

提供和获取安全身份信息的方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及身份安全认证领域，尤其涉及提供和获取安全身份信息的方法和装置。

5 背景技术

[02] 在线下的各种应用场景中，传统对用户的身份核验通常是基于证件实现的，即遵循“由证件实现证实人的身份真实性”逻辑。具体实现中，自然人提供证件（如身份证、护照等），由代表场景商户的自然人（如酒店的前台人员，行政办理大厅的窗口办事人员）通过视检的方式确认用户与证件的对应关系，并且通过视检或是读卡设备的协助确
10 认证件的真实性，在此基础上从证件上获取所需要的验证信息，即可认为该验证信息是可信身份信息，之后根据场景商户的业务逻辑提供服务。

[03] 然而，随着用户隐私保护（如最小可用原则）的不断加强，以及用户对便捷性要求越来越高，以上所述的传统的线下对于用户身份的核验方式目前面临着越来越多的挑战，在很多场景中出现了无法满足需求的情况。例如：

15 [04]--用户可能并没有随身携带身份证；

[05]--在一些低级别的线下应用场景中，用户并不愿意将身份证等核心证件交付他人核验，甚至留存复印件；

[06]--业务本身只需要部分用户信息，不需要身份证中所有的要素信息。

[07] 随着线上商业化的不断发展，网络空间实名/实人/实证等认证方式的普及，证件电
20 子化成为了未来的趋势。然而，基于证件电子化的身份核验也面临着安全威胁：如身份证电子版照片可能被 ps（针对实名核验的攻击），人脸核验可能被攻破（针对实名实人核验的攻击）等，这就需要一个可信的核验源提供身份核验服务。例如公安的制证数据库、人口库等。

[08] 因此，希望能有改进的方案，更加安全更加便捷地实现身份的核验。

25 发明内容

[09] 本说明书一个或多个实施例描述了提供和获取安全身份信息的方法及装置，通过这

样的方法和装置，用户在线下可以利用可信应用，通过扫描业务方展示的二维码，安全便捷地向业务方提供经过核验的安全身份信息。

[10]根据第一方面，提供了一种提供安全身份信息的方法，该方法由可信应用服务端执行，包括：

5 [11]获取用户扫描的二维码对应的二维码信息，所述二维码由注册平台针对第一业务方预先生成；

[12]向所述注册平台发送查询请求，所述查询请求包括所述二维码信息；

[13]从所述注册平台接收查询结果，所述查询结果包括所述第一业务方的标识信息，所述第一业务方的公钥，以及所述第一业务方需要的第一身份信息；

10 [14]获取用户的第二身份信息；

[15]将所述用户的第二身份信息发送到核验源，以得到核验结果；

[16]生成安全身份信息，所述安全身份信息包括所述第一业务方的标识信息，以及加密信息，所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到，所述经过核验的第一身份信息基于所述第二身份信息和所述核验结果而确定；

15 [17]将所述安全身份信息发送至所述注册平台，以使得注册平台将所述加密信息发送至所述第一业务方。

[18]根据一种实施方式，获取用户的第二身份信息包括，通过所述可信应用的客户端所在的终端，采集所述第二身份信息

[19]进一步地，在具体实施例中，采集所述第二身份信息可以包括以下中的一项或多项：

20 [20]通过所述终端上的摄像头采集人脸信息；

[21]通过所述终端的 NFC 功能和其上的控件，读取身份证信息。

[22]根据另一种实施方式，获取用户的第二身份信息包括，通过所述可信应用的客户端，接收用户的输入信息。

[23]在一种可能的设计中，上述方法还包括，根据需要的第一身份信息和获取的第二身
25 份信息，确定所述核验源以及所需的核验模式。

[24]进一步地，在一个实施例中，获取的第二身份信息包括需要的第一身份信息；在这样的情况下，确定所述核验源以及所需的核验模式包括，确定所需的核验模式为鉴别模

述第一业务方的公钥，以及所述第一身份信息；

[40]从第一应用接收安全身份信息，所述安全身份信息包括所述第一业务方的标识信息以及加密信息，所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到；

5 [41]根据所述第一业务方的标识信息，将所述加密信息发送至所述第一业务方。

[42]在一个实施例中，在从第一应用接收查询请求之前，方法还包括：

[43]从所述第一业务方接收所述注册信息；

[44]基于所述注册信息，为所述第一业务方生成二维码。

[45]在一个实施例中，所述注册信息还包括，第一业务方的路由信息；将所述加密信息

10 发送至所述第一业务方具体包括：

[46]从所述安全身份信息中分别提取出所述第一业务方的标识信息，以及加密信息；

[47]根据所述第一业务方的标识信息确定出第一业务方的路由信息；

[48]按照所述路由信息，将所述加密信息发送至所述第一业务方对应的终端。

[49]根据一种可能的设计，所述注册中心与特定应用的服务端位于同一物体实体中；并且，查询请求包括第一字段，在所述第一字段具有第一值的情况下，指示出所述第一应用为所述特定应用，在所述第一字段具有第二值的情况下，指示出所述第一应用不是所述特定应用。

15 [50]进一步地，在一个实施例中，所述第一字段具有第一值；此时，可以在本地将所述查询结果提供给所述第一应用的应用逻辑；并且，在本地从所述第一应用的应用逻辑获取所述安全身份信息。

[51]根据第三方面，提供一种提供安全身份信息的装置，该装置部署在可信应用服务端，包括：

[52]二维码获取单元，配置为获取用户扫描的二维码对应的二维码信息，所述二维码由注册平台针对第一业务方预先生成；

20 [53]查询请求发送单元，配置为向所述注册平台发送查询请求，所述查询请求包括所述二维码信息；

[54]查询结果接收单元，配置为从所述注册平台接收查询结果，所述查询结果包括第一

业务方的标识信息,所述第一业务方的公钥,以及所述第一业务方需要的第一身份信息;

[55]身份信息获取单元,配置为获取用户的第二身份信息;

[56]核验发送单元,配置为将所述用户的第二身份信息发送到核验源,以得到核验结果;

[57]安全信息生成单元,配置为生成安全身份信息,所述安全身份信息包括所述第一业务方的标识信息,以及加密信息,所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到,所述经过核验的第一身份信息基于所述第二身份信息和所述核验结果而确定;

[58]安全信息发送单元,配置为将所述安全身份信息发送至所述注册平台,以使得注册平台将所述加密信息发送至所述第一业务方。

10 [59]根据第四方面,提供一种获取安全身份信息的装置,该装置部署在注册平台,包括:

[60]查询请求接收单元,配置为从第一应用接收查询请求,所述查询请求包括二维码信息,该二维码信息是利用第一应用扫描所述注册平台预先为第一业务方生成的二维码而得到;

[61]注册信息确定单元,配置为基于所述二维码信息,确定所述第一业务方的注册信息,
15 所述注册信息至少包括,所述第一业务方的公钥,以及所述第一业务方需要的第一身份信息;

[62]查询结果发送单元,配置为向所述第一应用发送查询结果,所述查询结果包括第一业务方的标识信息,所述第一业务方的公钥,以及所述第一身份信息;

[63]安全信息接收单元,配置为从第一应用接收安全身份信息,所述安全身份信息包括
20 所述第一业务方的标识信息,以及加密信息,所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到;

[64]加密信息发送单元,配置为根据所述第一业务方的标识信息,将所述加密信息发送至所述第一业务方。

[65]根据第五方面,提供了一种计算机可读存储介质,其上存储有计算机程序,当所述
25 计算机程序在计算机中执行时,令计算机执行第一方面到第二方面的方法。

[66]根据第六方面,提供了一种计算设备,包括存储器和处理器,其特征在于,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现第一方面到第二方面的方法。

- [67]通过本说明书实施例提供的方法和装置，在需要身份核验的情况下，用户通过可信应用来扫描业务方展示的二维码，从而通过注册平台将经过核验的身份信息提供给业务方。在提供身份信息之前，可信应用首先将用户的身份信息发到第三方核验源进行核验，如此保证了提供身份信息的准确性和权威性。并且在以上过程中，通过注册平台来实现
- 5 不同业务方与不同可信应用之间的互联互通，如此，业务方无需关注用户使用哪个应用来提供身份信息，核验更加灵活和便捷。

附图说明

- [68]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
- 10 本领域普通技术人员来讲，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它的附图。

- [69]图 1 示出本说明书披露的一个实施例的实施场景示意图；
- [70]图 2 示出根据一个实施例的获取安全身份信息的方法；
- [71]图 3 示出根据另一个实施例的获取安全身份信息的方法；
- 15 [72]图 4 示出根据一个实施例的提供安全身份信息的装置的示意性框图；
- [73]图 5 示出根据一个实施例的获取安全身份信息的装置的示意性框图。

具体实施方式

- [74]下面结合附图，对本说明书提供的方案进行描述。
- [75]图 1 为本说明书披露的一个实施例的实施场景示意图。根据图 1 的实施例，需要安全身份信息的各个业务方（也就是前述的场景商户）预先向注册平台进行注册，注册平台为各个业务方生成其专属的二维码。在线下需要进行身份核验或提供身份信息的场景下，用户并不需要直接将身份信息提供给业务方的工作人员，而是通过可信应用扫描业务方展示的二维码，然后将获取的用户身份信息交由权威的第三方核验源进行身份核验。核验通过之后，可信应用经由注册平台，将加密的身份信息提供给业务方。
- 20 [76]具体地，在用户需要进行身份核验或提供安全身份信息的情况下，用户首先使用可信应用中扫描功能，扫描业务方展示的二维码。然后，可信应用针对该二维码向注册平台发起查询。由于该二维码是注册平台针对该业务方生成的，因此，注册平台可以查询
- 25

获知该二维码对应的信息，其中包括哪个业务方需要什么样的身份信息。一旦得到包含上述信息的查询结果，可信应用可以对应获取用户的身份信息，例如包括姓名，身份证信息，人脸信息等，然后将这些信息发往第三方核验源进行核验。在核验通过之后，可信应用将核验通过的身份信息进行加密，发送给注册平台；注册平台解析之后，将加密的身份信息转发给业务方。如此，业务方通过解密即可获得所需的身份信息。下面描述以上过程的具体实现步骤。

[77]图 2 示出根据一个实施例的获取安全身份信息的方法。如图 2 所示，该方法至少涉及可信应用，核验源，注册平台和业务方。

[78]核验源，又称为可信核验源或第三方核验源，是提供可信身份信息核验服务的第三方。第三方核验源通常掌握着可信的数据库，配置了可信电子身份的核验策略，通常支持可信凭证，根据提供的用户信息验证是否真实准确，并且其核验结果被认为是准确有效的。上述核验源例如包括，公安一所目前搭建的 CTID 网证平台，人口库等等。

[79]业务方，或称为场景商户，是线下应用场景中需要安全身份信息的业务应用方。业务方原本需要线下根据实体证件确认用户身份，在确定了用户可信身份信息后，根据业务逻辑开展服务，如需要身份核验的酒店、行政办理大厅、网吧等等。

[80]可信应用，是受到场景商户和第三方核验源信任的应用。该可信应用与可信核验源进行对接，通过签名确保双方的可信性。可信应用例如是支付宝。

[81]注册平台负责维护业务方的注册，可信应用的注册，以及进行注册信息与码串的映射和解析。注册平台可以对接若干个可信应用，以及许多个业务方。

[82]下面，首先描述业务方获得并展示二维码的过程，该过程对应于图 2 的步骤 S101 到 S104。

[83]首先，在步骤 S101，需要安全身份信息的业务方向注册平台提交注册信息，以请求二维码。一般地，注册信息至少包括，业务方的名称（例如商户 id），业务方公钥，业务方的路由信息（例如目的地址，网关信息等）以及业务方所需的身份信息，以下称为第一身份信息。可选的，注册信息还可以包含其他信息，例如一些描述信息等。

[84]在不同实施例中，第一身份信息可以包括，姓名，身份证号，民族，证件有效期，人脸照片，驾驶证信息等等中的一项或多项，具体内容 by 业务方根据其业务逻辑设定，或者由业务方所属行业统一规定。

[85]注册平台针对业务方提交的注册信息，生成业务索引，或称为业务令牌（token），

将业务索引与注册信息绑定，换言之，将业务索引与注册信息相关联、相对应地进行存储。

[86]接着，在步骤 S102，注册平台根据业务方的注册信息，生成二维码信息。可以理解，每个二维码可以对应一个码串，该码串可以映射为二维码。因此，本文所称的二维码信息既可以是二维码本身，也可以是二维码对应的码串。

[87]具体地，在一个例子中，注册平台可以将上述业务索引落成码串，从而生成二维码；在另一例子中，注册平台也可以将注册信息落成码串，从而生成二维码。

[88]在步骤 S103，注册平台向业务方返回二维码信息。在该步骤中，注册平台既可以将二维码图案返回给业务方，也可以向其返回一个码串，使得业务方根据约定方式，将码串映射为二维码。

[89]于是，在步骤 S104，业务方可以根据得到的二维码信息，展示二维码，供有需要的用户扫描。例如，业务方可以将该二维码打印出来，展示在前台；或者，业务方可以利用电子显示设备来展示该二维码。

[90]需要理解，以上获得并展示二维码的过程，是用户通过二维码方式进行安全核验的预备步骤，在用户进行身份核验并提供安全身份信息之前预先进行。

[91]下面描述用户通过扫码方式利用可信应用进行身份核验，进而向业务方提供安全身份信息的过程。

[92]可以理解，用户通常是自然人，也是电子核验身份的对象，如支付宝的用户。当用户在线下遇到需要身份核验的场景时，例如入住酒店需要核验身份时，取代于将身份证提供给酒店前台，用户可以打开可信应用，请求可信应用扫描业务方展示的二维码。也就是，如图 2 所示，在步骤 S201，用户向可信应用发出请求，用于请求可信应用执行扫码，读取业务方展示的二维码。例如，在一个例子中，用户可以打开支付宝，点击“扫一扫”，从而发出扫码请求。

[93]在步骤 S202，可信应用执行扫码，获取用户扫描的二维码对应的二维码信息。可以理解，该二维码由注册平台针对业务方预先生成，如前述步骤 S101-S104 所示。

[94]更具体而言，可信应用客户端通过调用客户端所在的终端所配备的摄像头，读取二维码的图像，获取对应的二维码信息，并将该二维码信息传送至服务端。

[95]可以理解，二维码中都会携带该二维码的生成方的信息，例如标识或地址。因此，

可信应用扫描上述二维码之后，可以按照常规方式解析该二维码，确定出生成该二维码的注册平台，以及获取到二维码对应的码串。但是需要理解，上述二维码信息是注册平台根据一定规则，基于业务方的注册信息进行编码、映射等各种操作而生成的（如前述步骤 S102 所示），可信应用虽然可以读取到二维码对应的码串，但是不能从中解析中业务方信息。因此，可信应用仍然需要与注册平台交互，以查询获得业务方相关信息。

[96] 于是，在步骤 S203，可信应用（服务端）向注册平台发送查询请求，所述查询请求包括所述二维码信息。

[97] 在步骤 S204，注册平台根据接收到的查询请求进行查询。具体而言，该查询至少包括，基于查询请求中包含的二维码信息，确定对应的业务方以及该业务方的注册信息。在一个例子中，注册平台可以根据二维码信息确定出对应的业务索引，然后基于业务索引确定出关联存储的注册信息。如前所述，注册信息中至少包括，业务方的名称，业务方的公钥，业务方的路由信息，以及业务方所需的身份信息等。以下将业务方所需的身份信息称为第一身份信息。应该理解，本文中的“第一”，“第二”仅仅是为了表述的清楚而对类似概念进行的标记和区分，并不具有其他限定作用。

[98] 可以理解，业务方展示的二维码是在之前的步骤 S102，由注册平台根据业务方的注册信息而生成的，因此，注册平台可以根据生成该二维码时采用的操作的逆向操作，从二维码信息反向确定出业务方的注册信息。

[99] 在查询得到业务方的注册信息后，在步骤 S205，注册平台向可信应用返回查询结果，其中包括业务方的标识信息，业务方的公钥，以及该业务方需要的第一身份信息。此处，注册平台可以将注册信息中的业务方名称作为业务方的标识信息，也可以将注册平台为其生成的业务索引作为标识信息，只要注册平台可以依据该标识信息确定出对应的业务方的信息即可。

[100] 接收到这样的查询结果之后，在步骤 S206，可信应用根据业务方需要的第一身份信息，获取用户的各种身份信息，所获取的用户身份信息称为第二身份信息。

[101] 具体地，获取用户的身份信息可以采用硬件采集、用户手工输入、读取已有信息等多种方式。在一种实施方式中，可信应用首先根据要获取的身份信息的内容，以及所在终端的硬件和控件配置状况，确定用户身份信息的获取方式。

[102] 在一个实施例，终端配置有相应硬件和控件，那么该步骤 S206 中获取第二身份信息可以包括，通过可信应用的客户端所在的终端，采集第二身份信息。例如，在一

个例子中，可以通过终端上的摄像头采集人脸信息；在另一例子中，可以通过终端的 NFC 功能和其上的控件，读取身份证信息。

5 [103] 在另一实施例中，该步骤 S206 中获取第二身份信息可以包括，通过可信应用的客户端渲染输入界面，接收用户的输入信息。例如输入信息可以包括，用户姓名，身份证号，口令等等。

[104] 在又一实施例中，该步骤 S206 中获取第二身份信息可以包括，读取可信应用中存储的用户身份信息。例如，用户可以预先将其姓名、身份证号存储在可信应用客户端或服务端。如此，在步骤 206，可以直接提取可信应用已经存储的用户身份信息，来减少用户手工输入的次数，提升用户便捷度。

10 [105] 以上实施例可以结合使用。例如，在一个例子中，可以通过终端的 NFC 功能和相应控件，读取用户的二代身份证，获取姓名、身份证号、证件有效期，并通过终端的摄像头采集人脸照片，作为第二身份信息。

[106] 在另一例子中，可以通过客户端接收用户手工输入的姓名、身份证号，并通过摄像头采集人脸照片，作为第二身份信息。

15 [107] 如此，在步骤 S206，可信应用通过多种方式，获取用户的第二身份信息。

[108] 在获取用户的身份信息之后，可信应用需要将获取的身份信息交由核验源进行核验，以保证身份信息的安全性和准确性。在对接的核验源不唯一，和/或核验模式不唯一的情况下，在一个实施例中，可信应用在获取到第二身份信息之后，在步骤 S207，根据需要的第一身份信息和获取的第二身份信息，确定需要的核验源以及所需的核验模
20 式。

[109] 可以理解，可信应用预先可以对接多个核验源。在与各个核验源对接时，双方会明确约定，可以核验哪些信息，以及所支持的核验模式。因此，根据第一身份信息和第二身份信息的信息内容，可以确定出需要哪些核验源，以及所需的核验模式。

25 [110] 一般地，核验源提供的核验模式包括鉴别模式和信息模式。在鉴别模式下，核验源对发送来的身份信息进行核验之后，返回核验是否通过的通知结果。在信息模式下，核验源返回的核验结果包括，核验是否通过的通知，以及基于核验通过的身份信息而确定的补充身份信息。

[111] 在一种实施方式中，步骤 S206 中获取的第二身份信息即为业务方需要的第一身份信息，甚至可以包含更多内容。在这样的情况下，在步骤 S207 可以确定仅需要鉴别

模式即可，也就是，仅需要获知，第二身份信息的各项是否核验通过。

[112] 在另一种可能的实施方式中，由于采集困难或其他原因，获取的第二身份信息也可以是第一身份信息的一部分。此时，就需要借助核验源提供补充信息。因此，在这样的情况下，在步骤 S207 可以确定需要的核验模式为信息模式。

- 5 [113] 于是，在步骤 S208，可信应用根据以上确定的核验源和核验模式，将第二身份信息发送给对应核验源，并请求以对应核验模式进行核验。这个过程中，可信应用和核验源可以通过签名和验签建立信任关系，确保数据的安全有效。

[114] 在步骤 S209，核验源根据请求的核验模式，对获得的身份信息进行核验。

- 10 [115] 在鉴别模式下，核验源对身份的核验包括信息的比对。在一个例子中，核验源保存完整的用户信息。这种情况下，核验源通过将获得的第二身份信息与保存的用户信息直接比对，来进行用户身份核验。在另一例子中，核验源为了避免遭受攻击从而批量泄露用户信息，因此可以配置策略，仅保存用户信息的哈希值。这种情况下，核验源对接收到的用户身份信息进行同样的哈希运算，比较运算的哈希值和存储的哈希值，以此进行用户身份核验。进一步地，核验源可以在一定时间间隔内删除接收到的用户信息，
15 以增加安全性。

[116] 在信息模式下，核验源首先对接收到的身份信息与保存的相应信息进行对比，在确定接收到的身份信息准确无误之后，基于这样的信息确定补充身份信息。

- [117] 例如人口库作为一种核验源，可以在信息模式下，对接收到的用户姓名和身份证号进行核验，在核验通过之后，基于姓名和身份证号，确定用户的民族信息作为补充
20 身份信息。

[118] 在核验之后，在步骤 S210，核验源向可信应用返回核验结果。如前所述，在鉴别模式下，核验源可以反馈核验通过/核验失败的通知结果，在信息模式下，核验源还可以返回补充身份信息。

- [119] 以上描述了通过单个核验源进行身份核验的过程。然而，在一些情况下，单个
25 核验源不足以核验获得第一身份信息。由此，在步骤 S207，可以确定出需要多个核验源。为了描述的简单方便，假定需要的核验源包括第一核验源和第二核验源。

[120] 在这样的情况下，在步骤 S208，可信应用将第二身份信息中的第一部分发送到第一核验源，以及将第二身份信息中的第二部分发送到第二核验源。在一个实施例中，上述第一部分和第二部分可以存在交集。

[121] 在步骤 S209, 第一核验源对上述第二身份信息的第一部分进行核验, 第二核验源对上述第二身份信息的第二部分进行核验。

[122] 在步骤 S210, 可信应用从第一核验源接收第一结果, 从第二核验源接收第二结果。在这之后, 可信应用还将所述第一结果和第二结果合并, 从而得到总的核验结果。

5 [123] 以上多个核验源可以各自具有不同的核验模式, 因此, 不同数目的核验源的实施例可以与不同模式进行核验的实施例进行组合。

[124] 例如, 在一个实施例中, 业务方所需的第一身份信息包括: 用户姓名、身份证号、人脸、用户民族。在步骤 S206 中, 获得的第二身份信息包括: 用户手工输入的姓名、身份证号, 以及采集的人脸照片。根据以上的第一身份信息和第二身份信息, 可信应用判断, 可以采用公安一所核验源 (第一核验源), 以鉴别模式验证姓名、身份证号和人脸, 并采用人口库 (第二核验源), 以信息模式, 通过用户姓名+身份证号获取民族信息作为补充身份信息。

10

[125] 于是, 在步骤 S208, 可信应用将用户姓名、身份证号和人脸发送到公安一所, 请求以鉴别模式进行核验, 将用户姓名和身份证号发送到人口库, 请求以信息模式进行核验。

15

[126] 在另一实施例中, 业务方所需的第一身份信息包括: 用户姓名、身份证号、人脸、用户民族。在步骤 S206 中, 获得的第二身份信息包括: 用户手工输入的姓名、身份证号、民族, 以及采集的人脸照片。根据以上的第一身份信息和第二身份信息, 可信应用判断, 可以采用公安一所核验源 (第一核验源), 以鉴别模式验证姓名、身份证号和人脸, 并采用人口库 (第二核验源), 以鉴别模式验证用户的民族信息。

20

[127] 于是, 在步骤 S208, 可信应用将用户姓名、身份证号和人脸发送到公安一所, 请求以鉴别模式进行核验, 将用户姓名、身份证号和民族发送到人口库, 请求以鉴别模式进行核验。

[128] 在步骤 S210, 可信应用获得各个核验源的核验结果, 并对核验结果进行合并。

25 根据不同核验源的核验模式, 合并后的核验结果可以表示为不同形式。

[129] 在一个例子中, 合并后的核验结果包括, 经过核验的各个信息项的内容。例如, 在一个具体例子中, 核验结果可以表示为: 用户姓名为**, 用户身份证号为**, 用户民族为***, 用户人脸与身份证上的人脸一致。

[130] 在又一例子中, 合并后的核验结果包括, 鉴别模式下得到的各个信息项是否正

确的结果。例如，在一个具体例子中，核验结果可以表示为：用户姓名正确，用户身份证号正确，用户民族正确，用户人脸与身份证上的人脸一致。

[131] 在另一例子中，合并后的核验结果包括，鉴别模式下得到的各个信息项的内容以及是否正确的结果，以及信息模式下提供的补充身份信息。例如，在一个例子中，核验结果可以表示为：用户姓名为***正确，用户身份证号为***正确，用户民族为***（补充身份信息），用户人脸与身份证上的人脸一致。

[132] 可以理解，核验结果的具体表示形式可以不限于以上举例。

[133] 基于以上获得的核验结果，在步骤 S211，可信应用生成安全身份信息。

[134] 具体地，在一个实施例，可信应用可以首先基于第二身份信息和上述核验结果，得到经过核验的第一身份信息。

[135] 更具体地，在一个例子中，获取的第二身份信息与需要的第一身份信息的信息项一致，甚至包含更多内容，并且，在前述步骤中，请求采用鉴别模式对第二身份信息进行核验。如果核验结果显示，第二身份信息的各个信息项核验通过，那么，就可以将核验通过的第二身份信息，作为所述经过核验的第一身份信息。

[136] 在另一例子中，获取的第二身份信息为需要的第一身份信息的一部分，并且，在前述步骤中，请求采用信息模式对第二身份信息进行核验。如果在该信息模式下的核验结果包括，核验通过的通知，以及基于核验通过的信息项确定的补充身份信息，那么，在该步骤中，可以将核验通过的第二身份信息，以及所述补充身份信息，共同作为所述经过核验的第一身份信息。

[137] 然后，可信应用利用步骤 S205 获得的业务方的公钥，对上述得到的经过核验的第一身份信息进行加密，得到加密信息。

[138] 此外，可信应用还在上述加密信息之外，附上业务方的标识信息，如此生成所述安全身份信息。

[139] 接着，在步骤 S212，可信应用将上述生成的安全身份信息发送给注册平台。

[140] 在步骤 S213，注册平台将安全身份信息中的加密信息发送给业务方。

[141] 具体地，注册平台接收到上述安全身份信息后，可以从中提取出加密信息和业务方的标识信息。一旦得到业务方的标识信息，注册平台就可以确定出相应的业务方，并根据该业务方注册时的信息，确定出业务方的路由信息，例如目的地址。然后，可信

应用按照路由信息（例如目的地址），将加密信息发送至第一业务方对应的终端。

[142] 业务方接收到上述加密信息后，在步骤 S214，对上述加密信息进行解密，从而得到需要的第一身份信息。

[143] 可以理解，该加密信息是可信应用利用业务方的公钥对经过核验的第一身份信息进行加密得到的，业务方本地存储有与该公钥对应的私钥。公钥与私钥是成对的密钥，可以用于对另一密钥加密的数据进行解密。因此，在一个实施例中，业务方利用自身的私钥，对接收到的加密信息进行解密，从而获得用户的经过核验的第一身份信息。

[144] 在获得所需的身份信息之后，业务方就可以根据其业务逻辑开展服务，例如网吧可以判断用户年龄是否达到标准，酒店可以基于用户姓名和身份证号进行入住登记，等等。

[145] 通过以上描述可以看到，在线下需要进行身份核验或者提供身份信息的场景下，用户可以不必将身份证件交给业务方的工作人员，而是可以通过可信应用来扫描业务方展示的二维码，该二维码由业务方预先向注册平台注册而生成。可信应用在扫码后，通过向注册平台查询而获知，该业务方需要哪些身份信息，进而采集获取用户的身份信息。之后，可信应用将获取的身份信息发往核验源进行核验，并将核验通过的身份信息进行加密，通过注册平台转发至业务方。在该过程中，引入了公共的注册平台，来实现不同业务方与不同可信应用之间的互联互通，因此业务方只需展示一个二维码，即可适用于与注册平台对接的多种可信应用，而不必针对每个应用展示一个二维码。此外，可信应用在将用户的身份信息发到第三方核验源进行核验之后才将经过核验的身份信息提供给业务方，如此还保证了提供身份信息的准确性和权威性。

[146] 如本领域技术人员所知，一般地，可信应用包含客户端和服务端。客户端例如是移动终端上安装的 App（例如支付宝 App），或者 PC 机上的应用软件客户端。在图 2 所示的方法中，可信应用与用户的交互均通过客户端进行。例如，在步骤 S201，用户通过客户端发出扫码请求，例如点击客户端界面中的相应选项，例如“扫一扫”。在步骤 S202，客户端调用终端的摄像头读取二维码，获取二维码信息，并将二维码信息发送到服务端。在步骤 S206，根据一种实施方式，可以通过客户端采集或接收用户的第一身份信息的至少一部分。之外的其他步骤，包括可信应用与核验源的交互步骤，以及与注册平台的交互步骤，均是通过服务端来执行。

[147] 图 3 示出根据另一实施例的获取安全身份信息的方法。在图 3 的实施例中，注

册中心与某个特定应用位于同一物理实体中，因此简单地示出为可信应用+注册平台。
下文中又将可信应用和注册平台共同所在的实体称为统一服务端。

5 [148] 在这样的情况下，注册平台仍然可以对接多个可信应用，包括本地的特定应用，和其他应用。业务方仍然预先通过注册信息向注册平台发起注册请求来获得并展示二维码，各个可信应用仍然通过扫描获得业务方的二维码信息，并针对读取的二维码向注册平台发起查询请求。在一个实施例中，查询请求可以包括一个特定字段（以下称为第一

10 [149] 假定注册平台接收到来自第一应用的查询请求，该查询请求除了包含二维码信息外，还包括第一字段。在第一字段具有第一值（例如值为 1）的情况下，指示出第一应用即为注册平台本地的特定应用，在第一字段具有第二值（例如值为 0）的情况下，指示出第一应用不是本地的特定应用。

[150] 如果第一字段具有第二值，也就是，注册平台接收到的请求信息来自于非本地的可信应用，那么就按照图 2 所示的通信交互方式，执行后续步骤。

15 [151] 如果所述第一字段具有第一值，也就是，注册平台接收到的请求信息来自于本地的可信应用，那么注册平台与可信应用之间的交互都可以在本地执行，也就是如图 3 所示在统一服务端内部执行。

[152] 具体地，在注册平台接收到查询请求之后，对二维码信息进行查询，得到业务方的注册信息，并基于该注册信息生成查询结果。在第一应用为本地的特定应用的情况下，注册平台可以在本地将上述查询结果提供给第一应用的应用逻辑。因此，图 2 中的
20 步骤 S203 到 S205，可以在统一服务端内部执行，并在图 3 中示出为查询步骤。

[153] 在可信应用（在其应用逻辑中）基于经过核验的第一身份信息生成安全身份信息后，注册平台可以在本地从第一应用的应用逻辑获取所述安全身份信息，从中获得加密信息，提供给业务方。也就是说，图 2 中的步骤 S211 到 S212，可以在统一服务端内部执行，如图 3 所示。

25 [154] 除此之外的其他步骤，例如 S207 到 S210 的身份核验步骤，以及与业务方的交互步骤，与图 2 所示的相同，不再赘述。

[155] 通过图 2 到图 3 所示的实施例中的方法，在需要身份核验的情况下，用户通过可信应用来扫描业务方展示的二维码，从而通过注册平台将经过核验的身份信息提供给业务方。在提供身份信息之前，可信应用首先将用户的身份信息发到第三方核验源进行

核验，如此保证了提供身份信息的准确性和权威性。并且在以上过程中，通过注册平台来实现不同业务方与不同可信应用之间的互联互通，如此，业务方无需关注用户使用哪个应用来提供身份信息，核验更加灵活和便捷。

5 [156] 在以上的获取安全身份信息的过程中，涉及可信应用，注册平台和业务方的多方交互。下面分别描述以上各方的装置构成。

[157] 图 4 示出根据一个实施例的提供安全身份信息的装置的示意性框图，该装置部署于可信应用服务端。如图 4 所示，该装置 400 包括：

[158] 二维码获取单元 41，配置为获取用户扫描的二维码对应的二维码信息，所述二维码由注册平台针对第一业务方预先生成；

10 [159] 查询请求发送单元 42，配置为向所述注册平台发送查询请求，所述查询请求包括所述二维码信息；

[160] 查询结果接收单元 43，配置为从所述注册平台接收查询结果，所述查询结果包括所述第一业务方的标识信息，所述第一业务方的公钥，以及所述第一业务方需要的第一身份信息；

15 [161] 身份信息获取单元 44，配置为获取用户的第二身份信息；

[162] 核验发送单元 45，配置为将所述用户的第二身份信息发送到核验源，以得到核验结果；

[163] 安全信息生成单元 46，配置为生成安全身份信息，所述安全身份信息包括所述第一业务方的标识信息，以及加密信息，所述加密信息是利用所述第一业务方的公钥对
20 经过核验的第一身份信息加密得到，所述经过核验的第一身份信息基于所述第二身份信息和所述核验结果而确定；

[164] 安全信息发送单元 47，配置为将所述安全身份信息发送至所述注册平台，以使得注册平台将所述加密信息发送至所述第一业务方。

25 [165] 根据一种实施方式，身份信息获取单元 44 配置为，通过所述可信应用的客户端所在的终端，采集所述第二身份信息。

[166] 进一步地，在具体实施例中，身份信息获取单元 44 可以如下采集所述第二身份信息：通过所述终端上的摄像头采集人脸信息；和/或，通过所述终端的 NFC 功能和其上的控件，读取身份证信息。

[167] 根据另一种实施方式，身份信息获取单元 44 配置为，通过所述可信应用的客户端，接收用户的输入信息。

[168] 在一种可能的设计中，上述装置还包括确定单元（未示出），配置为根据需要的第一身份信息和获取的第二身份信息，确定所述核验源以及所需的核验模式。

- 5 [169] 进一步地，在一个实施例中，获取的第二身份信息包括需要的第一身份信息；在这样的情况下，确定单元可以确定所需的核验模式为鉴别模式，在所述鉴别模式下，所述核验结果为核验是否通过的通知结果。

[170] 在另一实施例中，获取的第二身份信息为需要的第一身份信息的一部分；在这样的情况下，确定单元可以确定所需的核验模式为信息模式，在所述信息模式下，所述
10 核验结果包括，核验是否通过的通知，以及基于核验通过的第二身份信息的至少一部分确定的补充身份信息。

[171] 根据一个实施例，确定单元确定需要的核验源包括第一核验源和第二核验源；在这样的情况下，核验发送单元 45 配置为：

[172] 将所述第二身份信息中的第一部分发送到第一核验源，以及将所述第二身份信息
15 息中的第二部分发送到第二核验源；

[173] 从所述第一核验源接收第一结果，从所述第二核验源接收第二结果；

[174] 将所述第一结果和第二结果合并，从而得到所述核验结果。

[175] 在一个实施例中，安全信息生成单元 46 具体配置为：

[176] 基于所述第二身份信息和所述核验结果，得到经过核验的第一身份信息；

20 [177] 利用所述第一业务方的公钥对经过核验的第一身份信息进行加密，得到所述加密信息；

[178] 基于所述加密信息以及所述第一业务方的标识信息，生成所述安全身份信息。

[179] 在一个例子中，上述核验结果为鉴别模式下核验通过的通知结果；此时，安全
25 信息生成单元 46 可以将核验通过的所述第二身份信息作为所述经过核验的第一身份信息。

[180] 在另一例子中，上述核验结果包括，核验通过的通知，以及基于核验通过的第二身份信息的至少一部分确定的补充身份信息；此时，安全信息生成单元 46 可以将核验通过的所述第二身份信息，以及所述补充身份信息，作为所述经过核验的第一身份信息

息。

[181] 图 5 示出根据一个实施例的获取安全身份信息的装置的示意性框图，该装置部署于注册平台。如图 5 所示，该装置 500 包括：

5 [182] 查询请求接收单元 51，配置为从第一应用接收查询请求，所述查询请求包括二维码信息，该二维码信息是利用第一应用扫描所述注册平台预先为第一业务方生成的二维码而得到；

[183] 注册信息确定单元 52，配置为基于所述二维码信息，确定所述第一业务方的注册信息，所述注册信息至少包括，所述第一业务方的公钥，以及所述第一业务方需要的第一身份信息；

10 [184] 查询结果发送单元 53，配置为向所述第一应用发送查询结果，所述查询结果包括第一业务方的标识信息，所述第一业务方的公钥，以及所述第一身份信息；

[185] 安全信息接收单元 54，配置为从第一应用接收安全身份信息，所述安全身份信息包括所述第一业务方的标识信息，以及加密信息，所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到；

15 [186] 加密信息发送单元 55，配置为根据所述第一业务方的标识信息，将所述加密信息发送至所述第一业务方。

[187] 在一个实施例中，上述装置 500 还包括，二维码生成单元 50，配置为：从所述第一业务方接收所述注册信息；基于所述注册信息，为所述第一业务方生成二维码。

20 [188] 在一个实施例中，所述注册信息还包括，第一业务方的路由信息；所述加密信息发送单元 55 具体配置为：

[189] 从所述安全身份信息中分别提取出所述第一业务方的标识信息，以及加密信息；

[190] 根据所述第一业务方的标识信息确定出第一业务方的路由信息；

[191] 按照所述路由信息，将所述加密信息发送至所述第一业务方对应的终端。

25 [192] 根据一种可能的设计，所述注册中心与特定应用的服务端位于同一物体实体中；并且，查询请求接收单元 51 接收到的查询请求包括第一字段，在所述第一字段具有第一值的情况下，指示出所述第一应用为所述特定应用，在所述第一字段具有第二值的情况下，指示出所述第一应用不是所述特定应用。

[193] 进一步地，在一个实施例中，所述第一字段具有第一值；此时，查询结果发送

单元 53 可以在本地将所述查询结果提供给所述第一应用的应用逻辑；并且，安全信息接收单元 54 可以在本地从所述第一应用的应用逻辑获取所述安全身份信息。

5 [194] 根据另一方面的实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行结合图 2 到图 3 所描述的方法。

[195] 根据再一方面的实施例，还提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现结合图 2 到图 3 所述的方法。

10 [196] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

15 [197] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1. 一种提供安全身份信息的方法，该方法由可信应用服务端执行，包括：
获取用户扫描的二维码对应的二维码信息，所述二维码由注册平台针对第一业务方预先生成；
- 5 向所述注册平台发送查询请求，所述查询请求包括所述二维码信息；
从所述注册平台接收查询结果，所述查询结果包括所述第一业务方的标识信息，所述
所述第一业务方的公钥，以及所述第一业务方需要的第一身份信息；
获取用户的第二身份信息；
将所述用户的第二身份信息发送到核验源，以得到核验结果；
- 10 生成安全身份信息，所述安全身份信息包括所述第一业务方的标识信息，以及加密
信息，所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到，
所述经过核验的第一身份信息基于所述第二身份信息和所述核验结果而确定；
将所述安全身份信息发送至所述注册平台，以使得注册平台将所述加密信息发送至
所述第一业务方。
- 15 2. 根据权利要求 1 所述的方法，其中获取用户的第二身份信息包括，通过所述可信
应用的客户端所在的终端，采集所述第二身份信息。
3. 根据权利要求 2 所述的方法，其中采集所述第二身份信息包括以下中的一项或多
项：
通过所述终端上的摄像头采集人脸信息；
- 20 通过所述终端的 NFC 功能和其上的控件，读取身份证信息。
4. 根据权利要求 1 所述的方法，其中获取用户的第二身份信息包括，通过所述可信
应用的客户端，接收用户的输入信息。
5. 根据权利要求 1 所述的方法，还包括，根据需要的第一身份信息和获取的第二身
份信息，确定所述核验源以及所需的核验模式。
- 25 6. 根据权利要求 5 所述的方法，其中，获取的第二身份信息包括需要的第一身份信
息；
所述确定所述核验源以及所需的核验模式包括，确定所需的核验模式为鉴别模式，
在所述鉴别模式下，所述核验结果为核验是否通过的通知结果。
7. 根据权利要求 5 所述的方法，其中，获取的第二身份信息为需要的第一身份信息
30 的一部分；
所述确定所述核验源以及所需的核验模式包括，确定所需的核验模式为信息模式，

在所述信息模式下,所述核验结果包括,核验是否通过的通知,以及基于核验通过的所述第二身份信息的至少一部分确定的补充身份信息。

8. 根据权利要求5所述的方法,其中确定所述核验源以及所需的核验模式包括,确定所述核验源包括第一核验源和第二核验源;

5 所述将所述用户的第二身份信息发送到核验源,以得到核验结果,包括:

将所述第二身份信息中的第一部分发送到第一核验源,以及将所述第二身份信息中的第二部分发送到第二核验源;

从所述第一核验源接收第一结果,从所述第二核验源接收第二结果;

将所述第一结果和第二结果合并,从而得到所述核验结果。

10 9. 根据权利要求1所述的方法,其中所述生成安全身份信息包括:

基于所述第二身份信息和所述核验结果,得到经过核验的第一身份信息;

利用所述第一业务方的公钥对经过核验的第一身份信息进行加密,得到所述加密信息;

基于所述加密信息以及所述二维码信息,生成所述安全身份信息。

15 10. 根据权利要求9所述的方法,其中所述核验结果为鉴别模式下核验通过的通知结果;

所述基于所述第二身份信息和所述核验结果,得到经过核验的第一身份信息包括:将核验通过的所述第二身份信息作为所述经过核验的第一身份信息。

20 11. 根据权利要求9所述的方法,其中所述核验结果包括,核验通过的通知,以及基于核验通过的第二身份信息的至少一部分确定的补充身份信息;

所述基于所述第二身份信息和所述核验结果,得到经过核验的第一身份信息包括:将核验通过的所述第二身份信息,以及所述补充身份信息,作为所述经过核验的第一身份信息。

12. 一种获取安全身份信息的方法,该方法由注册平台执行,包括:

25 从第一应用接收查询请求,所述查询请求包括二维码信息,该二维码信息是利用第一应用扫描所述注册平台预先为第一业务方生成的二维码而得到;

基于所述二维码信息,确定所述第一业务方的注册信息,所述注册信息至少包括,所述第一业务方的公钥,以及所述第一业务方需要的第一身份信息;

30 向所述第一应用发送查询结果,所述查询结果包括第一业务方的标识信息,所述第一业务方的公钥,以及所述第一身份信息;

从第一应用接收安全身份信息,所述安全身份信息包括所述第一业务方的标识信息,

以及加密信息,所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到;

根据所述第一业务方的标识信息,将所述加密信息发送至所述第一业务方。

13. 根据权利要求 12 所述的方法,在从第一应用接收查询请求之前,还包括:

5 从所述第一业务方接收所述注册信息;

基于所述注册信息,为所述第一业务方生成二维码。

14. 根据权利要求 13 所述的方法,还包括,

针对所述注册信息,生成业务索引;

将所述业务索引与所述注册信息相关联地进行存储。

10 15. 根据权利要求 12 所述的方法,其中所述注册信息还包括,第一业务方的路由信息;

将所述加密信息发送至所述第一业务方,包括:

从所述安全身份信息中分别提取出所述第一业务方的标识信息,以及加密信息;

根据所述第一业务方的标识信息确定出第一业务方的路由信息;

15 按照所述路由信息,将所述加密信息发送至所述第一业务方对应的终端。

16. 根据权利要求 12 所述的方法,其中所述注册中心与特定应用的服务端位于同一物体实体中;

所述查询请求包括第一字段,在所述第一字段具有第一值的情况下,指示出所述第一应用为所述特定应用,在所述第一字段具有第二值的情况下,指示出所述第一应用不是所述特定应用。

20 17. 根据权利要求 16 所述的方法,其中所述第一字段具有第一值;

所述向所述第一应用发送查询结果包括,在本地将所述查询结果提供给所述第一应用的应用逻辑;

25 所述从第一应用接收安全身份信息包括,在本地从所述第一应用的应用逻辑获取所述安全身份信息。

18. 一种提供安全身份信息的装置,该装置部署在可信应用服务端,包括:

二维码获取单元,配置为获取用户扫描的二维码对应的二维码信息,所述二维码由注册平台针对第一业务方预先生成;

30 查询请求发送单元,配置为向所述注册平台发送查询请求,所述查询请求包括所述二维码信息;

查询结果接收单元,配置为从所述注册平台接收查询结果,所述查询结果包括所述

第一业务方的标识信息, 所述第一业务方的公钥, 以及所述第一业务方需要的第一身份信息;

身份信息获取单元, 配置为获取用户的第二身份信息;

核验发送单元, 配置为将所述用户的第二身份信息发送到核验源, 以得到核验结果;

- 5 安全信息生成单元, 配置为生成安全身份信息, 所述安全身份信息包括所述第一业务方的标识信息, 以及加密信息, 所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到, 所述经过核验的第一身份信息基于所述第二身份信息和所述核验结果而确定;

- 10 安全信息发送单元, 配置为将所述安全身份信息发送至所述注册平台, 以使得注册平台将所述加密信息发送至所述第一业务方。

19. 一种获取安全身份信息的装置, 该装置部署在注册平台, 包括:

查询请求接收单元, 配置为从第一应用接收查询请求, 所述查询请求包括二维码信息, 该二维码信息是利用第一应用扫描所述注册平台预先为第一业务方生成的二维码而得到;

- 15 注册信息确定单元, 配置为基于所述二维码信息, 确定所述第一业务方的注册信息, 所述注册信息至少包括, 所述第一业务方的公钥, 以及所述第一业务方需要的第一身份信息;

查询结果发送单元, 配置为向所述第一应用发送查询结果, 所述查询结果包括第一业务方的标识信息, 所述第一业务方的公钥, 以及所述第一身份信息;

- 20 安全信息接收单元, 配置为从第一应用接收安全身份信息, 所述安全身份信息包括所述第一业务方的标识信息, 以及加密信息, 所述加密信息是利用所述第一业务方的公钥对经过核验的第一身份信息加密得到;

加密信息发送单元, 配置为根据所述第一业务方的标识信息, 将所述加密信息发送至所述第一业务方。

- 25 20. 一种计算机可读存储介质, 其上存储有计算机程序, 当所述计算机程序在计算机中执行时, 令计算机执行权利要求 1-17 中任一项的所述的方法。

21. 一种计算设备, 包括存储器和处理器, 其特征在于, 所述存储器中存储有可执行代码, 所述处理器执行所述可执行代码时, 实现权利要求 1-17 中任一项所述的方法。