的公钥，生成所述智能密码设备证书，并向所述智能密码设备发送所述智能密码设备证书；

- 所述智能密码设备，还配置为接收所述后台系统服务器发送的所述智能密码设备密钥
20 对生成指令，生成智能密码设备密钥对；向所述后台系统服务器发送所述智能密码设备密钥对中的公钥；存储所述智能密码设备证书。

27、根据权利要求 26 所述的系统，

- 所述终端，还配置为获取终端销户申请，利用所述终端的私钥对所述销户申请进行签名获得第六签名信息，并向所述后台系统服务器发送所述终端销户申请以及所述第六签名
25 信息；接收所述后台系统服务器发送的所述终端销户完成信息，删除所述终端的私钥；

 所述后台系统服务器，还配置为接收所述终端发送的所述终端销户申请以及所述第六签名信息，利用预存的所述终端证书中的公钥对所述第六签名信息进行验证；在验证所述第六签名信息通过后，删除预存的所述终端证书，并生成终端销户完成信息，向所述终端发送所述终端销户完成信息；

- 30 和/或

 所述智能密码设备，还配置为获取智能密码设备销户申请，利用所述智能密码设备的

私钥对所述销户申请进行签名获得第七签名信息，并向所述后台系统服务器发送所述智能密码设备销户申请以及所述第七签名信息；接收所述后台系统服务器发送的所述智能密码设备销户完成信息，删除所述智能密码设备的私钥；

所述后台系统服务器，还配置为接收所述智能密码设备发送的所述智能密码设备销户申请以及所述第七签名信息，利用预存的所述智能密码设备证书中的公钥对所述第七签名信息进行验证；在验证所述第七签名信息通过后，删除预存的所述智能密码设备证书，并生成智能密码设备销户完成信息，向所述智能密码设备发送所述智能密码设备销户完成信息。

28、根据权利要求 18 所述的系统，其特征在于，

所述后台系统服务器，还配置为通过所述终端向所述智能密码设备发送用户授权请求信息；接收所述智能密码设备通过所述终端发送的所述授权信息，向所述终端发送所述用户信息读取请求的响应信息；

所述智能密码设备，还配置为接收所述后台系统服务器通过所述终端发送的所述用户授权请求信息，生成授权信息，并通过所述终端向所述后台系统服务器发送所述授权信息。

29、根据权利要求 28 所述的系统，其特征在于，

所述智能密码设备，还配置为在接收到所述用户授权请求信息后，由休眠状态转换为唤醒状态；在唤醒状态下生成授权信息。

30、根据权利要求 21 所述的系统，其特征在于，

所述智能密码设备，还配置为在接收到所述第二认证请求信息后，由休眠状态转换为唤醒状态；在唤醒状态下生成第四待签名信息。

31、根据权利要求 17 至 30 任一项所述的系统，其特征在于，

所述智能密码设备，还配置为在被所述终端扫描之前，进入可被扫描状态。

32、根据权利要求 17 至 31 任一项所述的系统，其特征在于，

所述后台系统服务器与所述终端之间传输的信息均通过第一会话密钥加密计算和/或校验计算后传输，其中，所述第一会话密钥预存在所述后台系统服务器和所述终端中或者所述第一会话密钥通过所述后台系统服务器和所述终端协商生成；和/或

所述终端与所述智能密码设备之间传输的信息均通过第二会话密钥加密计算和/或校验计算后传输，其中，所述第二会话密钥预存在所述终端和所述智能密码设备中或者所述第二会话密钥通过所述终端和所述智能密码设备协商生成。