

一种信息处理方法及系统

技术领域

5 本发明涉及电子技术领域，尤其涉及一种信息处理方法及系统。

背景技术

10 现今越来越多的人使用网络进行购物，而网络购物存在一定的风险，比如：网络交易所采用的账号和密码容易被盗取，给用户带来经济上的损失，网络购物的安全性有待进一步提高。

现有的网络购物交易过程中，对于买家来说，如果登陆到诈骗网站，在收货之前已将货款打入到诈骗网站的账户，造成买家经济上的损失；对于卖家来说，买家若采用货到付款的方式进行网络购物时，卖家在收到货款之前将货物发送至买家，若买家收到货物后仍拒绝付款或货物被他人冒领后买家拒绝付款，则会造成卖家经济上的损失。因此，现有的网络购物交易过程无法保证买卖双方交易过程中的安全。

发明内容

本发明旨在解决现有技术中网络交互双方信息安全性差的问题。

一种信息处理方法，方法包括：

20 第一终端在检测到用户的操作请求后，向电子签名装置发送用户的操作请求信息；电子签名装置在获取到第一终端输出的操作请求信息后，保存操作请求信息，并根据本地预先保存的密码生成策略生成联合密码，在得到联合密码后，根据操作请求信息和联合密码生成签名报文，以及，根据预先存储的联合密码的调整策略，对联合密码的内容进行调整，将调整后的联合密码作为第一处理密码，并将第一处理密码和签名报文一起发送给第一终端；第一终端在接收到签名报文和第一处理密码后，通知第一验证装置根据第一处理密码和操作请求信息对签名报文进行验证；如果验证通过，则第一验证装置通知后台系统服务器预处理操作请求信息；后台系统服务器根据预先设置的预处理策略对操作请求信息进行预处理，得到预处理信息；电子签名装置输出联合密码的提示信息；第二终端获取提示信息对应的联合密码，并将获取到的联合密码作为待验证密码；第二终端通知第二验证装置对待验证密码进行验证；如果验证通过，则第二验证装置触发后台系统服务器根据预处理信息响应操作请求信息的流程。

此外，根据操作请求信息和联合密码信息生成签名报文的步骤，包括：电子签名装置

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，电子签名装置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，将调整后的联合密码作为第二处理密码；电子签名装置对如下任一组合进行签名，生成签名
5 报文，其中组合包括：调整后的操作请求信息和联合密码；操作请求信息和第二处理密码；调整后的操作请求信息和第二处理密码。

此外，方法还包括：通知第一终端调整后的操作请求信息所使用的内容调整策略；或者，通知第一终端第二处理密码所使用的内容调整策略，或者，通知第一终端调整后的操作请求信息所使用的内容调整策略以及第二处理密码所使用的内容调整策略。

10 此外，第一终端通知第一验证装置根据第一处理密码和操作请求信息对签名报文进行验证，还包括：第一终端通知第一验证装置调整后的操作请求信息所使用的内容调整策略；或者，通知第一验证装置第二处理密码所使用的内容调整策略，或者，通知第一验证装置调整后的操作请求信息所使用的内容调整策略以及第二处理密码所使用的内容调整策略。

此外，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，
15 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。

此外，第一处理密码和/或第二处理密码是通过任一方式得到的：

20 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第一处理密码和/或第二处理密码输出；

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；
25 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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理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；根据获取到的随机数和随机数组合策略，
30 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，获取调整后的联合密码对

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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理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联合密码进行加密并在加密后的联合密码中增加
5 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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处
10 理密码和/或第二处理密码所使用的随机数和随机数组合策略。

此外，电子签名装置输出联合密码提示信息的步骤之前还包括：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。

此外，待验证密码是通过如下任一方式得到的：对第二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；如果电子签名装置通过显示屏幕显示联合密码
15 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；通过以非接触通讯方式与电子签名装置建立通信连接，并通过通信连接获取电子签名装置发送的联合密码，将接收到联合密码作为待验证密码。

一种信息处理系统，系统包括第一终端、电子签名装置、第一验证装置、后台系统服务器、第二终端和第二验证装置，第一终端包括第一发送模块和第一通知模块，电子签名
20 装置包括保存模块、第一生成模块、第二生成模块、调整模块、第二发送模块和输出模块，后台系统服务器包括预处理模块，第一验证装置包括第二通知模块，第二终端包括获取模块和第三通知模块，第二验证装置包括触发模块，其中：第一终端中的第一发送模块，用于在检测到用户的操作请求后，向电子签名装置发送用户的操作请求信息；电子签名装置中的保存模块，用于在获取到第一终端输出的操作请求信息后，保存操作请求信息；电子
25 签名装置中的第一生成模块，与保存模块相连，用于根据本地预先保存的密码生成策略生成联合密码；电子签名装置中的第二生成模块，与第一生成模块相连，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；电子签名装置中的调整模块，用于与第一生成模块相连，用于根据预先存储的联合密码的调整策略，对联合密码的内容进行调整，将调整后的联合密码作为第一处理密码；电子签名装置中的第二发送模块，与第二生成模块和调整模块相连，用于将第一处理密码和签名报文一起发送给第一终端；第一终端
30 中的第一通知模块，与第二发送模块相连，用于在接收到签名报文和第一处理密码后，通

知第一验证装置根据第一处理密码和操作请求信息对签名报文进行验证；第一验证装置中的第二通知模块，与第一通知模块相连，用于如果验证通过，则通知后台系统服务器预处理操作请求信息；后台系统服务器中的预处理模块，与第二通知模块相连，用于根据预先设置的预处理策略，对操作请求信息进行预处理，得到预处理信息；电子签名装置中的输出模块，用于输出联合密码的提示信息；第二终端中的获取模块，与输出模块相连，用于获取提示信息对应的联合密码，并将获取到的联合密码作为待验证密码；第二终端中的第三通知模块，与获取模块相连，用于通知第二验证装置对待验证密码进行验证；第二验证装置中的触发模块，与第三通知模块相连，用于如果验证通过，则触发后台系统服务器根据预处理信息响应操作请求信息的流程。

- 10 此外，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：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，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，用于获取联合密码的内容调整策略；第二处理单元，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，将调整后的联合密码作为第二处理密码；生成子模块，用于对如下任一组合进行签名，生成签名报文，其中组合包括：调整后的操作请求信息和联合密码；操作请求信息和第二处理密码；调整后的操作请求信息和第二处理密码。

- 15 此外，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，通知终端第二处理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所使用的内容调整策略以及第二处理密码所使用的内容调整策略。

- 20 此外，第一终端还包括：第四通知模块，与第一通知模块相连，用于通知第一验证装置调整后的操作请求信息所使用的内容调整策略；或者，通知第一验证装置第二处理密码所使用的内容调整策略，或者，通知第一验证装置调整后的操作请求信息所使用的内容调整策略以及第二处理密码所使用的内容调整策略。

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的步骤，包括：

- 30 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。

此外，调整模块通过以下任一方式得到第一处理密码和/或第二处理子模块通过以下任一

一方式得到第二处理密码：

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第一处理密码和/或第二处理密码输出；

5 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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理密码所使用的随机数和随机数组合策略；

10 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，获取调整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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理密码所使用的随机数和随机数组合策略；

15 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，

20 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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理密码所使用的随机数和随机数组合策略。

此外，输出模块还包括：认证单元，用于按照预先设置的身份认证策略，对请求输出

25 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。

此外，获取模块是通过如下任一方式得到的待验证密码：对第二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；如果电子签名装置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；通过以非接触通讯方式与电子签名装置建立通信连接，并通过通信连接获取电子签名装置

30 发送的联合密码，将接收到联合密码作为待验证密码。

此外，第一验证装置和第二验证装置中的至少一个内置于终端或后台系统服务器。

此外，电子签名装置为具有签名功能的智能卡或电子签名设备。

由上述本发明提供的技术方案可以看出，本发明提供的信息处理方法和系统，通过第二终端获取联合密码以完成交易，可以令联合密码以明文的形式进行传输，并且保证了即便明文传输联合密码，也不会造成用户本身账户信息的泄露，保证了用户账户信息的安全，
5 提高了交易的安全性；同时，根据操作请求信息和联合密码进行签名，保证了交易不可抵赖，提高了交易的安全性；

另外，通过对操作请求信息进行预处理，保证用户无法反悔或撤销此次操作请求信息，并在联合密码验证通过后，再执行该操作请求信息，以保证与用户交互一方的安全；由于是在联合密码验证通过后才最终执行该操作请求信息，保证了用户的安全。尤其是在网络
10 交易系统，通过预处理将用户部分款项冻结，在确认交易后，将该冻结款项支付给卖家，以保证卖家的安全；并且，只有在确认交易时，买家输入了正确的联合密码后，才能将冻结款项支付给卖家，以保证买家资金的安全，同时，在确认交易时买家输入的联合密码不正确时，不将货物提供给买家，从而保证卖家的安全；由此，本发明通过将网购的下单操作与完成交易（收货）时确认交易的操作在两个不同的终端上完成，保证了网络交易的安全。
15 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。
20 图。

图 1 为本发明提供的信息处理方法实施例的流程示意图；

图 2 为本发明提供的信息处理系统实施例的结构示意图。

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。
25

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
30

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，可以根据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。

10 图 1 为本发明提供的信息处理方法实施例的流程示意图。图 1 所示方法实施例包括：

步骤 101、第一终端在检测到用户的操作请求后，向电子签名装置发送用户的操作请求信息；

步骤 102、电子签名装置在获取到第一终端输出的操作请求信息后，保存操作请求信息；

15 步骤 103、电子签名装置根据本地预先保存的密码生成策略生成联合密码；

步骤 104、在得到联合密码后，电子签名装置根据操作请求信息和联合密码生成签名报文；

步骤 105、电子签名装置根据预先存储的联合密码的调整策略，对联合密码的内容进行调整，将调整后的联合密码作为第一处理密码；

20 步骤 106、电子签名装置将第一处理密码和签名报文一起发送给第一终端；

步骤 107、第一终端在接收到签名报文和第一处理密码后，通知第一验证装置根据第一处理密码和操作请求信息对签名报文进行验证；

步骤 108、如果验证通过，则第一验证装置通知后台系统服务器预处理操作请求信息；

25 步骤 109、后台系统服务器根据预先设置的预处理策略对操作请求信息进行预处理，得到预处理信息；

步骤 110、电子签名装置输出联合密码的提示信息；

步骤 111、第二终端获取提示信息对应的联合密码，并将获取到的联合密码作为待验证密码；

步骤 112、第二终端通知第二验证装置对待验证密码进行验证；

30 步骤 113、如果验证通过，则第二验证装置触发后台系统服务器根据预处理信息响应

操作请求信息的流程。

与现有技术相比，本发明提供的方法实施例，通过第二终端获取联合密码以完成交易，可以令联合密码以明文的形式进行传输，并且保证了即便明文传输联合密码，也不会造成用户本身账户信息的泄露，保证了用户账户信息的安全，提高了交易的安全性；同时，根据操作请求信息和联合密码进行签名，保证了交易不可抵赖，提高了交易的安全性。

下面对本发明提供的方法实施例作进一步说明：

步骤 A01、第一终端在检测到用户的操作请求后，向电子签名装置发送用户的操作请求信息；

10 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。

第一终端可以为：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。

其中，该电子签名装置可以为具有电子签名功能的智能卡或电子签名设备，如 USBkey、二代 UKEY、二代 U 盾等。其中，该智能卡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。

其中，第一终端可通过手工输入、网络等方式检测到用户的操作请求，再通过非接触方式发送给电子签名装置，当然，智能卡也可以通过接触方式接入第一终端，例如通过 USB 接口或音频接口接入。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。

20 步骤 A02：电子签名装置在获取到第一终端输出的操作请求信息后，保存操作请求信息；

步骤 A03、电子签名装置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。

具体的，智能卡可以采用生成随机数的方法生成联合密码，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。

当然，智能卡还可以随机生成数字、字母或者符号等，并任意组合成联合密码。

5 智能卡还可以将联合密码转换为条形码或者二维码，以方便后续获取。

本发明的联合密码是在智能卡一侧生成并上传至服务器，也不同于现有的 OTP 需要服务器和终端同时生成，本发明的单侧生成联合密码并进行签名，以保证联合密码传输的安全性和联合密码验证的准确性。

10 步骤 A04、在得到联合密码后，电子签名装置根据操作请求信息和联合密码生成签名报文；

在实际应用中，可以不对操作请求信息和联合密码都进行处理，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：

根据操作请求信息和联合密码信息生成签名报文的步骤，包括：

15 电子签名装置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，电子签名装置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，将调整后的联合密码作为第二处理密码；

电子签名装置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；

20 组合二为操作请求信息和第二处理密码；

组合三为调整后的操作请求信息和第二处理密码。

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：

25 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。

30 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，以及终端与电子签名装置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。

其中第二处理密码的生成方式与第一处理密码的生成方式在下文进行说明。

需要说明的是，生成签名报文时所使用的策略以及生成第一处理密码时所使用的策略可以是第一终端和电子签名装置预先协商的，从而减少第一终端和电子签名装置之间信息的交互次数；

如果第一终端和电子签名装置未预先协商上述策略，则第一终端通知第一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，通知第一终端组合二中第二处理密码所使用的内容调整策略，或者，通知第一终端组合三中调整后的操作请求信息所使用的内容调整策略以及第二处理密码所使用的内容调整策略。

在实际应用中，每次可以使用不同的策略，通过向第一终端通知内容调整策略，可以保证第一终端能够获知本次使用的策略，触发对签名报文的验证流程，且由于使用的策略随机性高，降低了策略被破解的风险。

步骤 A05、电子签名装置根据预先存储的联合密码的调整策略，对联合密码的内容进行调整，将调整后的联合密码作为第一处理密码；

针对于步骤 A04 和步骤 A05 中的第一处理密码和/或第二处理密码是通过以下任一方式得到的，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第一处理密码和/或第二处理密码输出；

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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理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，获取调整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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理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；

5 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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理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。

10

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。

15 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。

20 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，

25 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。

30 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。

其中第一处理密码和第二处理密码所采用的策略可以是相同的，也可以是不同的。优选采用不同的策略，如果采用不同的策略，即使破解了其中一个密码，但是由于不知道另一个密码的调整策略，也不会轻易得到另一个密码，提高了密码的安全系数。

5 步骤 A06、电子签名装置将第一处理密码和签名报文一起发送给第一终端；

步骤 A07、第一终端在接收到签名报文和第一处理密码后，通知第一验证装置根据第一处理密码和操作请求信息对签名报文进行验证；

需要说明的是，第一验证装置可以为除了第一终端和后台系统服务器之外的第三方设备，也可以是内置于第一终端或后台系统服务器中的软件模块。前者可以降低后台系统服务器和第一终端的处理压力，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10 本低。

其中，第一终端通知第一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：第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15 报文进行验证；

方式二：第一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待验证密码和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，如在第一终端处理能力较强时，可以采用20 方式一，在处理能力有限或者验证操作过多时，采用方式二，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，第一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25 时，方法还包括：

第一终端从电子签名装置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，第一终端从电子签名装置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；

30 第一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第一验证装置。

其中，第一验证装置验证签名报文的流程与电子签名装置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，
5 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。

10 对于后者，第一验证装置在采用方式二对签名报文进行验证时，如果第一终端、电子签名装置以及第一验证装置三者预先协商好了内容调整策略，则使用协商好的内容调整策略进行验证；

如果第一验证装置与第一终端未协商好，则第一终端从电子签名装置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，第一终端从电子签名装置获取操作请求信息的内容调整策略，其中
15 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；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第一验证装置。

步骤 A08、如果验证通过，则第一验证装置通知后台系统服务器预处理操作请求信息；

20 步骤 A09、根据预先设置的预处理策略，后台系统服务器对操作请求信息进行预处理，得到预处理信息；

具体的，通过对操作请求信息进行预处理，可以保证发起该操作请求信息的用户不能反悔，同时也能给予与该用户交互的另一方一定的安全保证。

例如，在金融交易系统，后台系统服务器验证签名报文通过后，根据用户操作请求中的
25 的款项内容冻结该电子签名装置对应的账户中与交易报文中的款项对应的金额，通过冻结款项，保证买家无法使用冻结的款项，从而保证交易确认后，将该冻结款项支付给卖家，以保证卖家的安全，此处的预处理方式可以是银行直接冻结款项，也可以是将款项转账给第三方机构暂存。

步骤 A10、电子签名装置输出联合密码的提示信息；

30 其中，该电子签名装置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，又或者“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，电子签名装

5 置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 A11、第二终端获取提示信息对应的联合密码，并将获取到的联合密码作为待验
10 证密码；

具体的，第二终端与第一终端是不同的设备，但是第二终端与第一终端均可以为 POS 机、移动终端、平板电脑、PC 机等设备。第二终端可以采用如下方式获取联合密码：第二终端接收通过按键输入的信息获取联合密码，例如通过从 POS 机的键盘输入联合密码获得联合密码；或第二终端通过扫描智能卡显示的信息获取联合密码，例如 POS 机扫描智能卡
15 显示的二维码或者条形码等获取该联合密码；或第二终端通过短距离无线通讯方式从智能卡获取联合密码，例如可以通过将智能卡放置在第二终端的扫描范围内，以 NFC 等方式获取联合密码。

当然，在用户需要代收货时，可以将联合密码告知第三人，以便第三人确认交易。

由此可见，通过联合密码的形式，可以令联合密码明文传输，即便明文传输联合密码，
20 也不会造成用户本身账户信息的泄露，保证了用户账户信息的安全，提高了交易的安全性。

通过将网购的下单操作与收货时确认交易的操作在两个不同的终端上完成，保证了买卖双方的安全以及资金的安全。

步骤 A12、第二终端通知第二验证装置对待验证密码进行验证；

同理，第二验证装置可以为除了第二终端和后台系统服务器之外的第三方设备，也可以
25 是内置于第二终端或后台系统服务器中的软件模块。前者可以降低后台系统服务器和第二终端的处理压力，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。

步骤 A13、如果验证通过，则第二验证装置触发后台系统服务器根据预处理信息响应操作请求信息的流程。

简单来说，将之前未处理完的操作请求信息执行完成。例如，解冻款项并执行交易，
30 其中，后台系统服务器验证第二终端发送的联合密码是否与第一终端发送的联合密码的相关信息一致，以保证买家身份的真实性。

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
5 为非银行系统的服务器，比如网络交易系统中暂存金额的服务器，如淘宝网对应的支付宝系统中暂存用户存款的服务器。终端可以为 PC 机和移动终端等。

具有电子签名功能的智能卡接入第一终端，接收交易报文；

智能卡生成联合密码，并至少根据联合密码生成加密联合密码；

智能卡根据交易报文和加密联合密码生成签名报文；

10 智能卡将签名报文和加密联合密码发送至第一终端；

第一终端至少将交易报文、签名报文和加密联合密码发送至后台系统服务器；

后台系统服务器验证签名报文，并在验证通过后，根据交易报文冻结款项或者将交易
报文对应的款项发送至第三方服务器；

确认交易时，智能卡显示联合密码，第二终端获取联合密码并将联合密码发送至后台
15 系统服务器；

后台系统服务器验证联合密码，并在验证通过后，解冻款项并执行交易或发送交易指令至第三方服务器并由第三方服务器执行交易。

本发明提供的应用实例，通过第二终端获取联合密码以完成交易，可以令联合密码以明文的形式进行传输，并且保证了即便明文传输联合密码，也不会造成用户本身账户信息的泄露，保证了用户账户信息的安全，提高了交易的安全性；同时，通过对交易报文和加密联合密码进行签名，保证了交易不可抵赖，提高了交易的安全性；另外，通过对款项进行冻结，保证买家无法使用冻结的款项，从而在确认交易后，将该冻结款项支付给卖家，以保证卖家的安全；并且，只有在确认交易时，买家输入了正确的联合密码后，才能将冻结款项支付给卖家，以保证买家资金的安全，同时，在确认交易时买家输入的联合密码不
20 正确时，不将货物提供给买家，从而保证卖家的安全；由此，本发明通过将网购的下单操作与完成交易（收货）时确认交易的操作在两个不同的终端上完成，保证了网络交易的安全。

图 2 为本发明提供的信息处理系统实施例的结构示意图。图 2 所示系统包括电子签名装置 201、第一终端 202、第一验证装置 203、后台系统服务器 204、第二终端 205 和第二
30 验证装置 206，其中：

第一终端 202 中的第一发送模块，用于在检测到用户的操作请求后，向电子签名装置

发送用户的操作请求信息；

电子签名装置 201 中的保存模块，用于在获取到第一终端输出的操作请求信息后，保存操作请求信息；

电子签名装置 201 中的第一生成模块，与保存模块相连，用于根据本地预先保存的密码生成策略生成联合密码；

电子签名装置 201 中的第二生成模块，与第一生成模块相连，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；

电子签名装置 201 中的调整模块，用于与第一生成模块相连，用于根据预先存储的联合密码的调整策略，对联合密码的内容进行调整，将调整后的联合密码作为第一处理密码；

电子签名装置 201 中的第二发送模块，与第二生成模块和调整模块相连，用于将第一处理密码和签名报文一起发送给第一终端；

第一终端 202 中的第一通知模块，与第二发送模块相连，用于在接收到签名报文和第一处理密码后，通知第一验证装置 203 根据第一处理密码和操作请求信息对签名报文进行验证；

第一验证装置 203 中的第二通知模块，与第一通知模块相连，用于如果验证通过，则通知后台系统服务器预处理操作请求信息；

后台系统服务器 204 中的预处理模块，与第二通知模块相连，用于根据预先设置的预处理策略，对操作请求信息进行预处理，得到预处理信息；

电子签名装置 201 中的输出模块，用于输出联合密码的提示信息；

第二终端 205 中的获取模块，用于获取提示信息对应的联合密码，并将获取到的联合密码作为待验证密码；

第二终端 205 中的第三通知模块，与获取模块相连，用于通知第二验证装置对待验证密码进行验证；

第二验证装置 206 中的触发模块，与第三通知模块相连，用于如果验证通过，则触发后台系统服务器 204 根据预处理信息响应操作请求信息的流程。

其中，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：

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，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，用于获取联合密码的内容调整策略；

第二处理单元，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，将调整后的联合密码作为第二处理密码；

5 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第二处理密码；

组合三为调整后的操作请求信息和第二处理密码。

其中，第二生成模块还包括：

10 通知子模块，用于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，通知终端组合二中第二处理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所使用的内容调整策略以及第二处理密码所使用的内容调整策略。

其中，第一终端还包括：

15 第四通知模块，与第一通知模块相连，用于通知第一验证装置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，通知第一验证装置组合二中第二处理密码所使用的内容调整策略，或者，通知第一验证装置组合三中调整后的操作请求信息所使用的内容调整策略以及第二处理密码所使用的内容调整策略。

其中，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的步骤，包括：

20 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，调整模块通过如下任一方式得到第一处理密码和/或第二处理子模块通过如下任一方式得到第二处理密码，包括：

25 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第一处理密码和/或第二处理密码输出；

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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第

30

二处理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，获取调整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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理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第一处理密码和/或第二处理密码输出，并向第一终端通知第一处理密码和/或第二处理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，获取模块是通过如下任一方式得到的待验证密码，包括：

方式一：对第二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：如果电子签名装置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电子签名装置建立通信连接，并通过通信连接获取电子签名装置发送的联合密码，将接收到联合密码作为待验证密码。

其中，第一验证装置和第二验证装置中的至少一个内置于终端或后台系统服务器。

其中，电子签名装置为具有签名功能的智能卡或电子签名设备。

与现有技术相比，本发明提供的系统实施例，通过第二终端获取联合密码以完成交易，可以令联合密码以明文的形式进行传输，并且保证了即便明文传输联合密码，也不会造成用户本身账户信息的泄露，保证了用户账户信息的安全，提高了交易的安全性；同时，根

据操作请求信息和联合密码进行签名，保证了交易不可抵赖，提高了交易的安全性。

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

5 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

10 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

15 过程序来指令相关的硬件完成，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。集成的模块如果以软件

20 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

25 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。

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

30 附权利要求及其等同限定。

权利要求书

1、一种信息处理方法，其特征在于，所述方法包括：

第一终端在检测到用户的操作请求后，向所述电子签名装置发送所述用户的操作请求
5 信息；

电子签名装置在获取到第一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，以及，根据预先存储的联合密码的调整策略，对
联合密码的内容进行调整，将调整后的联合密码作为第一处理密码，并将所述第一处理密
10 码和所述签名报文一起发送给第一终端；

所述第一终端在接收到所述签名报文和第一处理密码后，通知第一验证装置根据所述
第一处理密码和所述操作请求信息对所述签名报文进行验证；

如果验证通过，则所述第一验证装置通知后台系统服务器预处理所述操作请求信息；

后台系统服务器根据预先设置的预处理策略对所述操作请求信息进行预处理，得到预
15 处理信息；

所述电子签名装置输出所述联合密码的提示信息；

第二终端获取所述提示信息对应的联合密码，并将获取到的联合密码作为待验证密码；

第二终端通知第二验证装置对所述待验证密码进行验证；

如果验证通过，则所述第二验证装置触发所述后台系统服务器根据所述预处理信息响
20 应所述操作请求信息的流程。

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，包括：

所述电子签名装置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，
25 所述电子签名装置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，
对所述联合密码的内容进行调整，将调整后的联合密码作为第二处理密码；

所述电子签名装置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第二处理密码；

调整后的操作请求信息和第二处理密码。

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：

通知所述第一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

通知所述第一终端所述第二处理密码所使用的内容调整策略；或者

5 通知所述第一终端所述调整后的操作请求信息所使用的内容调整策略以及所述第二处理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，所述第一终端通知所述第一验证装置根据所述第一处理密码和所述操作请求信息对所述签名报文进行验证，还包括：

10 所述第一终端通知所述第一验证装置所述调整后的操作请求信息所使用的内容调整策略；或者

所述第一终端通知所述第一验证装置所述第二处理密码所使用的内容调整策略；或者

所述第一终端通知所述第一验证装置所述调整后的操作请求信息所使用的内容调整策略以及所述第二处理密码所使用的内容调整策略。

15 5、根据权利要求 2 至 4 中任一项所述的方法，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。

20 6、根据权利要求 2 至 4 中任一项所述的方法，其特征在于，所述第一处理密码和/或所述第二处理密码是通过以下任一方式得到的，包括：

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第一处理密码和/或所述第二处理密码输出；

25 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第一处理密码和/或所述第二处理密码输出，并向第一终端通知所述第一处理密码

和/或所述第二处理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第一处理密码和/或所述第二处理密码输出，并向所述第一终端通知第一处理密码和/或所述第二处理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所述第一处理密码和/或所述第二处理密码输出，并向所述第一终端通知所述第一处理密码和/或所述第二处理密码所使用的随机数和随机数组合策略。

7、根据权利要求 1 至 6 中任一项所述的方法，其特征在于，所述电子签名装置输出联合密码提示信息之前还包括：

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。

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

对所述第二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；

如果所述电子签名装置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电子签名装置建立通信连接，并通过所述通信连接获取所述电子签名装置发送的联合密码，将接收到联合密码作为待验证密码。

9、一种信息处理系统，其特征在于，所述系统包括第一终端、电子签名装置、第一验

证装置、后台系统服务器、第二终端和第二验证装置，所述第一终端包括第一发送模块和第一通知模块，所述电子签名装置包括保存模块、第一生成模块、第二生成模块、调整模块、第二发送模块和输出模块，所述后台系统服务器包括预处理模块，所述第一验证装置包括第二通知模块，所述第二终端包括获取模块和第三通知模块，所述第二验证装置包括

5 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，向所述电子签名装置发送所述用户的操作请求信息；

所述保存模块，用于在获取到第一终端输出的操作请求信息后，保存所述操作请求信息；

10 所述第一生成模块，与所述保存模块相连，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，与所述第一生成模块相连，用于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；

15 所述调整模块，用于与所述第一生成模块相连，用于根据预先存储的联合密码的调整策略，对联合密码的内容进行调整，将调整后的联合密码作为第一处理密码；

所述第二发送模块，与所述第二生成模块和所述调整模块相连，用于将所述第一处理密码和所述签名报文一起发送给第一终端；

20 所述第一通知模块，与所述第二发送模块相连，用于在接收到所述签名报文和第一处理密码后，通知第一验证装置根据所述第一处理密码和所述操作请求信息对所述签名报文进行验证；

所述第二通知模块，与所述第一通知模块相连，用于如果验证通过，则通知后台系统服务器预处理所述操作请求信息；

所述预处理模块，与所述第二通知模块相连，用于根据预先设置的预处理策略，对所述操作请求信息进行预处理，得到预处理信息；

25 所述输出模块，用于输出所述联合密码的提示信息；

所述获取模块，用于获取所述提示信息对应的联合密码，并将获取到的联合密码作为待验证密码；

所述第三通知模块，与所述获取模块相连，用于通知第二验证装置对所述待验证密码进行验证；

30 所述触发模块，与所述第三通知模块相连，用于如果验证通过，则触发所述后台系统

服务器根据所述预处理信息响应所述操作请求信息的流程。

10、根据权利要求 9 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：

5 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，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；

10 第二处理单元，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，将调整后的联合密码作为第二处理密码；

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第二处理密码；

15 调整后的操作请求信息和第二处理密码。

11、根据权利要求 10 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，通知所述终端所述第二处理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所使用的内容调整策略以及所述第二处理密码所使用的内容调整策略。

20 12、根据权利要求 10 或 11 所述的系统，其特征在于，所述第一终端还包括：

第四通知模块，与所述第一通知模块相连，用于通知所述第一验证装置所述调整后的操作请求信息所使用的内容调整策略；或者，通知所述第一验证装置所述第二处理密码所使用的内容调整策略，或者，通知所述第一验证装置所述调整后的操作请求信息所使用的内容调整策略以及所述第二处理密码所使用的内容调整策略。

25 13、根据权利要求 9 至 12 中任一项所述的系统，其特征在于，所述第一处理子模块用于：

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。

14、根据权利要求 10 至 12 中任一项所述的系统，其特征在于，所述调整模块通过以下任一方式得到所述第一处理密码和/或所述第二处理子模块通过以下任一方式得到所述第二处理密码：

5 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第一处理密码和/或所述第二处理密码输出；

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；
10 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第一处理密码和/或所述第二处理密码输出，并向第一终端通知所述第一处理密码和/或所述第二处理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，获取调整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第一处理密码和/或所述第二处理密码输出，并向所述第一终端通知第一处理密码和/或所述第二处理密码所使用的随机数和随机数组合策略；
15

20 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所述第一处理密码和/或所述第二处理密码输出，并向所述第一终端通知所述第一处理密码和/或所述第二处理密码所使用的随机数和随机数组合策略。
25

15、根据权利要求 9 至 14 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；
30

输出单元，用于如果认证成功，则输出联合密码。

16、根据权利要求 9 至 15 中任一项所述的系统，其特征在于，所述获取模块是通过如下任一方式得到的所述待验证密码：

5 对所述第二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；

如果所述电子签名装置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电子签名装置建立通信连接，并通过所述通信连接获取所述电子签名装置发送的联合密码，将接收到联合密码作为待验证密码。

10 17、根据权利要求 9 至 16 中任一项所述的系统，其特征在于，所述第一验证装置和第二验证装置中的至少一个内置于所述终端或后台系统服务器。

18、根据权利要求 9 至 17 中任一项所述的系统，其特征在于，所述电子签名装置为具有签名功能的智能卡或电子签名设备。

15