

身份认证、号码保存和发送、绑定号码方法、装置及设备

技术领域

[01] 本说明书涉及互联网金融技术领域，尤其是涉及一种身份认证、号码保存和发送、绑定号码方法、装置及设备。

5 背景技术

[02] 随着互联网金融技术的发展和运用，越来越多的用户在购物时选择使用快捷支付，提高了用户的支付体验。为实现快捷支付，可以将用户的银行卡或银行账户预先绑定在电子钱包或线上商户的收银台服务器上，这样用户在购买商品进行支付时，便不需要登录网银，不需要银行做任何验证，使得线上支付极简、快速化。通常，在将用户的银行卡或银行账户绑定在电子钱包或线上商户的收银台服务器时，需要对用户自己进行身份验证，以验证操作人是银行卡或银行账户的合法持有人。

[03] 对用户的身份验证，可以采用多种方式。但是，目前在海外一些没有中央统一身份验证体系的国家，以及用户手机号经常换号不做实名登记的国家，或者其他类似场景中，身份验证方式受限，比如，在上述这些场景中，可能无法采用常用的人脸识别和短信验证码等身份认证方法。以前述的海外市场的场景为例，较多采用的是将信用卡的卡号和有效期保存在电子钱包或线上商户的收银台，利用 3DS (3 Domain Security) 进行身份认证的方式，尽管这种方式也能实现身份认证并完成快捷支付。然而，由于这种身份认证方式通过收单行，卡组织，发卡行这一支付路径每个环节都收费，因此利用这种身份认证方式成本比较高。再者，3DS 的安全校验常常会被黑产通过欺诈等手段骗到用户的安全校验码，使用户资金受损，因此利用这种身份认证方式安全性不强。此外，这种身份认证方式涉及的中间环节比较多，用户进行快捷支付时比较麻烦，用户会主动放弃支付，因此利用此种身份认证方式进行支付的成功率比较低。

发明内容

[04] 本说明书实施例提供一种身份认证、号码保存和发送、绑定号码方法、装置及设备。解决或改善了现有技术中采用 3DS 身份认证方式导致的成本比较高，安全性不强以及支付成功率比较低等问题。

[05] 为解决上述技术问题，本说明书实施例是这样实现的：

- [06]本说明书实施例提供的一种身份认证方法，该方法包括：
- [07]接收数据认证平台客户端发送的用户身份认证请求，其中，所述用户身份认证请求包括用户认证信息和用户标识信息，所述数据认证平台服务器预先存储有用用户认证信息和与该用户标识信息对应的注册号码及密令；
- 5 [08]根据所述用户标识信息获取数据认证平台服务器中预先存储的用户认证信息；
- [09]将接收的用户身份认证请求中的用户认证信息与获取的数据认证平台服务器中预先存储的用户认证信息进行匹配；
- [10]在匹配成功的情况下，接收数据认证平台客户端发送的所述用户对获取注册号码进行确认的结果；
- 10 [11]根据接收的确认结果，获取所述用户的注册号码及对应的密令；
- [12]将获取的所述用户的注册号码及对应的密令发送到第三方机构服务器。
- [13]本说明书实施例提供的一种号码保存和发送方法，该方法包括：
- [14]接收数据认证平台服务器发送的用户的注册号码及对应的密令；
- [15]将接收的所述用户的注册号码对应的密令与预先存储的数据认证平台服务器批量发
- 15 送的密令进行匹配；其中，所述批量发送的密令与预先存储的用户标识信息相关联；
- [16]在匹配成功的情况下，保存接收的所述用户的注册号码；其中，保存的用户的注册号码与预先存储的该用户的用户标识信息相关联；
- [17]接收第三方机构客户端发送的用户绑定号码请求，其中，所述用户绑定号码请求包括用户认证信息和用户标识信息；
- 20 [18]根据所述用户标识信息获取第三方机构服务器中预先存储的用户认证信息；
- [19]将接收的用户绑定号码请求中的用户认证信息与获取的第三方机构服务器中预先存储的用户认证信息进行匹配；
- [20]在匹配成功的情况下，根据用户标识信息，获取该用户的注册号码；
- [21]将获取的用户的注册号码发送到第三方机构客户端。
- 25 [22]本说明书实施例提供的一种绑定号码方法，该方法包括：
- [23]接收用户绑定号码请求并将所述用户绑定号码请求发送到第三方机构服务器；其中，所述用户绑定号码请求包括用户认证信息和用户标识信息；

[24]在第三方机构服务器匹配用户认证信息成功的情况下，接收第三方机构服务器发送的用户的注册号码；

[25]获取所述用户对确定绑定号码按钮进行确认的结果，绑定号码成功。

[26]本说明书实施例提供的一种身份认证装置，该装置包括：

5 [27]请求接收模块、信息获取模块、信息匹配模块、结果接收模块、号码及密令获取模块和号码及密令发送模块；

[28]所述请求接收模块，用于接收数据认证平台客户端发送的用户身份认证请求，其中，所述用户身份认证请求包括用户认证信息和用户标识信息，所述数据认证平台服务器预先存储有用户认证信息和与该用户标识信息对应的注册号码及密令；

10 [29]所述信息获取模块，用于根据所述用户标识信息获取数据认证平台服务器中预先存储的用户认证信息；

[30]所述信息匹配模块，用于将获取的用户身份认证请求中的用户认证信息与获取的数据认证平台服务器中预先存储的用户认证信息进行匹配；

15 [31]所述结果接收模块，用于在匹配成功的情况下，接收数据认证平台客户端发送的所述用户对获取注册号码进行确认的结果；

[32]所述号码及密令获取模块，用于根据接收的确认结果，获取所述用户的注册号码及对应的密令；

[33]所述号码及密令发送模块，用于将获取的所述用户的注册号码及对应的密令发送到第三方机构服务器。

20 [34]本说明书实施例提供的一种号码保存和发送装置，该装置包括：

[35]号码及密令接收模块、密令匹配模块、号码保存模块、请求接收模块、信息获取模块、信息匹配模块、号码获取模块和号码发送模块；

[36]所述号码及密令接收模块，用于接收数据认证平台服务器发送的用户的注册号码及对应的密令；

25 [37]所述密令匹配模块，用于将接收的所述用户的注册号码对应的密令与预先存储的数据认证平台服务器批量发送的密令进行匹配；其中，所述批量发送的密令与预先存储的用户标识信息相关联；

- [38]所述号码保存模块,用于在匹配成功的情况下,保存接收的所述用户的注册号码;
其中,保存的用户的注册号码与预先存储的该用户的用户标识信息相关联;
- [39]所述请求接收模块,用于接收第三方机构客户端发送的用户绑定号码请求,其中,
所述用户绑定号码请求包括用户认证信息和用户标识信息;
- 5 [40]所述信息获取模块,用于根据所述用户标识信息获取第三方机构服务器中预先存储
的用户认证信息;
- [41]所述信息匹配模块,用于将接收的用户绑定号码请求中的用户认证信息与获取的第
三方机构服务器中预先存储的用户认证信息进行匹配;
- [42]所述号码获取模块,用于在匹配成功的情况下,根据用户标识信息,获取该用户的
10 注册号码;
- [43]所述号码发送模块,用于将获取的用户的注册号码发送到第三方机构客户端。
- [44]本说明书实施例提供的一种绑定号码装置,该装置包括:
- [45]请求接收模块、请求发送模块、号码接收模块和结果接收模块;
- [46]所述请求接收模块,用于接收用户绑定号码请求;
- 15 [47]所述请求发送模块,用于将所述用户绑定号码请求发送到第三方机构服务器;其中,
所述用户绑定号码请求包括用户认证信息和用户标识信息;
- [48]所述号码接收模块,用于在第三方机构服务器匹配用户认证信息成功的情况下,接
收第三方机构服务器发送的用户的注册号码;
- [49]所述结果接收模块,用于接收所述用户对确定绑定号码进行确认的结果,绑定号码
20 成功。
- [50]本说明书实施例提供的一种身份认证设备,包括:存储器以及处理器,所述存储器
存储程序,并且被配置成由所述处理器执行上述身份认证方法。
- [51]本说明书实施例提供的一种号码保存和发送设备,包括:存储器以及处理器,所述
存储器存储程序,并且被配置成由所述处理器执行上述号码保存和发送方法。
- 25 [52]本说明书实施例提供的一种绑定号码设备,包括:存储器以及处理器,所述存储器
存储程序,并且被配置成由所述处理器执行上述绑定号码方法。
- [53]本说明书实施例提供的一种用于身份认证、号码保存和发送及绑定号码的系统,所

述系统包括上述的身份认证装置、号码保存和发送装置及绑定号码装置。

- [54]本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果：数据认证平台和第三方机构直连，不需要参与卡组织的 3DS 体系，中间交易环节不需要收费，交易成本低；中间交易环节少，交易路径短，安全性强，支付成功率高；解决了在无中央统一身份认证体系国家快捷绑卡进行身份认证的痛点。

附图说明

- [55]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术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说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

- [56]图 1 为本说明书实施例提供一种身份认证方法的流程示意图；
- [57]图 2 为本说明书实施例提供一种号码保存和发送方法的流程示意图；
- [58]图 3 为本说明书实施例提供一种绑定号码方法的流程示意图；
- [59]图 4 为本说明书实施例提供一种身份认证装置的结构示意图；
- [60]图 5 为本说明书实施例提供一种号码保存和发送装置的结构示意图；
- [61]图 6 为本说明书实施例提供一种绑定号码装置的结构示意图；
- [62]图 7 为本说明书实施例提供一种用于身份认证、号码保存和发送及绑定号码的系统的结构示意图。

具体实施方式

- [63]本说明书实施例提供一种身份认证、号码保存和发送、绑定号码方法、装置及设备。
- [64]为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书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申请一部分实施例，而不是全部的实施例。基于本说明书实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。
- [65]在海外一些没有中央统一身份认证体系的国家，以及用户手机号经常换号不做实名登

记的国家，无法采用国内常用的人脸识别和短信验证码等身份认证方法。该方案为了解决上述身份认证及绑卡的痛点，充分利用银行具有可信身份认证能力的渠道，例如银行网点、ATM、网银、手机银行等，把从第三方机构的绑卡操作变成反向从具有可信身份认证能力的银行渠道做激活操作。

- 5 [66]在本说明书以下实施例中，数据认证平台以快捷支付合作银行为例，第三方机构以支付宝为例，注册号码为银行卡号和/或银行账号。

[67]快捷支付合作银行侧实施例：

[68]图1为本说明书实施例提供的一种身份认证方法的流程示意图，该流程示意图包括：

- [69]步骤105，接收数据认证平台客户端发送的用户身份认证请求，其中，所述用户身份
10 份认证请求包括用户认证信息和用户标识信息，所述数据认证平台服务器预先存储有用户认证信息和与该用户标识信息对应的注册号码及密令；

[70]在本说明书实施例中，用户是快捷支付合作银行的客户，还是第三方机构的客户。

- [71]在本说明书实施例中，以利用招商银行的手机银行进行身份认证为例。用户张三登
录招商银行手机银行，发起了身份认证请求。上述身份认证请求包括张三登录手机银行
15 的用户认证信息和用户标识信息，且用户标识信息包括：身份证号码、手机号码、银行卡号或银行账号，用户认证信息包括密码和/或验证码。

[72]在本说明书实施例中，招商银行手机银行客户端获取到用户认证信息和用户标识信息后，将用户认证信息和用户标识信息发送到招商银行服务器。

- [73]作为一种可选地实施方式，在本说明书实施例中，上述用户张三是在数据认证平台
20 客户端发起用户身份认证请求之前的预注册用户。为提高利用本技术方案中的身份认证方法进行绑卡的用户数，银行为预注册用户发放红包。在本说明书实施例中，执行步骤105之前，快捷支付合作银行将一位或多位预注册用户的一个或多个银行卡号和/或银行账号生成具有唯一性的不可逆的密令，并将生成的密令批量发送到支付宝服务器。在本说明书实施例中，以招商银行将张三的银行卡号6225999878762456及
25 6225999878762457和李四的银行卡号6224890999097890生成具有唯一性的不可逆的密令，并将生成的密令发送到支付宝服务器为例。密令对于外界不可见，无论是用户或者其他人，都无法获取密令的内容。密令通过专用安全网络连接（VPN或专线），加密传输给支付宝服务器。

[74]步骤110，根据所述用户标识信息获取数据认证平台服务器中预先存储的用户认证

信息;

[75]在本说明书实施例中,根据步骤 105 获取到的张三本人的用户标识信息获取招商银行服务器中预先存储的张三的用户认证信息,如密码和/或验证码。

[76]作为一种可选地实施方式,在本说明书实施例中,快捷支付合作银行预先为每位客户分配一个与该用户标识信息对应的唯一性 ID,且每个 ID 与该客户的若干个银行卡号和/或若干个银行账号及对应的密令相关联。张三在招商银行服务器侧的 ID 为 00000000;张三的招商银行卡号为 6225999878762456 和 6225999878762457。上述 ID 和银行卡号及对应密令相关联。在步骤 105 之后,根据所述唯一性 ID 获取数据认证平台服务器中预先存储的用户认证信息。

10 [77]步骤 115,将接收的用户身份认证请求中的用户认证信息与获取的数据认证平台服务器中预先存储的用户认证信息进行匹配;

[78]在本说明书实施例中,将步骤 105 获取到的密码和/或验证码与步骤 110 中在招商银行服务器中根据张三的用户标识信息获取到的张三的用户认证信息进行匹配。

[79]步骤 120,在匹配成功的情况下,接收数据认证平台客户端发送的所述用户对获取注册号码进行确认的结果;

[80]在本说明书实施例中,在步骤 115 中的匹配操作成功的情况下,且用户点击“注册号码”按钮,数据认证平台服务器获取到用户对“注册号码”按钮进行点击的结果。

[81]步骤 125,根据接收的确认结果,获取所述用户的注册号码及对应的密令;

[82]作为一种可选地实施方式,获取所述用户的每个注册号码及对应的密令;或将获取的所述用户的每个注册号码发送到数据认证平台客户端并获取用户对注册号码进行选择的结果及获取的用户选择的注册号码对应的密令。在本说明书实施例中,以获取所述用户的每个注册号码及对应的密令为例。

[83]步骤 130,将获取的所述用户的注册号码及对应的密令发送到第三方机构服务器。

[84]在本说明书实施例中,快捷支付合作银行自动将需要在第三方机构服务器保存的预注册用户的银行卡号及对应的密令和/或银行账号及对应的密令发送到第三方机构服务器。进一步地,在本说明书实施例中,将上述张三的银行卡号 6225999878762456 及对应的密令和银行卡号 6225999878762457 及对应的密令发送到支付宝服务器。

[85]与现有技术相比,本说明书实施例采用的上述技术方案能够达到以下有益效果:银

行和支付宝直连，不需要参与卡组织的 3DS 体系，中间交易环节不需要收费，交易成本低；中间交易环节少，交易路径短，安全性强，支付成功率高；解决了在无中央统一身份认证体系国家快捷绑卡进行身份认证的痛点；预注册用户可领取红包，银行和支付宝双方都可以充分利用各自的渠道优势对此快捷支付对获客宣传，客户转化率和绑卡成功率有比较高的保障。

[86] 第三方机构服务器侧实施例：

[87] 图 2 为本说明书实施例提供的一种号码保存和发送方法的流程示意图，该流程示意图包括：

[88] 步骤 205，接收数据认证平台服务器发送的用户的注册号码及对应的密令；

10 [89] 在本说明书实施例中，招商银行服务器接收张三的银行卡号 6225999878762456 和 6225999878762457 的同时，还接收张三的两个银行卡号对应的密令。

[90] 作为一种可选地实施方式，在步骤 205 之前，招商银行服务器接收数据认证平台服务器根据一个或多个所述用户的一个或多个注册号码分别生成的密令。在本说明书实施例中，接收将张三的银行卡号 6225999878762456 和 6225999878762457 分别生成的密令
15 和将李四的银行卡号 6224890999097890 生成的密令。

[91] 步骤 210，将接收的所述用户的注册号码对应的密令与预先存储的数据认证平台服务器批量发送的密令进行匹配；其中，所述批量发送的密令与预先存储的用户标识信息相关联；

[92] 在本说明书实施例中，将步骤 205 中接收的张三的银行卡号 6225999878762456 对应的密令和银行卡号 6225999878762457 对应的密令与在支付宝服务器中预先存储的数据认证平台服务器批量发送的密令进行匹配。
20

[93] 步骤 215，在匹配成功的情况下，保存接收的所述用户的注册号码；其中，保存的用户的注册号码与预先存储的该用户的用户标识信息相关联；

[94] 在本说明书实施例中，在步骤 210 中的匹配操作成功的情况下，将接收的张三的银行卡号 6225999878762456 和 6225999878762457 保存在张三的用户标识信息下。
25

[95] 步骤 220，接收第三方机构客户端发送的用户绑定号码请求，其中，所述用户绑定号码请求包括用户认证信息和用户标识信息；

[96] 在本说明书实施例中，张三登录支付宝客户端，发起绑定号码请求。上述绑定号码

请求包括张三登录支付宝客户端的用户认证信息和用户标识信息，且用户标识信息包括：手机号码或身份证号码，用户认证信息包括密码和/或验证码。

[97] 步骤 225，根据所述用户标识信息获取第三方机构服务器中预先存储的用户认证信息；

- 5 [98] 在本说明书实施例中，根据获取的张三登录支付宝客户端的用户标识信息，如手机号码或身份证号码，获取支付宝服务器中张三注册过的用户认证信息。

[99] 作为一种可选地实施方式，在本说明书实施例中，支付宝服务器预先存储有与张三的用户标识信息对应的唯一性 ID；根据所述唯一性 ID 获取支付宝服务器中预先存储的张三的用户认证信息。

- 10 [100] 步骤 230，将接收的用户绑定号码请求中的用户认证信息与获取的第三方机构服务器中预先存储的用户认证信息进行匹配；

[101] 在本说明书实施例中，将步骤 210 中接收的绑定号码请求中的手机号码或身份证号码及密码和/或验证码与获取的支付宝服务器中预先存储的张三的手机号码或身份证号码及密码和/或验证码进行匹配。

- 15 [102] 步骤 235，在匹配成功的情况下，根据用户标识信息，获取该用户的注册号码；

[103] 在本说明书实施例中，在用户认证信息匹配成功的情况下，根据张三的用户标识信息，如手机号码或身份证号码获取张三的银行卡号为 6225999878762456 和 6225999878762457。

- 20 [104] 作为一种可选地实施方式，在本说明书实施例中，张三在支付宝服务器 ID 为 000000。根据张三的 ID 获取张三的银行卡号为 6225999878762456 和 6225999878762457。

[105] 步骤 240，将获取的用户的注册号码发送到第三方机构客户端。

[106] 在本说明书实施例中，将步骤 235 获取的张三的银行卡号 6225999878762456 和 6225999878762457 发送到支付宝客户端。

[107] 第三方机构客户端侧实施例：

- 25 [108] 图 3 为本说明书实施例提供的一种绑定号码方法的流程示意图，该流程示意图包括：

[109] 步骤 305，接收用户绑定号码请求并将所述用户绑定号码请求发送到第三方机构服务器；其中，所述用户绑定号码请求包括用户认证信息和用户标识信息；

- [110] 在本说明书实施例中，用户在支付宝客户端发起绑定号码请求。上述绑定号码请求包括用户认证信息和用户标识信息，且所述用户标识信息包括手机号码或身份证号码，所述用户认证信息包括密码和/或验证码。支付宝客户端将上述用户认证信息和用户标识信息发送到支付宝服务器。
- 5 [111] 步骤 310，在第三方机构服务器匹配用户认证信息成功的情况下，接收第三方机构服务器发送的用户的注册号码；
- [112] 作为一种可选地实施方式，接收第三方机构服务器发送的用户已选择的注册号码；或接收第三方机构服务器发送的用户的每个注册号码并获取所述用户对所述注册号码进行选择的结果。
- 10 [113] 在本说明书实施例中，在支付宝服务器匹配用户认证信息成功的情况下，接收支付宝服务器发送的张三的银行卡号 6225999878762456 和 6225999878762457。银行卡号 6225999878762456 和 6225999878762457 显示在支付宝客户端界面。
- [114] 作为一种可选地实施方式，在本说明书实施例中，在张三选择上述银行卡号 6225999878762456 的情况下，支付宝客户端接收张三对该银行卡号 6225999878762456
- 15 进行选择的结果。
- [115] 步骤 315，接收所述用户对确定绑定号码进行确认的结果，绑定号码成功。
- [116] 在本说明书实施例中，在张三点击“确定绑定号码”按钮的情况下，支付宝客户端接收张三对“确定绑定号码”进行点击的结果，绑定号码成功。
- [117] 作为一种可选地实施方式，在张三点击“取消绑定号码”按钮的情况下，支付宝客户端接收张三对“取消绑定号码”进行点击的结果，绑定号码不成功。
- 20 [118] 图 4 为本说明书实施例提供的一种身份认证装置的结构示意图，该结构示意图包括：请求接收模块 405、信息获取模块 410、信息匹配模块 415、结果确认模块 420、号码及密令获取模块 425 和号码及密令发送模块 430；
- [119] 所述请求接收模块 405，用于接收数据认证平台客户端发送的用户身份认证请求，
- 25 其中，所述用户身份认证请求包括用户认证信息和用户标识信息，所述数据认证平台服务器预先存储有用户认证信息和与该用户标识信息对应的注册号码及密令；
- [120] 所述信息获取模块 410，用于根据所述用户标识信息获取数据认证平台服务器中预先存储的用户认证信息；

- [121] 所述信息匹配模块 415, 用于将获取的用户身份认证请求中的用户认证信息与获取的数据认证平台服务器中预先存储的用户认证信息进行匹配;
- [122] 所述结果确认模块 420, 用于在匹配成功的情况下, 接收数据认证平台客户端发送的所述用户对获取注册号码进行确认的结果;
- 5 [123] 所述号码及密令获取模块 425, 用于根据接收的确认结果, 获取所述用户的注册号码及对应的密令;
- [124] 所述号码及密令发送模块 430, 用于将获取的所述用户的注册号码及对应的密令发送到第三方机构服务器。
- [125] 可选地, 所述号码及密令获取模块, 具体用于获取所述用户的每个注册号码及
- 10 对应的密令; 或将获取的所述用户的每个注册号码发送到数据认证平台客户端并获取用户对注册号码进行选择的结果及获取的用户选择的注册号码对应的密令。
- [126] 可选地, 所述用户为预注册用户; 所述装置还包括: 密令生成模块和密令发送模块; 所述密令生成模块, 用于在所述请求接收模块接收数据认证平台客户端发送的用户身份认证请求之前, 将一个或多个所述预注册用户的一个或多个注册号码分别生成具有唯一性的不可逆的密令;
- 15 [127] 所述密令发送模块, 用于将生成的密令批量发送到第三方机构服务器。
- [128] 可选地, 所述数据认证平台服务器预先存储有与该用户标识信息对应的唯一性 ID; 所述信息获取模块, 还用于在所述请求接收模块接收数据认证平台客户端发送的用户身份认证请求之后, 根据所述唯一性 ID 获取数据认证平台服务器中预先存储的用户
- 20 认证信息。
- [129] 图 5 为本说明书实施例提供的一种号码保存和发送装置的结构示意图, 该结构示意图包括: 号码及密令接收模块 505、密令匹配模块 510、号码保存模块 515、请求接收模块 520、信息获取模块 525、信息匹配模块 530、号码获取模块 535 和号码发送模块 540;
- 25 [130] 所述号码及密令接收模块 505, 用于接收数据认证平台服务器发送的用户的注册号码及对应的密令;
- [131] 所述密令匹配模块 510, 用于将接收的所述用户的注册号码对应的密令与预先存储的数据认证平台服务器批量发送的密令进行匹配; 其中, 所述批量发送的密令与预先

存储的用户标识信息相关联;

[132] 所述号码保存模块 515, 用于在匹配成功的情况下, 保存接收的所述用户的注册号码; 其中, 保存的用户的注册号码与预先存储的该用户的用户标识信息相关联;

5 [133] 所述请求接收模块 520, 用于接收第三方机构客户端发送的用户绑定号码请求, 其中, 所述用户绑定号码请求包括用户认证信息和用户标识信息;

[134] 所述信息获取模块 525, 用于根据所述用户标识信息获取第三方机构服务器中预先存储的用户认证信息;

[135] 所述信息匹配模块 530, 用于将接收的用户绑定号码请求中的用户认证信息与获取的第三方机构服务器中预先存储的用户认证信息进行匹配;

10 [136] 所述号码获取模块 535, 用于在匹配成功的情况下, 根据用户标识信息, 获取该用户的注册号码;

[137] 所述号码发送模块 540, 用于将获取的用户的注册号码发送到第三方机构客户端。

[138] 可选地, 所述第三方机构服务器预先存储有与该用户标识信息对应的唯一性 ID;

15 [139] 所述信息获取模块 525, 还用于在所述请求接收模块在接收第三方机构客户端发送的用户绑定号码请求之后, 根据所述唯一性 ID 获取第三方机构服务器中预先存储的用户认证信息。

[140] 可选地, 所述号码及密令接收模块 505, 在接收数据认证平台服务器发送的用户的注册号码及对应的密令之前, 还用于接收数据认证平台服务器根据一个或多个所述用户的一个或多个注册号码分别生成的密令。

20 [141] 图 6 为本说明书实施例提供的一种绑定号码装置的结构示意图, 该结构示意图包括: 请求接收模块 605、请求发送模块 610、号码接收模块 615 和结果确认模块 620;

[142] 所述请求接收模块 605, 用于接收用户绑定号码请求;

[143] 所述请求发送模块 610, 用于将所述用户绑定号码请求发送到第三方机构服务器; 其中, 所述用户绑定号码请求包括用户认证信息和用户标识信息;

25 [144] 所述号码接收模块 615, 用于在第三方机构服务器匹配用户认证信息成功的情况下, 接收第三方机构服务器发送的用户的注册号码;

[145] 所述结果确认模块 620, 用于接收所述用户对确定绑定号码进行确认的结果, 绑

定号码成功。

[146] 可选地, 所述号码接收模块 615, 具体用于接收第三方机构服务器发送的用户已选择的注册号码; 或接收第三方机构服务器发送的用户的每个注册号码并获取所述用户对所述注册号码进行选择的结果。

- 5 [147] 可选地, 所述装置还包括: 结果确认模块, 用于在号码接收模块接收第三方机构服务器发送的用户的注册号码之后, 接收所述用户对取消绑定号码进行确认的结果, 绑定号码不成功。

[148] 本说明书实施例提供的一种身份认证设备, 包括: 存储器以及处理器, 所述存储器存储程序, 并且被配置成由所述处理器执行接收数据认证平台客户端发送的用户身份认证请求, 其中, 所述用户身份认证请求包括用户认证信息和用户标识信息, 所述数据认证平台服务器预先存储有用户认证信息和与该用户标识信息对应的注册号码及密令; 根据所述用户标识信息获取数据认证平台服务器中预先存储的用户认证信息; 将获取的用户身份认证请求中的用户认证信息与获取的数据认证平台服务器中预先存储的用户认证信息进行匹配; 在匹配成功的情况下, 接收数据认证平台客户端发送的所述用户对获取注册号码进行确认的结果; 根据接收的确认结果, 获取所述用户的注册号码及对应的密令; 将获取的所述用户的注册号码及对应的密令发送到第三方机构服务器。

10

15

[149] 本说明书实施例提供的一种号码保存和发送设备, 包括: 存储器以及处理器, 所述存储器存储程序, 并且被配置成由所述处理器执行接收数据认证平台服务器发送的用户的注册号码及对应的密令; 将接收的所述用户的注册号码对应的密令与预先存储的数据认证平台服务器批量发送的密令进行匹配; 其中, 所述批量发送的密令与预先存储的用户标识信息相关联; 在匹配成功的情况下, 保存接收的所述用户的注册号码; 其中, 保存的用户的注册号码与预先存储的该用户的用户标识信息相关联; 接收第三方机构客户端发送的用户绑定号码请求, 其中, 所述用户绑定号码请求包括用户认证信息和用户标识信息; 根据所述用户标识信息获取第三方机构服务器中预先存储的用户认证信息; 将接收的用户绑定号码请求中的用户认证信息与获取的第三方机构服务器中预先存储的用户认证信息进行匹配; 在匹配成功的情况下, 根据用户标识信息, 获取该用户的注册号码; 将获取的用户的注册号码发送到第三方机构客户端。

20

25

[150] 本说明书实施例提供的一种绑定号码设备, 包括: 存储器以及处理器, 所述存储器存储程序, 并且被配置成由所述处理器执行接收用户绑定号码请求并将所述用户绑定号码请求发送到第三方机构服务器; 其中, 所述用户绑定号码请求包括用户认证信息

30

和用户标识信息；在第三方机构服务器匹配用户认证信息成功的情况下，接收第三方机构服务器发送的用户的注册号码；接收所述用户对确定绑定号码进行确认的结果，绑定号码成功。

5 [151] 图 7 为本说明书实施例提供的一种用于身份认证、号码保存和发送及绑定号码的系统的结构示意图，该结构示意图包括：身份认证装置 705、号码保存和发送装置 710 及绑定号码装置 715。

[152] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

10

[153] 本发明是参照根据本发明实施例方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

15

[154] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

20

[155] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

25

[156] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[157] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）

和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

[158] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[159] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个...”限定的要素，并不排除在包括要素的过程、方法、商品或者设备中还存在另外的相同要素。

[160] 以上仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。