处理操作请求的方法及系统

技术领域

本发明涉及电子技术领域，尤其涉及一种处理操作请求的方法及系统。

背景技术

现今，刷卡消费已经成为主流。图 1 为现有技术中电子签名交易的方法的流程示意图。图 1 所示方法包括：

步骤 S101，用户持卡以非接触方式接入 POS 机；其中，非接触方式可以为射频、蓝牙、NFC 等任意非接触方式。

步骤 S102，POS 机将交易信息发送至用户接入的智能卡；其中，交易信息可以至少包括帐号和金额，当然还可以包括交易明细信息。

步骤 S103，智能卡接收交易信息，显示交易信息，待用户确认交易信息无误后，接收用户输入的确认密码，对交易信息进行签名；

步骤 S104，智能卡再次以非接触方式接入 POS 机，将签名信息发送至 POS 机；

步骤 S105，POS 机将交易信息和签名信息上传至银行服务器，以便银行服务器根据交易信息执行交易。

由此可见，现有的智能卡在完成对交易信息进行签名的过程中需要以非接触方式与 POS 机进行至少两次接入，从而会存在接入过程中交易信息和/或签名信息被劫持的问题，造成用户损失，安全性不高。

发明内容

本发明旨在解决现有智能卡在多次接入过程中交易信息和/或签名信息被劫持而造成的安全性不高的问题。

一种处理操作请求的方法，所述方法包括：终端在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；智能卡在获取到终端输出的操作请求信息后，保存所述操作请求信息，并根据本地预先保存的密码生成策略生成联合密码，在得到所述联合密码后，根据所述操作请求信息和所述联合密码生成签名报文，并至少将所述签名报文发送给终端；在所述终端获取到签名报文后，如果所述智能卡检测到与所述终端断开连接，则智能卡输出所述联合密码的提示信息；所述终端在接收到所述提示信息对应的联合密码后，将获取到的所述联合密码作为待验证密码，所述终端通知验证装置根据所述待验证密

码和所述操作请求信息对所述签名报文进行验证，所述验证装置在所述签名报文验证通过后，触发响应所述操作请求的流程。

优选的，所述根据所述操作请求信息和所述联合密码生成签名报文的步骤，包括：获取操作请求信息的内容调整策略，并根据获取到操作请求信息的内容调整策略，对所述操作请求信息的内容进行处理，得到调整后的操作请求信息；和/或，获取联合密码的内容调整策略，并根据获取到联合密码的内容调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；对如下任一组合进行签名，生成签名报文，其中所述组合包括：调整后的操作请求信息和所述联合密码；所述操作请求信息和调整后的联合密码；调整后的操作请求信息和调整后的联合密码。

优选的，所述方法还包括：通知所述终端所述调整后的操作请求信息所使用的内容调整策略；或者，通知所述终端所述调整后的联合密码所使用的内容调整策略，或者，通知所述终端所述调整后的操作请求信息内容调整策略以及调整后的联合密码所使用的内容调整策略。

优选的，所述根据获取到操作请求信息的内容调整策略，对所述操作请求信息的内容进行处理，得到调整后的操作请求信息，包括：如果获取到操作请求信息的调整策略为对所述操作请求信息进行加密，则根据预先存储的加密算法的分配策略，获取所述用户操作请求对应的加密算法，根据该加密算法对所述用户操作请求进行加密，将加密后的所述用户操作请求作为调整后的操作请求信息。

优选的，所述根据获取到联合密码的内容调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码，包括以下任一方式：如果获取到联合密码的内容调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；如果内容调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，将处理后的联合密码作为调整后的联合密码，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的内容调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码

进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的内容调整策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

优选的，所述智能卡输出联合密码提示信息包括：按照预先设置的身份认证策略，对请求输出联合密码的请求方进行身份认证；如果认证成功，则输出联合密码。

优选的，所述待验证密码是通过如下任一方式得到的，包括：对所述终端上输入设备输入的信息进行检测，根据检测结果，得到所述待验证密码；如果所述智能卡通过显示屏幕显示所述联合密码的条码信息或图形信息，则对所述条码信息或图形信息进行扫描，得到所述待验证密码；通过以非接触通讯方式与所述智能卡建立通信连接，并通过所述通信连接获取所述智能卡发送的联合密码，将接收到联合密码作为待验证密码。

优选的，所述验证装置内置于终端和/或后台系统服务器。

优选的，所述终端通知验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证，包括如下任一方式：所述终端内的验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证；所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证。

优选的，所述方法还具有如下特点：所述验证装置在采用所述方式二对所述签名报文进行验证时，所述方法还包括：所述终端从智能卡获取所述联合密码的内容调整策略，其中根据所述联合密码的内容调整策略处理后的联合密码为生成所述签名报文所使用的联合密码，和/或，所述终端从智能卡获取所述操作请求信息的内容调整策略，其中根据所述操作请求信息的内容调整策略处理后的操作请求信息为生成所述签名报文所使用的操作请求信息；所述终端将所述联合密码的内容调整策略和/或所述操作请求信息的内容调整策略发送给所述后台系统服务器内的验证装置以对所述签名报文进行验证。

一种处理操作请求的方法，所述方法包括：终端在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；智能卡在获取到终端输出的操作请求信息后，根据

预先设置的签名生成策略对所述操作请求信息进行签名生成签名报文，以及，根据本地预先保存的密码生成策略生成联合密码，在得到联合密码后，根据预先设置的联合密码的调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；将所述调整后的联合密码和所述签名报文发送至所述终端；在所述终端获取到签名报文和调整后的联合密码后，如果所述智能卡检测到与所述终端断开连接，则输出所述联合密码的提示信息；所述终端在接收到所述提示信息对应的联合密码后，将获取到的所述联合密码作为待验证密码，所述终端通知验证装置对所述待验证密码和所述签名报文进行验证，所述验证装置在所述签名报文和所述待验证密码均验证通过后，触发响应所述操作请求的流程。

优选的，所述根据预先设置的联合密码的调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码，包括以下任一方式：如果联合密码的调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的调整策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

优选的，所述验证装置内置于终端和/或后台系统服务器。

优选的，所述终端通知验证装置对所述待验证密码和所述签名报文进行验证的步骤，包括如下任一方式：所述终端内的验证装置分别对所述待验证密码和所述签名报文进行验证；所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置对所述待验证密码和所述签名报文进行验证；所述终端内的验证装置对所述待验证密码进行验证，并在验证通过后，至少将所述签名报文、所述待验证密码和所述操作请求信息发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述签名报文进行验证；所述终端内的验证装置对所述签名报文进行验证，并在验证通过后，至少将所述待验证密码发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述待验证密码进行验证。

一种处理操作请求的系统，所述系统包括终端、智能卡和验证装置，其中所述终端包括第一发送模块和通知模块，所述智能卡包括保存模块、第一生成模块、第二生成模块、第二发送模块以及输出模块，所述验证装置还包括触发模块，其中：所述第一发送模块，用于在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；所述保存模块，与所述第一发送模块相连，用于在获取到终端输出的操作请求信息后，保存所述操作请求信息；

所述第一生成模块，用于根据本地预先保存的密码生成策略生成联合密码；所述第二生成模块，与所述保存模块和所述第一生成模块相连，用于在得到联合密码后，根据所述操作请求信息和所述联合密码生成签名报文；所述第二发送模块，与所述第二生成模块相连，用于将所述签名报文发送给终端；所述输出模块，用于在所述终端获取到签名报文后，如果所述智能卡检测到与所述终端断开连接，则输出所述联合密码的提示信息；所述通知模块，用于在接收到所述提示信息对应的联合密码后，将获取到的所述联合密码作为待验证密码，通知验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证；所述触发模块，用于在所述签名报文验证通过后，触发响应所述操作请求的流程。

优选的，所述第二生成模块，包括：第一处理子模块和第二处理子模块中的至少一个、生成子模块以及通知子模块，其中：所述第一处理子模块包括：第一获取单元，用于获取操作请求信息的内容调整策略；第一处理单元，与所述第一获取单元相连，用于根据获取到操作请求信息的内容调整策略，对所述操作请求信息的内容进行处理，得到调整后的操作请求信息；所述第二处理子模块，包括：第二获取单元，用于获取联合密码的内容调整策略；第二处理单元，与所述第二获取单元相连，用于根据获取到联合密码的内容调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；所述生成子模块，用于对如下任一组合进行签名，生成签名报文，其中所述组合包括：调整后的操作请求信息和所

述联合密码；所述操作请求信息和调整后的联合密码；调整后的操作请求信息和调整后的联合密码。

优选的，所述第二生成模块还包括：通知子模块，用于通知终端调整后的操作请求信息所使用的内容调整策略；或者，通知终端调整后的联合密码所使用的内容调整策略，或者，通知终端调整后的操作请求信息内容调整策略以及调整后的联合密码所使用的内容调整策略。

优选的，所述第一处理单元，用于如果获取到操作请求信息的调整策略为对所述操作请求信息进行加密，则根据预先存储的加密算法的分配策略，获取所述用户操作请求对应的加密算法，根据该加密算法对所述用户操作请求进行加密，将加密后的所述用户操作请求作为调整后的操作请求信息。

优选的，所述第二处理单元，用于根据如下任一方式处理联合密码：如果获取到联合密码的调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的调整策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

优选的，所述输出模块包括：认证单元，用于按照预先设置的身份认证策略，对请求输出联合密码的请求方进行身份认证；输出单元，用于如果认证成功，则输出联合密码。

优选的，所述待验证密码是通过如下任一方式得到的，包括：对所述终端上输入设备输入的信息进行检测，根据检测结果，得到所述待验证密码；如果所述智能卡通过显示屏幕显示所述联合密码的条码信息或图形信息，则对所述条码信息或图形信息进行扫描，得到所述待验证密码；通过以非接触通讯方式与所述智能卡建立通信连接，并通过所述通信连接获取所述智能卡发送的联合密码，将接收到联合密码作为待验证密码。

优选的，所述验证装置内置于终端和/或后台系统服务器。

优选的，所述验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证，包括如下任一方式：所述终端内的验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证；所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证。

优选的，所述终端还包括：获取模块，用于从智能卡获取所述联合密码的内容调整策略，其中根据所述联合密码的内容调整策略处理后的联合密码为生成所述签名报文所使用的联合密码，和/或，所述终端从智能卡获取所述操作请求信息的内容调整策略，其中根据所述操作请求信息的内容调整策略处理后的操作请求信息为生成所述签名报文所使用的操作请求信息；第三发送模块，与所述获取模块相连，用于将所述联合密码的内容调整策略和/或所述操作请求信息的内容调整策略发送给所述验证装置。

一种处理操作请求的系统，所述系统包括终端、智能卡和验证装置，其中所述终端包括第一发送模块和通知模块，所述智能卡包括第一生成模块、第二生成模块、调整模块、第二发送模块以及输出模块，所述验证装置包括触发模块，其中：所述第一发送模块，用于在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；所述第一生成模块，与所述第一发送模块相连，用于在获取到终端输出的操作请求信息后，根据预先设置的签名生成策略，根据所述操作请求信息生成签名报文；所述第二生成模块，用于根据本地预先保存的密码生成策略生成联合密码；所述调整模块，与所述第二生成模块相连，用于根据预先设置的联合密码的调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；所述第二发送模块，与所述第一生成模块和所述调整模块相连，用于将所述调整后的联合密码和所述签名报文发送至所述终端；所述输出模块，用于在所述终端获取到签名报文和调整后的联合密码后，如果所述智能卡检测到与所述终端断开连接，则输出所述联合密码的提示信息；所述通知模块，用于在接收到所述提示信息对应的联合密码后，

将获取到的所述联合密码作为待验证密码，通知验证装置对所述待验证密码和所述签名报文进行验证；所述触发模块，用于在所述签名报文和所述待验证密码均验证通过后，触发响应所述操作请求的流程。

优选的，所述调整模块采用如下任一方式对所述联合密码的内容进行调整，包括：如果联合密码的调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；方式二：如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；如果获取到联合密码的处理策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

优选的，所述验证装置内置于终端和/或后台系统服务器。

优选的，所述验证装置对所述待验证密码和所述签名报文进行验证的步骤，包括如下任一方式：所述终端内的验证装置分别对所述待验证密码和所述签名报文进行验证；所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置对所述待验证密码和所述签名报文进行验证；所述终端内的验证装置对所述待验证密码进行验证，并在验证通过后，至少将所述签名报文、所述待验证密码和所述操作请求信息发送给所述后台系统服务器，指示所述后台

系统服务器内的验证装置对所述签名报文进行验证；所述终端内的验证装置对所述签名报文进行验证，并在验证通过后，至少将所述待验证密码发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述待验证密码进行验证。

由上述本发明提供的技术方案可以看出，通过智能卡和终端的一次接入完成交易所需数据（例如签名数据）的交互，降低了多次接入造成的重要信息被截获的风险，提高了安全性。本发明的联合密码可以是在每次交易时随机生成的数字、字母和字符的一种或多种的组合，不同于现有的交易密码和 OTP 必须根据密文进行传输，本发明终端可以不同方式获取联合密码，在获取的过程中，该联合密码（验证密码）可以以明文的形式进行传输，并且不会降低交易过程中账户的安全性；本发明由智能卡生成联合密码并对联合密码进行加密或者进行签名，保证联合密码传输至终端的安全性和验证装置验证联合密码的准确性；本发明的验证装置是在输入了联合密码之后根据联合密码验证签名报文，并在验证通过后触发响应操作请求的流程，防止将签名数据等重要数据通过网络进行传输而导致不安全的隐患，保证了交易的安全性。

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 为现有技术中电子签名交易的方法的流程示意图；

图 2 为本发明提供的用户请求的处理方法的方法流程示意图；

图 3 为本发明提供的另一种用户请求的处理方法的流程示意图；

图 4 为本发明提供的用户请求的处理系统的结构示意图；

图 5 为本发明提供的另一种用户请求的处理系统的结构示意图。

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发明和简化描述，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发明的限制。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。

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发明中的具体含义。

下面将结合附图对本发明实施例作进一步地详细描述。

图 1 为本发明提供的用户请求的处理方法的流程示意图。图 1 所示方法包括如下步骤：

步骤 201、终端在检测到用户的操作请求后，向智能卡发送用户的操作请求信息；

步骤 202、智能卡在获取到终端输出的操作请求信息后，保存操作请求信息；

步骤 203、智能卡根据本地预先保存的密码生成策略生成联合密码；

步骤 204、智能卡在得到联合密码后，智能卡根据操作请求信息和联合密码生成签名报文；

步骤 205、智能卡将签名报文发送给终端；

步骤 206、在终端获取到签名报文后，如果智能卡检测到与终端断开连接，则智能卡输出联合密码的提示信息；

步骤 207、终端在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码，终端通知验证装置根据待验证密码和操作请求信息对签名报文进行验证；

步骤 208、验证装置在签名报文和待验证密码均验证通过后，触发响应操作请求的流程。

与现有技术中智能卡和终端至少两次接入才能完成用户身份的鉴权数据的生成和传输相比，本发明提供的方法实施例，通过智能卡和终端的一次接入完成用户身份的鉴权数据的生成和传输，降低了智能卡和终端多次接入造成重要信息被截获的风险，提高了安全性，且减少了多次接入给操作人员带来的手动操作。

下面对本发明提供的方法实施例作进一步说明：

本实施例所提供的方法包括如下步骤：

步骤 A01、终端在检测到用户的操作请求后，向智能卡发送用户的操作请求信息；

其中，用户的操作请求可以是访问某个账号；或者，修改个人的信息，如修改某一账号的密码，或者，将某一账号对应的信息进行修改，如修改某一存储账号的金额等；

例如，用户的操作请求为向某个账号转账一定数额的存款。则操作请求信息可以包括账户和金额，还可包括交易明细信息等。

终端可以为：固定终端或者移动终端，固定终端可以包括 ATM 机，PC 机、POS 机等，移动终端可以包括：手机、平板电脑、手持 POS 机等。

步骤 A02、智能卡在获取到终端输出的操作请求信息后，保存操作请求信息；

其中，智能卡接入终端之前，终端可通过手工输入、网络、扫描商品信息等方式获取操作请求信息。

其中，智能卡与终端的接入方式可以为通过非接触方式或接触方式。其中，优选非接触方式接入终端，其与接触方式接入终端相比，具有较高的安全性，防止信息被获取。

步骤 A03、智能卡根据本地预先保存的密码生成策略生成联合密码；

其中该密码生成策略可以预先保存的，也可以定期的进行更新，后者可以减少联合密码的生成规则被破解；

当然，密码生成策略可以包括密码生成算法和输入参数，其中密码生成算法可以有多种，输入参数可以是一些实时信息作为生成联合密码时所需的输入参数，如时间信息或随机数等，保证联合密码生成的多样性。

另外，该密码生成策略也可以是随机生成，如智能卡随机地生成数字、字母和/或符号，从数字、字母和符号中选择一种或多种组合生成联合密码，可以保证联合密码的不唯一性，随机性，提高联合密码的安全性。

步骤 A04、在得到联合密码后，智能卡根据操作请求信息和联合密码生成签名报文；

其中，该智能卡为具有电子签名功能的设备，可以包括含有用户账户信息的卡芯片和利用密钥进行数字签名的安全芯片，或者包括具有上述两个芯片功能的集成芯片。

在实际应用中，可以不对操作请求信息和联合密码都进行任何处理，就直接生成签名报文，但为了提高签名报文的安全性，可以根据如下处理方式：

智能卡获取操作请求信息的内容调整策略，根据获取到操作请求信息的内容调整策略，对操作请求信息的内容进行处理，得到调整后的操作请求信息；和/或，智能卡获取联合密码的内容调整策略，根据获取到联合密码的内容调整策略，对联合密码的内容进行调整，得到调整后的联合密码；

智能卡对如下任一组合进行签名，生成签名报文，其中：

组合一为调整后的操作请求信息和联合密码；

组合二为操作请求信息和调整后的联合密码；

组合三为调整后的操作请求信息和调整后的联合密码；

以及，通知终端组合一中调整后的操作请求信息所使用的内容调整策略；或者，通知终端组合二中调整后的联合密码所使用的内容调整策略，或者，通知终端组合三中调整后的操作请求信息内容调整策略以及调整后的联合密码所使用的内容调整策略。

优选的，根据获取到操作请求信息的处理策略，对操作请求信息进行处理，得到处理后的操作请求信息的步骤，包括：

如果获取到操作请求信息的调整策略为对操作请求信息进行加密，则根据预先存储的加密算法的分配策略，获取用户操作请求对应的加密算法，根据该加密算法对用户操作请求进行加密，将加密后的用户操作请求作为调整后的操作请求信息。

其中，操作请求信息的加密可以使用可逆的加密算法，也可以使用不可逆的加密算法，如对操作请求信息进行摘要计算，其中摘要计算方式可以包括如下的一种或其组合：通过哈希算法计算的哈希值、通过 MAC 算法计算的 MAC 值，通过对称加密获得的密文本身。

通过对用户操作请求进行签名并将签名生成的报文发送至验证装置，可以保证操作请求的真实性，以及终端与智能卡交互结果的不可抵赖性。例如，在对金融交易系统中，可以保证交易为真实的交易，以及交易的不可抵赖性。

其中，根据获取到联合密码的调整策略，对联合密码进行处理，得到调整后的联合密码，包括任一方式：

方式一：如果获取到联合密码的调整策略为对联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

方式二：如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式三：如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式四：如果获取到联合密码的调整策略为对联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略。

下面对方式一至四分别进行说明：

方式一与常规的加密算法不同的是，其所使用的加密算法在每次可以是不同的，增加了加密算法的随机性，使得加密效果更好，降低了加密算法被破解的可能。

方式二在联合密码中增加随机数，并在联合密码被破解后，如破解者不能获知对联合密码对应的随机数和随机数组合策略，提高了签名报文的安全性；另外，每次对联合密码内容的调整原则也可以是不同的，提高内容调整方式的多样性，增加调整方式的随机性，降低内容调整方式被破解的可能。

方式三和方式四均是对方式一和方式二的优化方案，较前两个方式安全性更高。

其中，针对方式二中，联合密码为 123456，生成的随机数为 789，随机数组合策略为在联合密码最后一位增加随机数，则调整后的联合密码为 123456789。

其中为了保证终端在后续验证时，能够得到最原始的联合密码，需通知终端所使用的联合密码和该随机数组合策略。

当然，随机数组合策略可以有很多种，如联合密码中每隔一位增加一个随机数。

当然，联合密码的调整策略还可以是如下方式：

在联合密码长度达到某一预先设置的阈值时，根据获取到的删除策略，删除该联合密码中一个或多个位置的信息，将执行删除操作后剩余的联合密码作为调整后的联合密码；或者，

在联合密码长度达到某一预先设置的阈值时，根据获取到的选取策略中设置的位置信息，选取该联合密码中对应的位置信息组成新的联合密码，将组合产生的新的联合密码作为调整后的联合密码；

从本地预先保存的多个计算表达式中，获取一个计算表达式，将该联合密码作为该运算表达式的输入参数进行计算，将计算结果作为调整后的联合密码。

当然上述方式中都需要通知终端在对联合密码处理时所需使用的策略。

由于随机数本身的随机性，可以使联合密码和随机数组合后的信息随机性提高，可以

防止重放攻击。

步骤 A05、智能卡将签名报文发送给终端；

步骤 A06、在终端获取到签名报文后，如果智能卡检测到与终端断开连接，则智能卡输出联合密码的提示信息；

其中，该智能卡输出的联合密码信息可以是直接显示该联合密码；或者，该联合密码的条码信息；也可以是，通过非接触方式发送出去；

其中，提示信息可以“与终端建立通信连接”，或者，“在终端输入下面的内容“XXXXXX”“其中“XXXXXX”为联合密码，再或者“请终端扫描该图片 Y”，其中 Y 为条码信息。

可选的，为了保证控制联合密码在有限范围内的输出，防止被他人读取，智能卡输出联合密码信息之前还包括：

按照预先设置的身份认证策略，对请求输出联合密码的请求方进行身份认证；

如果认证成功，则输出联合密码。

其中该认证方式可以访问该智能卡的密码信息，或者，专门的身份认证机制。

步骤 A08、终端在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码，终端通知验证装置根据待验证密码和操作请求信息对签名报文进行验证；

其中，待验证密码是通过如下任一方式得到的，包括：

方式一：对终端上输入设备输入的信息进行检测，根据检测结果，得到待验证密码；

方式二：如果智能卡通过显示屏幕显示联合密码的条码信息或图形信息，则对条码信息或图形信息进行扫描，得到待验证密码；

方式三：通过以非接触通讯方式与智能卡建立通信连接，并通过通信连接获取智能卡发送的联合密码，将接收到联合密码作为待验证密码。

需要说明的是，之所以步骤 A08 中的“终端在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码”，终端需要接收例如手动输入或者扫描获得的联合密码，根据上述方式进行获取的联合密码（即待验证密码），有可能因为信息传输或操作失误造成得到的联合密码（即待验证密码）错误，会造成得到的待验证密码与签名报文中的联合密码不一致，从而使得在验签过程中，验证不能通过。

其中，验证装置可以为除了终端和后台系统服务器之外的第三方设备，也可以是内置于终端和/或后台系统服务器中的软件模块。前者可以降低服务器和终端的处理压力，后者减少了信息与外部设备的交互次数，安全性高且硬件成本低。

其中，终端通知验证装置根据待验证密码和操作请求信息签名报文进行验证的步骤，

包括如下任一方式：

方式一：验证装置内置于终端，其中终端内的验证装置分别对待验证密码和签名报文进行验证；

方式二：验证装置内置于后台系统服务器，其中终端至少将待验证密码、操作请求信息和签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置根据所述待验证密码和所述操作请求信息对签名报文进行验证。

上述方式可以根据终端的处理性能进行选择，如在终端处理能力较强时，可以根据方式一，在处理能力有限或者验证操作过多时，根据方式二，在保证验证操作完成的前提下，兼顾终端的处理负荷。

由此可以看出，终端通过获取当前的处理负荷，并根据自身负荷控制验证方式，保证在完成验证的前提下，兼顾自身的处理性能。

其中，验证装置在采用方式二根据待验证密码和操作请求信息对签名报文进行验证时，方法还包括：

终端从智能卡获取联合密码的内容调整策略，其中根据联合密码的内容调整策略处理后的联合密码为生成签名报文所使用的联合密码，和/或，终端从智能卡获取操作请求信息的内容调整策略，其中根据操作请求信息的内容调整策略处理后的操作请求信息为生成签名报文所使用的操作请求信息；

终端将联合密码的内容调整策略和/或操作请求信息的内容调整策略发送给验证装置。

其中，验证装置验证签名报文的流程与智能卡生成签名报文的流程相似，具体来说：

如果没有接收到任何内容调整策略，则直接根据待验证密码和操作请求信息生成一个待验证报文，将该待验证报文与签名报文进行比较，如果相同，则验证通过；如果不相同，则验证不同；

如果接收到包括联合密码和操作请求信息中至少一个的内容调整策略，其中针对于联合密码的内容调整策略，则根据联合密码的内容调整策略对待验证密码进行调整，针对于操作请求信息的内容调整策略，则根据操作请求信息的内容调整策略对操作请求信息进行调整，最终将调整后的信息，得到待验证报文，将该待验证报文与签名报文进行验证即可。

对于后者，所述验证装置在采用所述方式二对所述签名报文进行验证时，所述终端从智能卡获取所述联合密码的内容调整策略，其中根据所述联合密码的内容调整策略处理后的联合密码为生成所述签名报文所使用的联合密码，和/或，所述终端从智能卡获取所述操作请求信息的内容调整策略，其中根据所述操作请求信息的内容调整策略处理后的操作请求信息为生成所述签名报文所使用的操作请求信息；将所述联合密码的内容调整策略和/或

所述操作请求信息的内容调整策略发送给所述验证装置。

步骤 A09、验证装置在签名报文验证通过后，触发响应操作请求的流程。

本发明的方法实施例，对待验证密码和签名报文进行验证，并在验证通过后，才会将交易指令发送至后台系统服务器，以触发后台系统服务器响应操作请求的流程，从而防止将签名数据等重要数据通过网络进行传输而导致不安全的隐患，保证了交易的安全性。另外，本发明的联合密码可以是在每次交易时随机生成的数字、字母和字符的一种或多种的组合，不同于现有的交易密码和 OTP 必须根据密文进行传输，本发明终端可以不同方式获取联合密码，在获取的过程中，该联合密码（验证密码）可以以明文的形式进行传输，并且不会降低交易过程中账户的安全性；本发明由智能卡生成联合密码并进行签名，以保证联合密码传输至终端的安全性和终端验证联合密码的准确性。

由此可见本发明的智能卡交易方法，通过智能卡和终端的一次接入即完成了交易所需数据（例如签名数据）的交互，降低了多次接入造成的重要信息被截获的风险，提高了安全性。

为了便于本领域技术人员更清晰的了解本发明公开的内容，下面以一具体场景进行说明：

该场景中后台系统服务器可以为银行后台系统服务器或第三方服务器，第三方服务器为非银行系统根据的服务器，比如公交系统所根据的对公交卡进行充值和扣款控制的服务器等，终端可以为各服务器的外设终端，如 POS 机等。

POS 机检测到用户的支付请求后，向该用户的智能卡发送本次的交易报文；

智能卡根据本地生成的联合密码和交易报文生成签名报文，将签名报文发送给 POS 机；

在 POS 机获取到签名报文后，如果智能卡检测到智能卡断开与智能卡连接，则输出签名报文所使用的联合密码的提示信息；

POS 机在获取到提示信息对应的联合密码，将获取到的联合密码作为待验证密码，通知内置于 POS 机的验证装置根据待验证密码和操作请求信息对签名报文进行验证的流程，在签名报文和联合密码均验证通过后，POS 向银行后台系统服务器发送支付请求；

之后，银行后台系统服务器会根据支付请求进行相应的操作。

由上可以看出，上述操作就是日常的刷卡支付行为，在保证信息安全的前提下，实现了 POS 的支付功能，且智能卡与 POS 机仅进行了一次连接，操作简单。

图 3 为本发明提供的另一种用户请求的处理方法实施例的流程示意图。图 3 所示方法

实施例包括：

步骤 301、终端在检测到用户的操作请求后，向智能卡发送用户的操作请求信息；

步骤 302、智能卡在获取到终端输出的操作请求信息后，根据预先设置的签名生成策略，根据操作请求信息生成签名报文；

步骤 303、智能卡根据本地预先保存的密码生成策略生成联合密码；

步骤 304、智能卡在得到联合密码后，根据预先设置的联合密码的调整策略，对联合密码调整，得到调整后的联合密码；

步骤 305、智能卡将调整后的联合密码和签名报文发送至终端；

步骤 306、在终端获取到签名报文和调整后的联合密码后，如果智能卡检测到与终端断开连接，则智能卡输出联合密码的提示信息，联合密码为与签名报文一同发送至终端的联合密码；

步骤 307、终端在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码，终端通知验证装置对待验证密码和签名报文进行验证；

步骤 308、验证装置在签名报文和待验证密码均验证通过后，触发响应操作请求的流程。

与现有技术中智能卡和终端至少两次接入才能完成用户身份的鉴权数据的生成相比，本发明提供的方法实施例，通过智能卡和终端的一次接入完成用户身份的鉴权数据的生成和传输，降低了智能卡和终端多次接入造成重要信息被截获的风险，提高了安全性，且减少了多次接入给操作人员带来的手动操作。

下面对上述方法实施例作进一步说明：本实施例所提供的方法包括如下步骤：

步骤 B01、终端在检测到用户的操作请求后，向智能卡发送用户的操作请求信息；

其中，用户的操作请求可以是访问某个账号；或者，修改个人的信息，如修改某一账号的密码，或者，将某一账号对应的信息进行修改，如修改某一存储账号的金额等；

例如，用户的操作请求为向某个账号转账一定数额的存款。则操作请求信息可以包括账户和金额，还可包括交易明细信息等。

步骤 B02、在获取到终端输出的操作请求信息后，根据预先设置的签名生成策略，根据操作请求信息生成签名报文；

其中，智能卡接入终端之前，终端可通过手工输入、网络、扫描商品信息等方式获取操作请求信息。

其中，智能卡与终端的接入方式可以为通过非接触方式或接触方式。其中，优选非接触方式接入终端，其与接触方式接入终端相比，具有较高的安全性，防止信息被获取。

在实际应用中，可以不对操作请求信息进行任何处理直接生成签名报文，但为了提高签名报文的安全性，可以根据如下处理方式：

智能卡获取操作请求信息的内容调整策略，根据获取到操作请求信息的内容调整策略，对操作请求信息的内容进行处理，得到调整后的操作请求信息；

智能卡根据调整后的操作请求信息，生成签名报文。

优选的，根据获取到操作请求信息的调整策略，对操作请求信息进行处理，得到调整后的操作请求信息的步骤，包括：

如果获取到操作请求信息的调整策略为对操作请求信息进行加密，则根据预先存储的加密算法的分配策略，获取用户操作请求对应的加密算法，根据该加密算法对用户操作请求进行加密，将加密后的用户操作请求作为调整后的操作请求信息。

其中，操作请求信息的加密可以使用可逆的加密算法，也可以使用不可逆的加密算法，如对操作请求信息进行摘要计算，其中摘要计算方式可以包括如下的一种或其组合：通过哈希算法计算的哈希值、通过 MAC 算法计算的 MAC 值，通过对称加密获得的密文本身。

通过对用户操作请求进行签名并将签名生成的报文发送至验证装置，可以保证操作请求的真实性，以及终端与智能卡交互结果的不可抵赖性。例如，在对金融交易系统中，可以保证交易为真实的交易，以及交易的不可抵赖性。

步骤 B03、智能卡根据本地预先保存的密码生成策略生成联合密码；

其中该密码生成策略可以预先保存的，也可以定期的进行更新，后者可以减少联合密码的生成规则被破解；

当然，密码生成策略可以包括密码生成算法和输入参数，其中密码生成算法可以有多种，输入参数可以是一些实时信息作为生成联合密码时所需的输入参数，如时间信息或随机数等，保证联合密码生成的多样性。

另外，该密码生成策略也可以是随机生成，如智能卡随机地生成数字、字母和/或符号，从数字、字母和符号中选择一种或多种组合生成联合密码，可以保证联合密码的不唯一性，随机性，提高联合密码的安全性。

通过对用户操作请求进行签名并将签名生成的报文发送至验证装置，可以保证操作请求的真实性，以及终端与智能卡交互结果的不可抵赖性。例如，在对金融交易系统中，可以保证交易为真实的交易，以及交易的不可抵赖性。

步骤 B04、在得到联合密码后，根据预先设置的联合密码的调整策略，对联合密码的内容进行调整，得到调整后的联合密码；

其中，采用如下任一方式对联合密码的内容进行调整：

方式一：如果获取到联合密码的调整策略为对联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

方式二：如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，将处理后的联合密码作为调整后的联合密码，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式三：如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式四：如果获取到联合密码的调整策略为对联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略。

下面对方式一至四分别进行说明：

方式一与常规的加密算法不同的是，其所使用的加密算法在每次可以是不同的，增加了加密算法的随机性，使得加密效果更好，降低了加密算法被破解的可能。

方式二在联合密码中增加随机数，并在联合密码被破解后，如破解者不能获知对联合密码对应的随机数和随机数组合策略，提高了签名报文的安全性；另外，每次对联合密码内容的调整原则也可以是不同的，提高内容调整方式的多样性，增加调整方式的随机性，降低内容调整方式被破解的可能。

方式三和方式四均是对方式一和方式二的优化方案，较前两个方式安全性更高。

其中，针对方式二中，联合密码为 123456，生成的随机数为 789，随机数组合策略为

在联合密码最后一位增加随机数，则调整后的联合密码为 123456789。

其中为了保证终端爱在后续验证时，能够得到最原始的联合密码，需通知终端所使用的联合密码和该随机数组合策略。

当然，随机数组合策略可以有很多种，如联合密码中每隔一位增加一个随机数。

当然，联合密码的调整策略还可以是如下方式：

在联合密码长度达到某一预先设置的阈值时，根据获取到的删除策略，删除该联合密码中一个或多个位置的信息，将执行删除操作后剩余的联合密码作为调整后的联合密码；或者，

在联合密码长度达到某一预先设置的阈值时，根据获取到的选取策略中设置的位置信息，选取该联合密码中对应的位置信息组成新的联合密码，将组合产生的新的联合密码作为调整后的联合密码；

从本地预先保存的多个计算表达式中，获取一个计算表达式，将该联合密码作为该运算表达式的输入参数进行计算，将计算结果作为调整后的联合密码。

当然上述方式中都需要通知终端在对联合密码调整时所需使用的策略。

其中，方式一对联合密码加密可以为对联合密码进行数字签名。

步骤 B05、将调整后的联合密码和签名报文发送至终端；

步骤 B06、在终端获取到签名报文和调整后的联合密码后，如果智能卡检测到与终端断开连接，则智能卡输出联合密码的提示信息；

其中，该智能卡输出的联合密码信息可以是直接显示该联合密码；或者，该联合密码的条码信息；也可以是，通过非接触方式发送出去；

可选的，为了保证控制联合密码在有限范围内的输出，防止被他人读取，智能卡输出联合密码信息之前还包括：

按照预先设置的身份认证策略，对请求输出联合密码的请求方进行身份认证；

如果认证成功，则输出联合密码。

其中该认证方式可以访问该智能卡的密码信息，或者，专门的身份认证机制。

步骤 B07、终端在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码，终端通知验证装置对待验证密码和签名报文进行验证；

需要说明的是，之所以步骤 A08 中的“终端在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码”，终端需要接收例如手动输入或者扫描获得的联合密码，根据上述方式进行获取的联合密码（即待验证密码），有可能因为信息传输或操作失误造成得到的联合密码（即待验证密码）错误，会造成得到的待验证密码与签名报文中的联

合密码不一致，从而使得验证不能通过。

其中，待验证密码是通过如下任一方式得到的，包括：

方式一：对终端上输入设备输入的信息进行检测，根据检测结果，得到待验证密码；

方式二：如果智能卡通过显示屏幕显示联合密码的条码信息或图形信息，则对条码信息或图形信息进行扫描，得到待验证密码；

方式三：通过以非接触通讯方式与智能卡建立通信连接，并通过通信连接获取智能卡发送的联合密码，将接收到联合密码作为待验证密码。

步骤 B08、验证装置在签名报文和待验证密码均验证通过后，触发响应操作请求的流程；

其中，验证装置可以为除了终端和后台系统服务器之外的第三方设备，也可以是内置于终端和/或后台系统服务器中的软件模块。前者可以降低服务器和终端的处理压力，后者减少了信息与外部设备的交互次数，安全性高且硬件成本低。

其中，终端通知验证装置对待验证密码和签名报文进行验证，包括如下任一方式：

方式一：验证装置内置于终端，其中终端分别对待验证密码和签名报文进行验证；

方式二：验证装置内置于服务器，其中终端将待验证密码和签名报文发送给后台系统服务器，指示后台系统服务器对待验证密码和签名报文进行验证；

方式三：验证装置内置于终端和服务器，其中终端对待验证密码进行验证，并在验证通过后，将签名报文发送给后台系统服务器，指示后台系统服务器对签名报文进行验证；

方式四：验证装置内置于终端和服务器，其中终端对签名报文进行验证待验证密码进行验证，并在验证通过后，将联合密码发送给后台系统服务器，指示后台系统服务器对联合密码进行验证。

上述方式可以根据终端的处理性能进行选择，如在终端处理能力较强时，可以根据方式一，在处理能力有限或者验证操作过多时，根据方式二，在保证验证操作完成的前提下，兼顾终端的处理负荷。方式三和方式四是方式一和方式二中的折中处理方式。

由此可以看出，终端通过获取当前的处理负荷，并根据自身负荷控制验证方式，保证在完成验证的前提下，兼顾自身的处理性能。

其中，验证装置验证签名报文的流程与智能卡生成签名报文的流程相似，具体来说：

如果没有接收到任何内容调整策略，则直接根据待验证密码和操作请求信息生成一个待验证报文，将该待验证报文与签名报文进行比较，如果相同，则验证通过；如果不相同，则验证不同；

如果接收到包括联合密码和操作请求信息中至少一个的内容调整策略，其中针对于联合密码的内容调整策略，则根据联合密码的内容调整策略对待验证密码进行调整，针对于操作请求信息的内容调整策略，则根据操作请求信息的内容调整策略对操作请求信息进行调整，最终将调整后的信息，得到待验证报文，将该待验证报文与签名报文进行验证即可。

对于后者，所述验证装置在采用所述方式二至四中任一对所述签名报文进行验证时，所述终端从智能卡获取所述联合密码的内容调整策略，其中根据所述联合密码的内容调整策略处理后的联合密码为生成所述签名报文所使用的联合密码，和/或，所述终端从智能卡获取所述操作请求信息的内容调整策略，其中根据所述操作请求信息的内容调整策略处理后的操作请求信息为生成所述签名报文所使用的操作请求信息；将所述联合密码的内容调整策略和/或所述操作请求信息的内容调整策略发送给所述验证装置。

本发明的实施例，对待验证密码和签名报文进行验证，并在验证通过后，才会将交易指令发送至后台系统服务器，以触发后台系统服务器响应操作请求的流程，从而防止将签名数据等重要数据通过网络进行传输而导致不安全的隐患，保证了交易的安全性。另外，本发明的联合密码可以是在每次交易时随机生成的数字、字母和字符的一种或多种的组合，不同于现有的交易密码和 OTP 必须根据密文进行传输，本发明终端可以不同方式获取联合密码，在获取的过程中，该联合密码（验证密码）可以以明文的形式进行传输，并且不会降低交易过程中账户的安全性；本发明由智能卡生成联合密码并进行签名，以保证联合密码传输至终端的安全性和终端验证联合密码的准确性。

由此可见本发明的智能卡交易方法，通过智能卡和终端的一次接入即完成了交易所需数据（例如签名数据）的交互，降低了多次接入造成的重要信息被截获的风险，提高了安全性。

为了便于本领域技术人员更清晰的了解本发明公开的内容，下面以一具体场景进行说明：

该场景中后台系统服务器可以为银行后台系统服务器或第三方服务器，第三方服务器为非银行系统根据的服务器，比如公交系统所根据的对公交卡进行充值和扣款控制的服务器等，终端可以为各服务器的外设终端，如 POS 机等。

POS 机检测到用户的支付请求后，向该用户的智能卡发送本次的交易报文；

智能卡根据交易报文生成签名报文；以及对本地生成的联合密码的内容调整，得到调整后的联合密码；

POS 机在获取到签名报文后，断开与智能卡连接；

智能卡在检测到与终端断开连接后，输出签名报文所使用的联合密码的信息；

POS 机获取智能卡输出的联合密码，将获取到的联合密码作为待验证密码，触发分别对待验证密码和签名报文进行验证的流程，在签名报文和联合密码均验证通过后，POS 向银行后台系统服务器发送支付请求；

之后，银行后台系统服务器会根据支付请求进行相应的操作。

由上可以看出，上述操作就是日常的刷卡支付行为，在保证信息安全的前提下，实现了移动支付功能，且智能卡与 POS 机仅进行了一次连接，操作简单。

为了便于本领域技术人员更清晰的了解本发明公开的内容，下面以一具体场景进行说明：

该场景中后台系统服务器可以为银行服务器或第三方服务器，第三方服务器为非银行系统根据的服务器，比如公交系统所根据的对公交卡进行充值和扣款控制的服务器等，终端可以为各服务器的外设终端，如 POS 机等。

POS 机检测到用户的支付请求后，向该用户的智能卡发送本次的交易报文；

智能卡根据交易报文生成签名报文；以及，对本地生成的联合密码的内容进行调整，得到调整后的联合密码；

将签名报文和调整后的联合密码发送给 POS 机；

在 POS 机获取到签名报文后，如果智能卡检测到智能卡断开与智能卡连接，则输出签名报文所使用的联合密码的提示信息；

POS 机在获取到提示信息对应的联合密码，将获取到的联合密码作为待验证密码，通知内置于 POS 机的验证装置分别对待验证密码和签名报文进行验证的流程，在签名报文和联合密码均验证通过后，POS 向银行后台系统服务器发送支付请求；

之后，银行后台系统服务器会根据支付请求进行相应的操作。

由上可以看出，上述操作就是日常的刷卡支付行为，在保证信息安全的前提下，实现了移动支付功能，且智能卡与 POS 机仅进行了一次连接，操作简单。

图 4 为本发明提供的处理操作请求的系统实施例的结构示意图。图 3 所示系统实施例中，系统包括终端、智能卡和验证装置，其中终端包括第一发送模块 401 和通知模块 402，智能卡包括保存模块 403、第一生成模块 404、第二生成模块 405、第二发送模块 406 以及输出模块 407，验证装置还包括触发模块 408，其中：

第一发送模块 401，用于在检测到用户的操作请求后，向智能卡发送用户的操作请求信息；

保存模块 403，与第一发送模块 401 相连，用于在获取到终端输出的操作请求信息后，

保存操作请求信息；

第一生成模块 404，用于根据本地预先保存的密码生成策略生成联合密码；

第二生成模块 405，与保存模块 403 和第一生成模块 404 相连，用于在得到联合密码后，根据操作请求信息和联合密码生成签名报文；

第二发送模块 406，与第二生成模块 405 相连，用于将签名报文发送给终端；

输出模块 407，用于在终端获取到签名报文后，如果智能卡检测到与终端断开连接，则输出联合密码的提示信息；

通知模块 402，用于在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码，通知验证装置根据待验证密码和操作请求信息对签名报文进行验证；

触发模块 408，用于在签名报文验证通过后，触发响应操作请求的流程。

其中，第二生成模块 405，包括：第一处理子模块和第二处理子模块中的至少一个、生成子模块以及通知子模块，其中：

第一处理子模块包括：

第一获取单元，用于获取操作请求信息的内容调整策略；

第一处理单元，与第一获取单元相连，用于根据获取到操作请求信息的内容调整策略，对操作请求信息的内容进行处理，得到调整后的操作请求信息；

第二处理子模块，包括

第二获取单元，用于智能卡获取联合密码的内容调整策略；

第二处理单元，与第二获取单元相连，用于根据获取到联合密码的内容调整策略，对联合密码的内容进行调整，得到调整后的联合密码；

生成子模块，用于对如下任一组合进行签名，生成签名报文，其中：

组合一为调整后的操作请求信息和联合密码；

组合二为操作请求信息和调整后的联合密码；

组合三为调整后的操作请求信息和调整后的联合密码；

其中，通知子模块，用于通知组合一中调整后的操作请求信息所使用的内容调整策略；或者，通知组合二中调整后的联合密码所使用的内容调整策略，或者，通知调整后的操作请求信息内容调整策略以及调整后的联合密码所使用的内容调整策略。

其中，第一处理单元，用于如果获取到操作请求信息的调整策略为对操作请求信息进行加密，则根据预先存储的加密算法的分配策略，获取用户操作请求对应的加密算法，根据该加密算法对用户操作请求进行加密，将加密后的用户操作请求作为调整后的操作请求信息。

其中，第二处理单元，用于根据如下任一方式处理联合密码：

方式一：如果获取到联合密码的调整策略为对联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

方式二：如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式三：如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式四：如果获取到联合密码的处理策略为对联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略。

其中，输出模块包括：

认证单元，用于按照预先设置的身份认证策略，对请求输出联合密码的请求方进行身份认证；

输出单元，用于如果认证成功，则输出联合密码。

其中，待验证密码是通过如下任一方式得到的，包括：

方式一：对终端上输入设备输入的信息进行检测，根据检测结果，得到待验证密码；

方式二：如果智能卡通过显示屏幕显示联合密码的条码信息或图形信息，则对条码信息或图形信息进行扫描，得到待验证密码；

方式三：通过以非接触通讯方式与智能卡建立通信连接，并通过通信连接获取智能卡发送的联合密码，将接收到联合密码作为待验证密码。

其中，验证装置为内置于终端和/或后台系统服务器的软件模块。

其中，终端通知验证装置对待验证密码和签名报文进行验证，包括如下任一方式：

方式一：验证装置内置于终端，其中终端内的验证装置分别对待验证密码和签名报文进行验证；

方式二：验证装置内置于后台系统服务器，其中终端将待验证密码和签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置对待验证密码和签名报文进行验证；

方式三：验证装置内置于终端和后台系统服务器，其中终端内的验证装置对待验证密码进行验证，并在验证通过后，将签名报文发送给后台系统服务器，指示后台系统服务器内的验证装置对签名报文进行验证；

方式四：验证装置内置于终端和后台系统服务器，其中终端内的验证装置对签名报文进行验证，并在验证通过后，将待验证密码发送给后台系统服务器，指示后台系统服务器内的验证装置对联合密码进行验证。

本发明的系统实施例，对待验证密码和签名报文进行验证，并在验证通过后，才会将交易指令发送至后台系统服务器，以触发后台系统服务器响应操作请求的流程，从而防止将签名数据等重要数据通过网络进行传输而导致不安全的隐患，保证了交易的安全性。另外，本发明的联合密码可以是在每次交易时随机生成的数字、字母和字符的一种或多种的组合，不同于现有的交易密码和 OTP 必须根据密文进行传输，本发明终端可以不同方式获取联合密码，在获取的过程中，该联合密码（验证密码）可以以明文的形式进行传输，并且不会降低交易过程中账户的安全性；本发明由智能卡生成联合密码并进行签名，以保证联合密码传输至终端的安全性和终端验证联合密码的准确性。

由此可见本发明的智能卡交易方法，通过智能卡和终端的一次接入即完成了交易所需数据（例如签名数据）的交互，降低了多次接入造成的重要信息被截获的风险，提高了安全性。

图 5 为本发明提供的另一种处理操作请求的系统实施例的结构示意图。图 5 所示系统实施例包括终端、智能卡和验证装置，其中终端包括第一发送模块 501 和通知模块 502，智能卡包括第一生成模块 503、第二生成模块 504、调整模块 505、第二发送模块 506 以及输出模块 507，验证装置包括触发模块 508，其中：

第一发送模块 501，用于在检测到用户的操作请求后，向智能卡发送用户的操作请求信息；

第一生成模块 503，与第一发送模块 501 相连，用于在获取到终端输出的操作请求信息后，根据预先设置的签名生成策略，根据操作请求信息生成签名报文；

第二生成模块 504，用于根据本地预先保存的密码生成策略生成联合密码；

调整模块 505，与第二生成模块 504 相连，用于根据预先设置的联合密码的调整策略，对联合密码的内容进行调整，得到调整后的联合密码；

第二发送模块 506，与第一生成模块 503 和调整模块 505 相连，用于将调整精辟的联合密码和签名报文发送至终端；

输出模块 506，用于在终端获取到签名报文和调整后的联合密码后，如果智能卡检测到与终端断开连接，则输出联合密码的提示信息；

通知模块 507，用于在接收到提示信息对应的联合密码后，将获取到的联合密码作为待验证密码，通知验证装置对待验证密码和签名报文进行验证；

触发模块 508，用于在签名报文和待验证密码均验证通过后，触发响应操作请求的流程。

其中，调整模块 505 采用如下任一方式对联合密码的内容进行调整，包括：

方式一：如果获取到联合密码的调整策略为对联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

方式二：如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式三：如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略；

方式四：如果获取到联合密码的处理策略为对联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据获取到的随机数和随机数组合策略，对加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知终端调整后的联合密码所使用的随机数和随机数组合策略。

其中，所述验证装置内置于终端和/或后台系统服务器。

其中，所述验证装置对所述待验证密码和所述签名报文进行验证的步骤，包括如下任一方式：

方式一：所述验证装置内置于所述终端，其中所述终端内的验证装置分别对所述待验证密码和所述签名报文进行验证；

方式二：所述验证装置内置于所述后台系统服务器，其中所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置对所述待验证密码和所述签名报文进行验证；

方式三：所述验证装置内置于所述终端和所述后台系统服务器，其中所述终端内的验证装置对所述待验证密码进行验证，并在验证通过后，至少将所述签名报文、所述待验证密码和所述操作请求信息发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述签名报文进行验证；

方式四：所述验证装置内置于所述终端和所述后台系统服务器，其中所述终端内的验证装置对所述签名报文进行验证，并在验证通过后，至少将所述待验证密码发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述待验证密码进行验证。

本发明的系统实施例，对待验证密码和签名报文进行验证，并在验证通过后，才会将交易指令发送至后台系统服务器，以触发后台系统服务器响应操作请求的流程，从而防止将签名数据等重要数据通过网络进行传输而导致不安全的隐患，保证了交易的安全性。另外，本发明的联合密码可以是在每次交易时随机生成的数字、字母和字符的一种或多种的组合，不同于现有的交易密码和 OTP 必须根据密文进行传输，本发明终端可以不同方式获取联合密码，在获取的过程中，该联合密码（验证密码）可以以明文的形式进行传输，并且不会降低交易过程中账户的安全性；本发明由智能卡生成联合密码并进行签名，以保证联合密码传输至终端的安全性和终端验证联合密码的准确性。

由此可见本发明的智能卡交易方法，通过智能卡和终端的一次接入即完成了交易所需

数据（例如签名数据）的交互，降低了多次接入造成的重要信息被截获的风险，提高了安全性。

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。

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根据硬件的形式实现，也可以根据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时，也可以存储在一个计算机可读取存储介质中。

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、材料或者特点包括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的一个或多个实施例或示例中以合适的方式结合。

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、一种处理操作请求的方法，其特征在于，所述方法包括：

终端在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；

智能卡在获取到终端输出的操作请求信息后，保存所述操作请求信息，并根据本地预先保存的密码生成策略生成联合密码，在得到所述联合密码后，根据所述操作请求信息和所述联合密码生成签名报文，并至少将所述签名报文发送给终端；

在所述终端获取到签名报文后，如果所述智能卡检测到与所述终端断开连接，则智能卡输出所述联合密码的提示信息；

所述终端在接收到所述提示信息对应的联合密码后，将获取到的所述联合密码作为待验证密码，所述终端通知验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证，所述验证装置在所述签名报文验证通过后，触发响应所述操作请求的流程。

2、根据权利要求 1 所述的方法，其特征在于，所述根据所述操作请求信息和所述联合密码生成签名报文的步骤，包括：

获取操作请求信息的内容调整策略，并根据获取到操作请求信息的内容调整策略，对所述操作请求信息的内容进行处理，得到调整后的操作请求信息；和/或，获取联合密码的内容调整策略，并根据获取到联合密码的内容调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；

对如下任一组合进行签名，生成签名报文，其中所述组合包括：

调整后的操作请求信息和所述联合密码；

所述操作请求信息和调整后的联合密码；

调整后的操作请求信息和调整后的联合密码；

3、根据权利要求 2 所述的方法，其特征在于，所述方法还包括：

通知所述终端所述调整后的操作请求信息所使用的内容调整策略；或者

通知所述终端所述调整后的联合密码所使用的内容调整策略；或者

通知所述终端所述调整后的操作请求信息内容调整策略以及调整后的联合密码所使用的内容调整策略。

4、根据权利要求 2 或 3 所述的方法，其特征在于，所述根据获取到操作请求信息的内

容调整策略，对所述操作请求信息的内容进行处理，得到调整后的操作请求信息，包括：

如果获取到操作请求信息的内容调整策略为对所述操作请求信息进行加密，则根据预先存储的加密算法的分配策略，获取所述用户操作请求对应的加密算法，根据所述加密算法对所述用户操作请求进行加密，将加密后的所述用户操作请求作为所述调整后的操作请求信息。

5、根据权利要求 2 或 3 所述的方法，其特征在于，所述根据获取到联合密码的内容调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码，包括以下任一方式：

如果获取到联合密码的内容调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取所述联合密码对应的加密算法，根据所述加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

如果内容调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取所述联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理得到调整后的联合密码，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果获取到联合密码的内容调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取所述联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理得到处理后的联合密码，再根据预先存储的加密算法的分配策略，获取所述处理后的联合密码对应的加密算法，根据所述加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果获取到联合密码的内容调整策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取所述联合密码对应的加密算法，根据所述加密算法对所述联合密码进行加密获取加密后的联合密码，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取所述加密后的联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

6、根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述智能卡输出所述联合密码的提示信息包括：

按照预先设置的身份认证策略，对请求输出联合密码的请求方进行身份认证；

如果认证成功，则输出联合密码。

7、根据权利要求 1 至 6 中任一项所述的方法，其特征在于，所述待验证密码是通过如下任一方式得到的，包括：

对所述终端上输入设备输入的信息进行检测，根据检测结果，得到所述待验证密码；

如果所述智能卡通过显示屏幕显示所述联合密码的条码信息或图形信息，则对所述条码信息或图形信息进行扫描，得到所述待验证密码；

通过以非接触通讯方式与所述智能卡建立通信连接，并通过所述通信连接获取所述智能卡发送的联合密码，将接收到联合密码作为待验证密码。

8、根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述验证装置内置于终端和/或后台系统服务器。

9、根据权利要求 8 所述的方法，其特征在于，所述终端通知验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证，包括如下任一方式：

所述终端内的验证装置直接根据所述待验证密码和所述操作请求信息对所述签名报文进行验证；

所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证。

10、根据权利要求 9 所述的方法，其特征在于，所述方法还包括：

在所述后台系统服务器内的验证装置对所述签名报文进行验证时，所述终端从智能卡获取所述联合密码的内容调整策略，其中根据所述联合密码的内容调整策略处理后的联合密码为生成所述签名报文所使用的联合密码，和/或，所述终端从智能卡获取所述操作请求信息的内容调整策略，其中根据所述操作请求信息的内容调整策略处理后的操作请求信息为生成所述签名报文所使用的操作请求信息；

所述终端将所述联合密码的内容调整策略和/或所述操作请求信息的内容调整策略发送给所述后台系统服务器内的验证装置以对所述签名报文进行验证。

11、一种处理操作请求的方法，其特征在于，所述方法包括：

终端在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；

智能卡在获取到终端输出的操作请求信息后，根据预先设置的签名生成策略对所述操作请求信息进行签名生成签名报文，以及根据本地预先保存的密码生成策略生成联合密码，在得到联合密码后，根据预先设置的联合密码的调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；将所述调整后的联合密码和所述签名报文发送至所述终端；

在所述终端获取到签名报文和调整后的联合密码后，如果所述智能卡检测到与所述终端断开连接，则输出所述联合密码的提示信息；

所述终端在接收到所述提示信息对应的联合密码后，将获取到的所述联合密码作为待验证密码，所述终端通知验证装置对所述待验证密码和所述签名报文进行验证，所述验证装置在所述签名报文和所述待验证密码均验证通过后，触发响应所述操作请求的流程。

12、根据权利要求 11 所述的方法，其特征在于，根据预先设置的联合密码的调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码，包括以下任一方式：

如果联合密码的调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取所述联合密码对应的加密算法，根据所述加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取所述联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取所述联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理获取处理后的联合密码，再根据预先存储的加密算法的分配策略，获取所述处理后的联合密码对应的加密算法，根据所述加密算法对所述处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果联合密码的调整策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取所述联合密码对应的加密算法，根据所述加密算法对所述联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取加密后的联合密码对应的随机数组合策略；

根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

13、根据权利要求 11 或 12 所述的方法，其特征在于，所述验证装置内置于终端和/或后台系统服务器。

14、根据权利要求 13 所述的方法，其特征在于，所述终端通知验证装置对所述待验证密码和所述签名报文进行验证的步骤，包括如下任一方式：

所述终端内的验证装置分别对所述待验证密码和所述签名报文进行验证；

所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置对所述待验证密码和所述签名报文进行验证；

所述终端内的验证装置对所述待验证密码进行验证，并在验证通过后，至少将所述签名报文、所述待验证密码和所述操作请求信息发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述签名报文进行验证；

所述终端内的验证装置对所述签名报文进行验证，并在验证通过后，至少将所述待验证密码发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述待验证密码进行验证。

15、一种处理操作请求的系统，其特征在于，所述系统包括终端、智能卡和验证装置，其中所述终端包括第一发送模块和通知模块，所述智能卡包括保存模块、第一生成模块、第二生成模块、第二发送模块以及输出模块，所述验证装置包括触发模块，其中：

所述第一发送模块，用于在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；

所述保存模块，与所述第一发送模块相连，用于在获取到终端输出的操作请求信息后，保存所述操作请求信息；

所述第一生成模块，用于根据本地预先保存的密码生成策略生成联合密码；

所述第二生成模块，与所述保存模块和所述第一生成模块相连，用于在得到联合密码后，根据所述操作请求信息和所述联合密码生成签名报文；

所述第二发送模块，与所述第二生成模块相连，用于将所述签名报文发送给终端；

所述输出模块，用于在所述终端获取到签名报文后，如果所述智能卡检测到与所述终

端断开连接，则输出所述联合密码的提示信息；

所述通知模块，用于在接收到所述提示信息对应的联合密码后，将获取到的所述联合密码作为待验证密码，通知所述验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证；

所述触发模块，用于在所述签名报文验证通过后，触发响应所述操作请求的流程。

16、根据权利要求 15 所述的系统，其特征在于，所述第二生成模块包括：第一处理子模块和第二处理子模块中的至少一个和生成子模块，其中：

所述第一处理子模块包括：

第一获取单元，用于获取操作请求信息的内容调整策略；

第一处理单元，与所述第一获取单元相连，用于根据获取到操作请求信息的内容调整策略，对所述操作请求信息的内容进行处理，得到调整后的操作请求信息；

所述第二处理子模块，包括：

第二获取单元，用于获取联合密码的内容调整策略；

第二处理单元，与所述第二获取单元相连，用于根据获取到联合密码的内容调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；

所述生成子模块，用于对如下任一组合进行签名，生成签名报文，其中所述组合包括：

调整后的操作请求信息和所述联合密码；

所述操作请求信息和调整后的联合密码；

调整后的操作请求信息和调整后的联合密码。

17、根据权利要求 16 所述的系统，其特征在于，所述第二生成模块还包括：

通知子模块，用于通知所述终端调整后的操作请求信息所使用的内容调整策略；或者，通知所述终端调整后的联合密码所使用的内容调整策略，或者，通知所述终端调整后的操作请求信息内容调整策略以及调整后的联合密码所使用的内容调整策略。

18、根据权利要求 16 或 17 所述的系统，其特征在于：

所述第一处理单元，用于如果获取到操作请求信息的调整策略为对所述操作请求信息进行加密，则根据预先存储的加密算法的分配策略，获取所述用户操作请求对应的加密算法，根据该加密算法对所述用户操作请求进行加密，将加密后的所述用户操作请求作为调整后的操作请求信息。

19、根据权利要求 16 或 17 所述的系统，其特征在于，所述第二处理单元，用于根据如下任一方式处理联合密码：

如果获取到联合密码的调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理获取处理后的联合密码，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果获取到联合密码的调整策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

20、根据权利要求 15 至 19 中任一项所述的系统，其特征在于，所述输出模块包括：

认证单元，用于按照预先设置的身份认证策略，对请求输出联合密码的请求方进行身份认证；

输出单元，用于如果认证成功，则输出联合密码。

21、根据权利要求 15 至 20 中任一项所述的系统，其特征在于，所述待验证密码是通过如下任一方式得到的，包括：

对所述终端上输入设备输入的信息进行检测，根据检测结果，得到所述待验证密码；

如果所述智能卡通过显示屏幕显示所述联合密码的条码信息或图形信息，则对所述条码信息或图形信息进行扫描，得到所述待验证密码；

通过以非接触通讯方式与所述智能卡建立通信连接，并通过所述通信连接获取所述智能卡发送的联合密码，将接收到联合密码作为待验证密码。

22、根据权利要求 15 至 21 中任一项所述的系统，其特征在于，所述验证装置内置于终端和/或后台系统服务器。

23、根据权利要求 22 所述的系统，其特征在于，所述验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证，包括如下任一方式：

所述终端内的验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证；

所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置根据所述待验证密码和所述操作请求信息对所述签名报文进行验证。

24、根据权利要求 23 所述的系统，其特征在于，所述终端还包括：

获取模块，用于从智能卡获取所述联合密码的内容调整策略，其中根据所述联合密码的内容调整策略处理后的联合密码为生成所述签名报文所使用的联合密码，和/或，所述终端从智能卡获取所述操作请求信息的内容调整策略，其中根据所述操作请求信息的内容调整策略处理后的操作请求信息为生成所述签名报文所使用的操作请求信息；

第三发送模块，与所述获取模块相连，用于将所述联合密码的内容调整策略和/或所述操作请求信息的内容调整策略发送给所述验证装置。

25、一种处理操作请求的系统，其特征在于，所述系统包括终端、智能卡和验证装置，其中所述终端包括第一发送模块和通知模块，所述智能卡包括第一生成模块、第二生成模块、调整模块、第二发送模块以及输出模块，所述验证装置包括触发模块，其中：

所述第一发送模块，用于在检测到用户的操作请求后，向所述智能卡发送所述用户的操作请求信息；

所述第一生成模块，与所述第一发送模块相连，用于在获取到终端输出的操作请求信息后，根据预先设置的签名生成策略，根据所述操作请求信息生成签名报文；

所述第二生成模块，用于根据本地预先保存的密码生成策略生成联合密码；

所述调整模块，与所述第二生成模块相连，用于根据预先设置的联合密码的调整策略，对所述联合密码的内容进行调整，得到调整后的联合密码；

所述第二发送模块，与所述第一生成模块和所述调整模块相连，用于将所述调整后的联合密码和所述签名报文发送至所述终端；

所述输出模块，用于在所述终端获取到签名报文和调整后的联合密码后，如果所述智能卡检测到与所述终端断开连接，则输出所述联合密码的提示信息；

所述通知模块，用于在接收到所述提示信息对应的联合密码后，将获取到的所述联合密码作为待验证密码，通知所述验证装置对所述待验证密码和所述签名报文进行验证；

所述触发模块，用于在所述签名报文和所述待验证密码均验证通过后，触发响应所述操作请求的流程。

26、根据权利要求 25 所述的系统，其特征在于，所述调整模块采用如下任一方式对所述联合密码的内容进行调整，包括：

如果联合密码的调整策略为对所述联合密码进行加密，则根据预先存储的加密算法的分配策略，获取该联合密码对应的加密算法，根据该加密算法对所述联合密码进行加密，将加密后的联合密码作为调整后的联合密码输出；

如果调整策略为在联合密码中增加随机数，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，将处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果获取到联合密码的调整策略为增加随机数并对增加随机数后的联合密码进行加密，则根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述联合密码进行处理，再根据预先存储的加密算法的分配策略，获取处理后的联合密码对应的加密算法，根据该加密算法对处理后的联合密码进行加密，将经增加随机数且加密处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略；

如果联合密码的调整策略为对所述联合密码进行加密并在加密后的联合密码中增加随机数，则根据预先存储的加密算法的分配策略，获取联合密码对应的加密算法，根据该加

密算法对所述联合密码进行加密，再根据预先设置的随机数生成策略，获取随机数，以及，根据预先设置的随机数组合策略，获取该加密后的联合密码对应的随机数组合策略；根据所述获取到的随机数和随机数组合策略，对所述加密后的联合密码进行处理，将经加密且增加随机数处理后的联合密码作为调整后的联合密码输出，并通知所述终端所述调整后的联合密码所使用的随机数和随机数组合策略。

27、根据权利要求 25 或 26 所述的系统，其特征在于，所述验证装置内置于终端和/或后台系统服务器。

28、根据权利要求 27 所述的系统，其特征在于，所述验证装置对所述待验证密码和所述签名报文进行验证的步骤，包括如下任一方式：

所述终端内的验证装置分别对所述待验证密码和所述签名报文进行验证；

所述终端至少将所述待验证密码、所述操作请求信息和所述签名报文发送给后台系统服务器内的验证装置，指示后台系统服务器内的验证装置对所述待验证密码和所述签名报文进行验证；

所述终端内的验证装置对所述待验证密码进行验证，并在验证通过后，至少将所述签名报文、所述待验证密码和所述操作请求信息发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述签名报文进行验证；

所述终端内的验证装置对所述签名报文进行验证，并在验证通过后，至少将所述待验证密码发送给所述后台系统服务器，指示所述后台系统服务器内的验证装置对所述待验证密码进行验证。