

一键登录业务的实现

技术领域

[01]本说明书一个或多个实施例涉及网络信息技术，尤其涉及一键登录业务的实现方法和装置。

背景技术

[02]随着网络的快速发展，基于网络产生了各种各样的业务应用。用户只需要在终端设备中下载相应业务应用的应用客户端即应用程序（APP），通过应用客户端注册并登录，就可以享受相应的业务应用，比如，看电影或者购买商品等。

[03]为了方便用户的使用，目前出现了一种新的登录 APP 的方法，即一键登录方法。在一键登录方法中，应用客户端，通常为手机，会预先嵌入认证 SDK，用户请求登录时，通过该 SDK 与运营商服务器通信以便采集用户手机号码，在获得用户同意授权后，应用客户端获得接口调用的令牌（token），将 token 传递给应用服务器，应用服务器利用 token 获取当前授权用户的手机号码等信息，从而完成了 APP 的登录。

[04]参见图 1，在一键登录业务中，用户只需要点击相关的“一键登录”的按键，而无需输入手机号码、用户名、密码以及短信验证码等，因此，可以让用户更方便、快捷地完成注册、登录流程，将原本可能需要 20 秒左右的流程，缩短到了 2 秒左右，为用户使用带来了很大的方便。

[05]但是，目前的一键登录业务的安全性相对较低，这样就容易造成用户隐私数据的泄露，因此需要一种更为安全的一键登录业务的实现方法。

发明内容

[06]本说明书一个或多个实施例描述了一键登录业务的实现方法和装置，能够提高一键登录业务的安全性。

[07]根据第一方面，提供了一种一键登录业务的实现方法，其中包括：从应用客户端发来的校验请求中获取第一 IP 地址的信息；向所述应用客户端下发令牌 token；从应用服务器发来的号码获取请求中获取第二 IP 地址的信息；判断所述第一 IP 地址与所述第二 IP 地址是否相同，如果相同，则根据所述号码获取请求中携带的 token 获取应用客户端所在的终端设备的手机号，并发送给所述应用服务器，如果不相同，则拒绝将该

终端设备的手机号发送给所述应用服务器。

[08]所述校验请求包括如下中的至少一个请求：携带 APP ID、APP sign， KEY ID、时间戳以及所述 IP 地址的登录验证请求；携带 APP ID、所述 IP 地址及时间戳的手机身份校验请求；携带 APP ID 及所述 IP 地址的新定义的校验请求。

[09]其中，所述校验请求为携带 APP ID、第一 IP 地址信息及时间戳的手机身份校验请求时；所述向所述应用客户端下发令牌 token，包括：根据手机身份校验请求进行身份验证，在身份验证成功后，向所述应用客户端下发 token。

[10]其中，在获取第一 IP 地址的信息之前，进一步包括：通过 https 链路接收所述应用客户端发来的登录验证请求，在登录验证成功后，生成对称密钥，通过 https 链路将该对称密钥下发给所述应用客户端；所述获取第一 IP 地址的信息，包括：利用生成的所述对称密钥对应用客户端发来的手机身份校验请求进行解密，从解密后的手机身份校验请求中获取所述第一 IP 地址的信息；所述向所述应用客户端下发令牌 token，包括：利用对称密钥对 token 进行加密，将加密后的 token 下发给应用客户端。

[11]根据第二方面，提供了一键登录业务的实现方法，该方法包括：将终端设备的 IP 地址的信息携带在校验请求中，并将该校验请求发送给运营商服务器；接收运营商服务器下发的 token；将终端设备的 IP 地址的信息及接收到的 token 发送给应用服务器；如果接收到应用服务器发来的登录授权，则一键登录成功。

[12]所述校验请求包括如下中的至少一个请求：携带 APP ID、APP sign， KEY ID、时间戳以及所述 IP 地址的登录验证请求；携带 APP ID、所述 IP 地址及时间戳的手机身份校验请求；携带 APP ID 及所述 IP 地址的新定义的校验请求。

[13]其中，在将手机身份校验请求发送给运营商服务器之前，进一步包括：通过 https 链路向运营商服务器发送登录验证请求，通过 https 链路接收运营商服务器下发的对称密钥；所述将该校验请求发送给运营商服务器，包括：利用所述对称密钥对手机身份校验请求进行加密，将加密后的手机身份校验请求发送给运营商服务器；所述接收运营商服务器下发的 token，包括：接收运营商服务器下发的加密后的 token，利用对称密钥对该加密后的 token 进行解密，得到 token。

[14]根据第三方面，提供了一键登录业务的实现方法，该方法包括：接收到应用客户端发来的登录请求之后，进行登录预授权；接收应用客户端发来的 token 及该应用客户端所在的终端设备的 IP 地址的信息；将接收到的 token 以及所述 IP 地址的信息携带在号

码获取请求中，并将该号码获取请求发送给运营商服务器；如果接收到运营商服务器发来的应用客户端所在的终端设备的手机号，则根据该手机号进行登录授权处理。

[15]其中，通过 https 链路与运营商服务器进行信息交互。

[16]根据第四方面，提供了一键登录业务的实现装置，包括：第一 IP 地址获取模块，配置为从应用客户端发来的校验请求中获取第一 IP 地址的信息；令牌下发模块，配置为向所述应用客户端下发 token；第二 IP 地址获取模块，配置为从应用服务器发来的号码获取请求中获取第二 IP 地址的信息；授权处理模块，配置为判断所述第一 IP 地址与所述第二 IP 地址是否相同，如果相同，则根据所述号码获取请求中携带的 token 获取应用客户端所在的终端设备的手机号，并发送给所述应用服务器，如果不相同，则拒绝将该终端设备的手机号发送给所述应用服务器。

[17]根据第五方面，提供了一键登录业务的实现装置，包括：校验请求模块，配置为将所在的终端设备的 IP 地址的信息携带在校验请求中，并将该校验请求发送给运营商服务器；令牌接收模块，配置为接收运营商服务器下发的 token；转发模块，配置为将所在的终端设备的 IP 地址的信息及接收到的 token 发送给应用服务器；登录授权模块，配置为如果接收到应用服务器发来的登录授权，则一键登录成功。

[18]根据第六方面，提供了一键登录业务的实现装置，包括：预登录模块，配置为在接收到应用客户端发来的登录请求之后，进行预登录处理；网络因子获取模块，配置为接收应用客户端发来的 token 以及该应用客户端所在的终端设备的 IP 地址的信息；号码获取模块，配置为将接收到的 token 以及所述 IP 地址的信息携带在号码获取请求中，并将该号码获取请求发送给运营商服务器；授权执行模块，配置为如果接收到运营商服务器发来的应用客户端所在的终端设备的手机号，则根据该手机号进行登录授权处理。

[19]根据第七方面，提供了一种计算设备，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，实现本说明书任一实施例所述的方法。

[20]本说明书实施例提供的一键登录业务的实现方法及装置避免了应用服务器为攻击者的终端设备提供对应的应用服务，提高了安全性。

附图说明

[21]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，下面描述中的附图是本说明书的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[22]图 1 是一键登录业务的一种操作示意图。

[23]图 2 是本说明书一个实施例所应用的系统架构的示意图。

[24]图 3 是本说明书一个实施例在运营商服务器中实现一键登录业务的方法的流程图。

[25]图 4 是本说明书一个实施例在应用客户端中实现一键登录业务的方法的流程图。

[26]图 5 是本说明书一个实施例在应用服务器中实现一键登录业务的方法的流程图。

[27]图 6 是本说明书一个实施例中运营商服务器、应用客户端及应用服务器配合实现一键登录业务的方法的流程图。

[28]图 7 是本说明书一个实施例中一键登录业务的装置的结构示意图。

[29]图 8 是本说明书另一个实施例中一键登录业务的装置的结构示意图。

[30]图 9 是本说明书又一个实施例中一键登录业务的装置的结构示意图。

具体实施方式

[31]下面结合附图，对本说明书提供的方案进行描述。

[32]为了方便对本说明书提供的方法进行理解，首先对本说明书所涉及和适用的系统架构进行描述。如图 2 中所示，该系统架构中主要包括三个网络节点：应用客户端、应用服务器和运营商服务器。

[33]其中，应用客户端安装并运行于终端设备中，终端设备可以包括但不限于诸如：智能移动终端、智能家居设备、网络设备、可穿戴式设备、智能医疗设备、PC（个人计算机）等。其中智能移动终端可以包括诸如手机、平板电脑、笔记本电脑、PDA（个人数字助理）、互联网汽车等。智能家居设备可以包括智能家电设备，诸如智能电视、智能空调、智能热水器、智能冰箱、智能空气净化器等等，智能家居设备还可以包括智能门锁、智能插座、智能电灯、智能摄像头等。网络设备可以包括诸如交换机、无线 AP、服务器等。可穿戴式设备可以包括诸如智能手表、智能眼镜、智能手环、虚拟

现实设备、增强现实设备、混合现实设备（即可以支持虚拟现实和增强现实的设备）等等。智能医疗设备可以包括诸如智能体温计、智能血压仪、智能血糖仪等等。

[34]应用客户端可以是各种类型的应用，包括但不限于诸如支付类应用、多媒体播放类应用、地图类应用、文本编辑类应用、金融类应用、浏览器类应用、即时通信类应用等等。

[35]运营商服务器指的是提供网络服务的供应商的服务端设备，可以是单一服务器，也可以是多个服务器构成的服务器群组。运营商服务器负责为各类应用提供网络服务，例如安全认证、提供一键登录的手机号等。

[36]应用服务器是一种具体应用的服务器，专门为应用客户端提供对应的应用服务，比如对于支付宝这种应用客户端，应用服务器则是提供支付宝业务的服务器。

[37]应该理解，图 2 中的应用客户端、应用服务器、运营商服务器的数目仅仅是示意性的。根据实现需要，可以选择和布设任意数目。

[38]参见图 2，应用客户端、应用服务器以及运营商服务器通过网络交互。其中，网络可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等。

[39]因为本说明书提供的一键登录业务的实现方法涉及到图 2 中所示的 3 种网络节点，因此，下面通过不同的实施例分别说明运营商服务器、应用客户端以及应用服务器在一键登录业务中的处理。

[40]首先，说明运营商服务器在一键登录业务中的处理。

[41]图 3 是本说明书一个实施例在运营商服务器中实现一键登录业务的方法的流程图。参见图 3，该方法包括以下步骤。

[42]步骤 301：从应用客户端发来的校验请求中获取第一 IP 地址的信息。

[43]步骤 303：向所述应用客户端下发令牌 token。

[44]步骤 305：从应用服务器发来的号码获取请求中获取第二 IP 地址的信息。

[45]步骤 307：判断所述第一 IP 地址与所述第二 IP 地址是否相同，如果相同，执行步骤 309，如果不相同，执行步骤 311。

[46]步骤 309：根据号码获取请求中携带的 token 获取应用客户端所在的终端设备的手机号，并发送给所述应用服务器。

[47]步骤 311: 拒绝将该终端设备的手机号发送给所述应用服务器。

[48]在现有的一键登录业务中, 会出现诸如如下情况: 一个攻击者利用自己的终端设备 X 盗取了下发给应用客户端的 token, 之后, 攻击者通过终端设备 X 仿冒该应用客户端所在的终端设备 Y 向应用服务器发送 token, 因为所利用的 token 正确, 应用服务器可以从运营商服务器处拿到应用客户端所在的终端设备 Y 的手机号, 从而导致应用服务器误认为发来 token 的终端设备 X 就是应用客户端所在的终端设备 Y, 即认为攻击者就是应用客户端的合法用户, 从而向攻击者提供对应的应用服务, 比如播放该合法用户才有权观看的视频资料或者完成转账等, 从而对用户的使用带来了安全问题, 并可能会造成用户隐私数据的泄露。

[49]而根据上述图 3 所示的过程可以看出, 运营商服务器会在下发 token 之前获取应用客户端发来的第一 IP 地址 (该第一 IP 地址对应的是: 在下发 token 之前, 向运营商服务器请求一键登录的终端设备的 IP 地址, 比如记为终端设备 Y 的 IP 地址), 在下发 token 之后获取应用服务器发来的第二 IP 地址 (该第二 IP 地址对应的是: 在下发 token 之后, 通过应用服务器请求一键登录的终端设备的 IP 地址), 如果该两个 IP 地址相同, 就可以认为在一次一键登录业务中, 下发 token 之前与运营商服务器通信的终端设备与下发 token 之后与应用服务器通信的终端设备是同一个终端设备, 都是终端设备 Y, 也就是说, 当前与应用服务器进行一键登录业务的终端设备 (即向应用服务器发送 token 的终端设备) 是合法用户使用的终端设备 Y, 下发的 token 没有被攻击者盗取, 没有发生攻击行为, 因此运营商服务器可以向应用服务器提供应用客户端所在的终端设备 Y 的手机号码, 从而使得应用服务器为其当前连接的终端设备 Y 提供对应的应用服务; 相反, 如果该两个 IP 地址不相同, 就可以认为在一次一键登录业务中, 下发 token 之前与运营商服务器通信的终端设备 Y 与下发 token 之后与应用服务器通信的终端设备 X 不是同一个终端设备, 也就是说, 当前与应用服务器连接的终端设备 X 不是合法用户使用的终端设备 Y, 而是盗取了 token 的一个攻击者使用的终端设备 X, 已经发生了攻击行为, 因此运营商服务器不向应用服务器提供应用客户端所在的终端设备 Y 的手机号码, 从而使得应用服务器无法为其当前连接的攻击者的终端设备 X 提供对应的应用服务。可见, 本说明书实施例的方法避免了应用服务器为攻击者的终端设备提供应用客户端对应的应用服务, 提高了安全性。

[50]下面结合具体的实施例对图 3 所示的过程进行说明。

[51]首先对于步骤 301: 运营商服务器从应用客户端发来的校验请求中获取第一 IP 地址

的信息。

[52]可以理解，应用客户端是通过其所在的终端设备 Y 向运营商服务器发送校验请求的，该校验请求中会携带终端设备 Y 的 IP 地址，记为第一 IP 地址。

[53]携带第一 IP 地址的校验请求可以包括如下中的任意一种或者多种：校验请求 1：在一键登录业务中，在运营商服务器下发 token 之前，应用客户端会向运营商服务器发送登录校验请求，以便对应用客户端的身份进行验证。因此，可以利用该登录校验请求携带所在终端设备的 IP 地址，并发送给运营商服务器，相应地，本步骤 301 中的校验请求可以是携带 APP ID、APP sign，KEY ID、时间戳以及第一 IP 地址的登录校验请求。

[54]校验请求 2：在一键登录业务中，在运营商服务器下发 token 之前，应用客户端会向运营商服务器发送手机身份校验请求，以便对应用客户端所在的终端设备的身份进行验证。因此，可以利用该手机身份校验请求携带第一 IP 地址，并发送给运营商服务器，相应地，本步骤 301 中的校验请求可以是携带 APP ID、第一 IP 地址及时间戳的手机身份校验请求。

[55]校验请求 3：在运营商服务器下发 token 之前，应用客户端可以利用新定义的一个校验请求将第一 IP 地址发送给运营服务器，相应地，本步骤 301 中的校验请求可以是携带 APP ID 及第一 IP 地址的新定义的校验请求。

[56]较佳地，步骤 301 中的校验请求采用上述的校验请求 2，即携带 APP ID、第一 IP 地址及时间戳的手机身份校验请求。此时为了提高安全性，避免终端设备 Y 的第一 IP 地址及其他信息的泄露，可以进行加密处理，具体为：在步骤 301 之前，运营商服务器会通过 https 链路接收所述应用客户端发来的登录验证请求，在登录验证成功后，运营商服务器生成对称密钥 key，通过 https 链路将该对称密钥 key 下发给所述应用客户端；这样，应用客户端会利用对称密钥 key 对携带 APP ID、第一 IP 地址及时间戳的手机身份校验请求进行加密，然后再将加密后的手机身份校验请求发送给运营商服务器；相应地，步骤 301 的一种实现过程包括：运营商服务器利用对称密钥 key 对应用客户端发来的手机身份校验请求进行解密，从解密后的手机身份校验请求中获取所述第一 IP 地址的信息。

[57]接下来对于步骤 303：运营商服务器向所述应用客户端下发令牌 token。

[58]这里，运营商服务器在接收到手机身份校验请求后，会根据手机身份校验请求进行

身份验证，在身份验证成功后，向所述应用客户端下发 token。

[59]如前所述，如果运营商服务器生成了对称密钥 key，那么，本步骤 303 中，运营商服务器利用对称密钥 key 对 token 进行加密，将加密后的 token 下发给应用客户端，从而尽可能地避免 token 泄露。

[60]应用客户端获取了 token 之后，如果已被加密，则可以利用预先获取的对称密钥 key 进行解密，获得 token。在应用客户端获得了 token 之后，应用客户端则可以将该 token 发送给应用服务器，同时，为了后续的合法性校验，应用客户端同时将所在的终端设备的 IP 地址记为第二 IP 地址也发送给应用服务器。应用服务器将接收到的 token 及第二 IP 地址携带在号码获取请求中发送给运营商服务器。

[61]接下来对于步骤 305：从应用服务器发来的号码获取请求中获取第二 IP 地址的信息。

[62]执行到本步骤时，运营商服务器则从应用客户端及应用服务器两方获取了两个 IP 地址。

[63]接下来在步骤 307 至步骤 311 中，如前所述，运营商服务器判断该两个 IP 地址是否相同，如果相同，就可以认为在一次一键登录业务中，下发 token 之前与运营商服务器通信的终端设备与在下发 token 之后与应用服务器通信的终端设备是同一个终端设备，都是终端设备 Y，也就是说，当前与应用服务器进行一键登录业务的终端设备是合法用户使用的终端设备 Y，因此运营商服务器可以向应用服务器提供应用客户端所在的终端设备 Y 的手机号码，从而使得应用服务器为其当前连接的终端设备 Y 提供对应的应用服务；相反，如果该两个 IP 地址不相同，就可以认为在一次一键登录业务中，下发 token 之前与运营商服务器通信的终端设备 Y 与在下发 token 之后与应用服务器通信的终端设备 X 不是同一个终端设备，也就是说，当前与应用服务器连接的终端设备 X 不是合法用户使用的终端设备 Y，而是盗取了 token 的一个攻击者使用的终端设备 X，已经发生了攻击行为，因此运营商服务器不向应用服务器提供应用客户端所在的终端设备 Y 的手机号码，从而使得应用服务器无法为其当前连接的终端设备 X 提供对应的应用服务。可见，本说明书实施例的方法避免了应用服务器为攻击者的终端设备提供应用客户端对应的应用服务，提高了安全性。

[64]需要说明的是，在本说明书的实施例中，IP 地址可以是 IPv4（Internet Protocol Version 4，互联网协议第 4 版）地址以及 IPv6（Internet Protocol Version 6，互联网协议第 6 版）地址中的任意一个或者两个。

[65]在本说明书实施例中，应用客户端可以通过专有链路与应用服务器进行通信，在获得对称密钥之前应用客户端可以通过 https 链路与应用服务器进行通信，在获得对称密钥之后应用客户端可以通过 http 链路与应用服务器进行通信，应用服务器可以通过 https 链路与应用服务器进行通信。

[66]下面说明应用客户端在一键登录业务中的处理。

[67]图 4 是本说明书一个实施例在应用客户端中实现一键登录业务的方法的流程图。参见图 4，该方法包括：步骤 401：将所在终端设备的 IP 地址的信息携带在校验请求中，并将该校验请求发送给运营服务器。

[68]本步骤 401 的具体实现的说明可以参见上述对步骤 301 的所有说明。

[69]比如，步骤 401 的校验请求包括如下中的至少一个请求：携带 APP ID、APP sign，KEY ID、时间戳以及所述 IP 地址的登录验证请求；携带 APP ID、所述 IP 地址及时间戳的手机身份校验请求；携带 APP ID 及所述 IP 地址的新定义的校验请求。

[70]再如，在一种较佳的实现方式中，校验请求为携带 APP ID、所在终端设备的 IP 地址的信息及时间戳的手机身份校验请求。此时，在将手机身份校验请求发送给运营服务器之前，进一步包括：应用客户端通过 https 链路向运营服务器发送登录验证请求，通过 https 链路接收运营服务器下发的对称密钥；本步骤 401 中，应用客户端利用对称密钥对手机身份校验请求进行加密，将加密后的手机身份校验请求发送给运营服务器；步骤 403：接收运营服务器下发的 token。

[71]本步骤 403 的具体实现的说明可以参见上述对步骤 303 的所有说明。比如，应用客户端接收运营服务器下发的加密后的 token，利用对称密钥对该加密后的 token 进行解密，得到 token。

[72]步骤 405：将所在终端设备的 IP 地址的信息及接收到的 token 发送给应用服务器。

[73]为了能够在运营服务器中进行合法性验证，应用客户端在向应用服务器发送 token 时，需要同时携带该应用客户端所在的终端设备的 IP 地址。

[74]步骤 407：如果接收到应用服务器发来的登录授权，则一键登录成功，如果未接收到应用服务器发来的登录授权，则一键登录失败。

[75]下面说明应用服务器在一键登录业务中的处理。

[76]图 5 是本说明书一个实施例在应用服务器中实现一键登录业务的方法的流程图。参

见图 5，该方法包括：步骤 501：接收应用客户端发来的登录请求，进行登录预授权。

[77]当一个应用客户端需要使用一键登录业务时，首先会向应用服务器发送登录请求，从而触发启动一键登录业务。应用服务器则会进行登录预授权处理，比如发送预登录界面给应用客户端。之后，应用客户端则会执行上述步骤 401 至步骤 405，具体可以参见对步骤 401 至步骤 405 的所有相关说明。

[78]步骤 503：接收应用客户端发来的 token 及该应用客户端所在的终端设备的 IP 地址的信息。

[79]这里，如果 token 未被攻击者盗取，那么步骤 503 中与应用服务器通信的终端设备与步骤 501 中的终端设备就是同一个终端设备，比如记为终端设备 Y，那么，步骤 503 中，应用服务器接收到的就是终端设备 Y 的 IP 地址。

[80]相反，如果 token 被攻击者盗取，那么步骤 503 中与应用服务器通信的终端设备与步骤 501 中的终端设备就不是同一个终端设备，比如本步骤 503 中通信的终端设备记为终端设备 X，那么，步骤 503 中，应用服务器接收到的就是终端设备 X 的 IP 地址。

[81]步骤 505：将接收到的 token 以及 IP 地址的信息携带在号码获取请求中，并将该号码获取请求发送给运营商服务器。

[82]本步骤 505 中，应用服务器可以通过 https 链路将所述号码获取请求发送给运营商服务器。

[83]运营商服务器接收到号码获取请求之后的处理可以参见上述对步骤 305 至步骤 311 的所有说明。

[84]步骤 507：如果接收到运营商服务器发来的应用客户端所在的终端设备的手机号，则根据该手机号进行登录授权处理。

[85]下面结合应用客户端、应用服务器以及运营商服务器三者的配合处理，来说明一键登录业务的实现方法，在该方法中，在运营商服务器下发 token 之前，以应用客户端通过上述的校验请求 2 即手机身份校验请求携带终端设备的 IP 地址为例进行说明，参见图 6，该方法包括如下步骤。

[86]步骤 601：应用客户端通过专有链路向自己所属的应用服务器发送登录请求。

[87]本步骤 601 中，应用客户端即安装在终端设备中的应用程序（APP）。应用客户端可以是在受到用户的触发后，执行本步骤中发送登录请求的处理。

[88]应用客户端与应用服务器之间存在专有链路，因此可以通过该专有链路而不是公网发送登录请求。

[89]步骤 603：应用服务器接收到登录请求后，进行登录预授权，包括通过专有链路向该应用客户端发送预登录界面。

[90]步骤 605：应用服务器通过 https 链路向运营商服务器发送登录验证请求。

[91]这里，https 链路是一种加密链路，通过该 https 链路发送登录验证请求可以进一步提高安全性。

[92]本步骤 605 中，登录验证请求中可以包括应用客户端的标识（APP ID）、应用客户端的签名（APP sign），密钥标识符（KEY ID）以及时间戳等信息。

[93]步骤 607：运营商服务器根据接收到的登录验证请求对应用客户端的身份进行认证，认证成功后会生成一个会话密钥 key，通过 https 链路向应用客户端发送 key。

[94]这里，key 是一个对称密钥。

[95]步骤 609：应用客户端生成携带 APP ID、所在的终端设备的 IP 地址和时间戳的手机身份校验请求，用对称密钥 key 加密后，通过 http 链路发送给运营商服务器。

[96]这里，手机身份校验请求中携带的应用客户端所在的终端设备的 IP 地址可以包括 IPv4 地址以及 IPv6 地址。

[97]步骤 611：运营商服务器利用 key 解密手机身份校验请求，进行身份验证，在身份验证成功后，从该手机身份校验请求中获取第一 IP 地址的信息，利用对称密钥 key 加密 token，并向应用客户端下发加密后的 token。

[98]这里，运营商服务器会保存在下发 token 之前得到的应用客户端所在的终端设备的 IP 地址，记为第一 IP 地址。

[99]步骤 613：应用客户端利用对称密钥解密出 token 之后，通过专有链路将该 token 以及所在的终端设备的 IP 地址发送给应用服务器。

[100]步骤 615：应用服务器将 APP ID、接收到的 token 以及 IP 地址携带在号码获取请求中通过 https 链路发送给运营商服务器。

[101]步骤 617：运营商服务器判断应用服务器发来的 IP 地址记为第二 IP 地址与之前获取的第一 IP 地址是否相同，如果相同，则通过 https 链路将从网关处查询到的终端设备的手机号码发送给应用服务器，否则，本次一键登录失败。

[102]比如，一键登录失败时，运营商服务器向应用服务器返回取号失败消息。

[103]步骤 619：应用服务器如果接收到运营商服务器发来的应用客户端所在的终端设备的手机号，则根据该手机号并通过专有链路向应用客户端进行登录成功授权处理。

[104]在本说明书的一个实施例中，提供了一键登录业务的实现装置，设置于运营商服务器中，参见图 7，包括：第一 IP 地址获取模块 701，配置为从应用客户端发来的校验请求中获取第一 IP 地址的信息；令牌下发模块 702，配置为向所述应用客户端下发 token；第二 IP 地址获取模块 703，配置为从应用服务器发来的号码获取请求中获取第二 IP 地址的信息；授权处理模块 704，配置为判断所述第一 IP 地址与所述第二 IP 地址是否相同，如果相同，则根据所述号码获取请求中携带的 token 获取应用客户端所在的终端设备的手机号，并发送给所述应用服务器，如果不相同，则拒绝将该终端设备的手机号发送给所述应用服务器。

[105]在本说明书一个实施例中，第一 IP 地址获取模块 701 被配置为执行从下述的任意一种或多种请求中获取第一 IP 地址：携带 APP ID、APP sign，KEY ID、时间戳以及所述第一 IP 地址的登录验证请求；以及携带 APP ID、所述第一 IP 地址及时间戳的手机身份校验请求；以及携带 APP ID 及所述第一 IP 地址的新定义的校验请求。

[106]在本说明书一个实施例中，所述校验请求为携带 APP ID、第一 IP 地址信息及时间戳的手机身份校验请求；第一 IP 地址获取模块 701 被配置为执行从该手机身份校验请求中获取第一 IP 地址的信息；令牌下发模块 702 被配置执行：根据手机身份校验请求进行身份验证，在身份验证成功后，向所述应用客户端下发 token。

[107]在本说明书一个实施例中，应用于运营商服务器中的一键登录业务的实现装置进一步包括：登录验证模块，配置为通过 https 链路接收应用客户端发来的登录验证请求，根据登录验证请求进行登录验证；密钥生成模块，配置为在登录验证模块验证成功后，生成对称密钥，通过 https 链路将该对称密钥下发给所述应用客户端；第一 IP 地址获取模块 701 被配置为执行利用生成的所述对称密钥对应用客户端发来的手机身份校验请求进行解密，从解密后的手机身份校验请求中获取所述第一 IP 地址的信息；令牌下发模块 702 被配置执行：利用对称密钥对 token 进行加密，将加密后的 token 下发给应用客户端。

[108]在本说明书的一个实施例中，提供了一键登录业务的实现装置，设置于应用客户端中，参见图 8，包括：校验请求模块 801，配置为将所在的终端设备的 IP 地址的信

息携带在校验请求中，并将该校验请求发送给运营商服务器；令牌接收模块 802，配置为接收运营商服务器下发的 token；转发模块 803，配置为将所在的终端设备的 IP 地址的信息及接收到的 token 发送给应用服务器；登录授权模块 804，配置为如果接收到应用服务器发来的登录授权，则一键登录成功。

[109]在本说明书的一个实施例中，校验请求模块 801 被配置为将如下中的任意一种或者多种请求发送给运营商服务器：携带 APP ID、APP sign，KEY ID、时间戳以及所述第一 IP 地址的登录验证请求；以及携带 APP ID、所述第一 IP 地址及时间戳的手机身份校验请求；以及携带 APP ID 及所述第一 IP 地址的新定义的校验请求。

[110]在本说明书的一个实施例中，当校验请求模块 801 发送的是携带 APP ID、所述第一 IP 地址及时间戳的手机身份校验请求时，应用于应用客户端的一键登录业务的实现装置中进一步包括：登录请求模块，配置为通过 https 链路向运营商服务器发送登录验证请求，通过 https 链路接收运营商服务器下发的对称密钥；校验请求模块 801 被配置为利用所述对称密钥对手机身份校验请求进行加密，将加密后的手机身份校验请求发送给运营商服务器；令牌接收模块 802 被配置为执行：接收运营商服务器下发的加密后的 token，利用对称密钥对该加密后的 token 进行解密，得到 token。

[111]在本说明书的一个实施例中，提供了一键登录业务的实现装置，设置于应用服务器中，参见图 9，包括：预登录模块 901，配置为在接收到应用客户端发来的登录请求之后，进行登录预处理；网络因子获取模块 902，配置为接收应用客户端发来的 token 以及该应用客户端所在的终端设备的 IP 地址的信息；号码获取模块 903，配置为将接收到的 token 以及所述 IP 地址的信息携带在号码获取请求中，并将该号码获取请求发送给运营商服务器；授权执行模块 904，配置为如果接收到运营商服务器发来的应用客户端所在的终端设备的手机号，则根据该手机号进行登录授权处理。

[112]在本说明书一个实施例中，号码获取模块 903 被配置为通过 https 链路将所述号码获取请求发送给运营商服务器；授权执行模块 904 被配置为通过 https 链路接收运营商服务器发来的应用客户端所在的终端设备的手机号。

[113]本说明书一个实施例提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行说明书中任一个实施例中的方法。

[114]本说明书一个实施例提供了一种计算设备，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，实现执行说明书中任一个实

施例中的方法。

[115]可以理解的是，本说明书实施例示意的结构并不构成对本说明书实施例的装置的具体限定。在说明书的另一些实施例中，上述装置可以包括比图示更多或者更少的部件，或者组合某些部件，或者拆分某些部件，或者不同的部件布置。图示的部件可以以硬件、软件或者软件和硬件的组合来实现。

[116]上述装置、系统内的各模块之间的信息交互、执行过程等内容，由于与本说明书方法实施例基于同一构思，具体内容可参见本说明书方法实施例中的叙述，此处不再赘述。

[117]本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[118]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、挂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。

[119]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、一键登录业务的实现方法，其中包括：

从应用客户端发来的校验请求中获取第一 IP 地址的信息；

向所述应用客户端下发令牌 token；

从应用服务器发来的号码获取请求中获取第二 IP 地址的信息；

判断所述第一 IP 地址与所述第二 IP 地址是否相同，如果相同，则根据所述号码获取请求中携带的 token 获取应用客户端所在的终端设备的手机号，并发送给所述应用服务器，如果不相同，则拒绝将该终端设备的手机号发送给所述应用服务器。

2、根据权利要求 1 所述的方法，其中，所述校验请求包括如下中的至少一个请求：

携带 APP ID、APP sign，KEY ID、时间戳以及所述第一 IP 地址的登录验证请求；

携带 APP ID、所述第一 IP 地址及时间戳的手机身份校验请求；

携带 APP ID 及所述第一 IP 地址的新定义的校验请求。

3、根据权利要求 2 所述的方法，其中，当所述校验请求包括携带 APP ID、第一 IP 地址信息及时间戳的手机身份校验请求时，

在获取第一 IP 地址的信息之前，进一步包括：通过 https 链路接收所述应用客户端发来的登录验证请求，在登录验证成功后，生成对称密钥，通过 https 链路将该对称密钥下发给所述应用客户端；

所述获取第一 IP 地址的信息，包括：利用生成的所述对称密钥对应用客户端发来的手机身份校验请求进行解密，从解密后的手机身份校验请求中获取所述第一 IP 地址的信息；

所述向所述应用客户端下发令牌 token，包括：利用对称密钥对 token 进行加密，将加密后的 token 下发给应用客户端。

4、一键登录业务的实现方法，该方法包括：

将终端设备的 IP 地址的信息携带在校验请求中，并将该校验请求发送给运营商服务器；

接收运营商服务器下发的 token；

将终端设备的 IP 地址的信息及接收到的 token 发送给应用服务器；

如果接收到应用服务器发来的登录授权，则一键登录成功。

5、根据权利要求 4 所述的方法，其中，所述校验请求包括如下中的至少一个请求：

携带 APP ID、APP sign，KEY ID、时间戳以及所述 IP 地址的登录验证请求；

携带 APP ID、所述 IP 地址及时间戳的手机身份校验请求；

携带 APP ID 及所述 IP 地址的新定义的校验请求。

6、根据权利要求 5 所述的方法，其中，当所述校验请求为携带 APP ID、所述 IP 地址及时间戳的手机身份校验请求时，

在将手机身份校验请求发送给运营商服务器之前，进一步包括：通过 https 链路向运营商服务器发送登录验证请求，通过 https 链路接收运营商服务器下发的对称密钥；

所述将该校验请求发送给运营商服务器，包括：利用所述对称密钥对手机身份校验请求进行加密，将加密后的手机身份校验请求发送给运营商服务器；

所述接收运营商服务器下发的 token，包括：接收运营商服务器下发的加密后的 token，利用对称密钥对该加密后的 token 进行解密，得到 token。

7、一键登录业务的实现方法，该方法包括：

接收应用客户端发来的登录请求，进行登录预授权；

接收应用客户端发来的 token 及该应用客户端所在的终端设备的 IP 地址的信息；

将接收到的 token 以及所述 IP 地址的信息携带在号码获取请求中，并将该号码获取请求发送给运营商服务器；

如果接收到运营商服务器发来的应用客户端所在的终端设备的手机号，则根据该手机号进行登录授权处理。

8、根据权利要求 7 所述的方法，其中，通过 https 链路与运营商服务器进行信息交互。

9、一键登录业务的实现装置，包括：

第一 IP 地址获取模块，配置为从应用客户端发来的校验请求中获取第一 IP 地址的信息；

令牌下发模块，配置为向所述应用客户端下发 token；

第二 IP 地址获取模块，配置为从应用服务器发来的号码获取请求中获取第二 IP 地址的信息；

授权处理模块，配置为判断所述第一 IP 地址与所述第二 IP 地址是否相同，如果相同，则根据所述号码获取请求中携带的 token 获取应用客户端所在的终端设备的手机号，并发送给所述应用服务器，如果不相同，则拒绝将该终端设备的手机号发送给所述应用服务器。

10、一键登录业务的实现装置，包括：

校验请求模块，配置为将所在的终端设备的 IP 地址的信息携带在校验请求中，并将该校验请求发送给运营商服务器；

令牌接收模块，配置为接收运营商服务器下发的 token；

转发模块，配置为将所在的终端设备的 IP 地址的信息及接收到的 token 发送给应用服务器；

登录授权模块，配置为如果接收到应用服务器发来的登录授权，则一键登录成功。

11、一键登录业务的实现装置，包括：

预登录模块，配置为在接收到应用客户端发来的登录请求之后，进行登录预授权；

网络因子获取模块，配置为接收应用客户端发来的 token 以及该应用客户端所在的终端设备的 IP 地址的信息；

号码获取模块，配置为将接收到的 token 以及所述 IP 地址的信息携带在号码获取请求中，并将该号码获取请求发送给运营商服务器；

授权执行模块，配置为如果接收到运营商服务器发来的应用客户端所在的终端设备的手机号，则根据该手机号进行登录授权处理。

12、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，实现权利要求 1-8 中任一项所述的方法。