

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 12 月 22 日 (22.12.2016)



(10) 国际公布号
WO 2016/202207 A1

- (51) 国际专利分类号:
G06F 21/62 (2013.01)
- (21) 国际申请号: PCT/CN2016/085216
- (22) 国际申请日: 2016 年 6 月 8 日 (08.06.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510330914.9 2015 年 6 月 15 日 (15.06.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Cayman Islands (KY)。

- (72) 发明人: 李克鹏 (LI, Kepeng); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。 李凯 (LI, Kai); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[续页]

(54) Title: METHOD AND DEVICE FOR OBTAINING ELECTRONIC DOCUMENT

(54) 发明名称: 获取电子文件的方法及装置

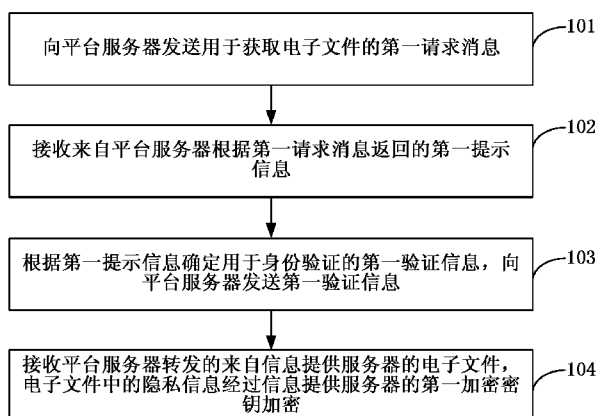


图 1

(57) Abstract: Provided are a method and device for obtaining an electronic document. A method for obtaining an electronic document comprises: sending a first request message for obtaining the electronic document to a platform server (101), wherein the first request message includes a first identifier of an information-providing server providing the electronic document; receiving first prompt information sent back from the platform server according to the first request message (102); determining, according to the first prompt information, first authentication information for authenticating identification, and sending the first authentication information to the platform server (103); and receiving the electronic document provided from the information-providing server and forwarded by the platform server, wherein private information in the electronic document is encrypted by a first encryption key of the information-providing server (104). Thus, private information of a user can be effectively prevented from leaking out via the platform server, thereby ensuring privacy security of the user.

(57) 摘要:

[续页]

- 101 Send a first request message for obtaining an electronic document to a platform server
- 102 Receive first prompt information sent back from the platform server according to the first request message
- 103 Determine, according to the first prompt information, first authentication information for authenticating identification, and send the first authentication information to the platform server
- 104 Receive the electronic document provided from the information-providing server and forwarded by the platform server, wherein private information in the electronic document is encrypted by a first encryption key of the information-providing server



WO 2016/202207 A1



(84) **指定国** (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ,

CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种获取电子文件的方法及装置, 该获取电子文件的方法包括: 向平台服务器发送用于获取电子文件的第一请求消息(101), 第一请求消息中携带有提供电子文件的信息提供服务器的第一标识; 接收来自平台服务器根据第一请求消息返回的第一提示信息(102); 根据第一提示信息确定用于身份验证的第一验证信息, 向平台服务器发送第一验证信息(103); 接收平台服务器转发的来自信息提供服务器的电子文件, 电子文件中的隐私信息经过信息提供服务器的第一加密密钥加密(104)。可以有效地保护用户的隐私信息不被平台服务器泄露, 确保用户的隐私安全。

获取电子文件的方法及装置

本申请要求 2015 年 06 月 15 日递交的申请号为 201510330914.9、发明名称为“获取电子文件的方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请涉及信息技术领域，尤其涉及一种获取电子文件的方法及装置。

背景技术

10

为了加强处方药的流通管理，保证民众用药安全、有效，处方药的销售需要依据医生开具的纸质处方才可以销售。目前国家正逐渐放开在线销售处方药，以进一步降低国家和民众的医疗成本、提高药品采购的便利性。电子处方相对于纸质处方，具有格式规范、内容全面清晰、便于医患查询历史记录等优点，是规模推广处方药在线销售的基础。

15

为保护电子处方中涉及到的患者的隐私信息，在使用电子处方的流程中，将患者的姓名、病历号、住址等患者隐私信息进行隐藏、删除或加解密处理。但电子处方在使用过程中会涉及不同的用户角色，例如，医生、患者、药房等，此外，医生在核对患者既往诊疗信息时、监管部门在进行案例审查时，还需要核对电子处方中涉及到的患者身份。因此单纯的隐藏或删除患者的身份信息，会因为丢失患者的关键信息而无法追溯患者的既往就诊记录。

20

发明内容

有鉴于此，本申请提供一种新的技术方案，可以解决现有技术中不能有效地保护用户的隐私信息的技术问题。

为实现上述目的，本申请提供技术方案如下：

25

根据本申请的第一方面，提出了一种获取电子文件的方法，应用在终端设备上，包括：

向平台服务器发送用于获取电子文件的第一请求消息，所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识；

接收来自所述平台服务器根据所述第一请求消息返回的第一提示信息；

30

根据所述第一提示信息确定用于身份验证的第一验证信息，向所述平台服务器发送

所述第一验证信息；

在所述平台服务器根据所述第一标识确定所述信息提供服务器，以及根据所述终端设备的用户在所述平台服务器的第一登录信息确定所述用户在所述信息提供服务器注册的用户标识，并将所述第一验证信息、所述用户标识发送至所述信息提供服务器后，接收所述平台服务器转发的来自所述信息提供服务器的所述电子文件，所述电子文件中的隐私信息经过所述信息提供服务器的第一加密密钥加密。

根据本申请的第二方面，提出了一种获取电子文件的方法，应用在平台服务器上，包括：

接收来自终端设备的用于获取电子文件的第一请求消息，所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识；

根据所述第一请求消息向所述终端设备返回第一提示信息；

在所述终端设备根据所述第一提示信息确定用于身份验证的第一验证信息后，接收来自所述终端设备的第一验证信息；

根据所述第一标识确定所述信息提供服务器，将所述第一验证信息、所述终端设备的用户在所述信息提供服务器注册的用户标识发送至所述信息提供服务器；

在所述信息提供服务器对所述第一验证信息验证通过并根据所述用户标识确定所述电子文件后，接收来自所述信息提供服务器的所述电子文件，将所述电子文件转发至所述终端设备，所述电子文件中的隐私信息经过所述信息提供服务器的第一加密密钥加密。

根据本申请的第三方面，提出了一种获取电子文件的方法，应用在信息提供服务器上，包括：

接收来自平台服务器的第一验证信息、终端设备的用户在所述信息提供服务器注册的用户标识；

对所述第一验证信息进行验证，在验证通过后根据所述用户标识确定所述电子文件；将所述电子文件中的隐私信息通过所述信息提供服务器的第一加密密钥加密；

将所述电子文件发送至所述平台服务器，以供所述平台服务器将所述电子文件转发至所述终端设备。

根据本申请的第四方面，提出了一种获取电子文件的装置，应用在终端设备上，包括：

第一发送模块，用于向平台服务器发送用于获取电子文件的第一请求消息，所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识；

第一接收模块，用于接收来自所述平台服务器根据所述第一发送模块发送的所述第一请求消息返回的第一提示信息；

第一确定模块，用于根据所述第一接收模块接收到的所述第一提示信息确定用于身份验证的第一验证信息，向所述平台服务器发送所述第一验证信息；

5 第二接收模块，用于在所述平台服务器根据所述第一标识确定所述信息提供服务器，以及根据所述终端设备的用户在所述平台服务器的第一登录信息确定所述用户在所述信息提供服务器注册的用户标识，并将所述第一确定模块确定的所述第一验证信息、所述用户标识发送至所述信息提供服务器后，接收所述平台服务器转发的来自所述信息提供服务器的所述电子文件，所述电子文件中的隐私信息经过所述信息提供服务器的第一加
10 密密钥加密。

根据本申请的第五方面，提出了一种获取电子文件的装置，应用在平台服务器上，包括：

第九接收模块，用于接收来自终端设备的用于获取电子文件的第一请求消息，所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识；

15 第七发送模块，用于根据所述第九接收模块接收到的所述第一请求消息向所述终端设备返回第一提示信息；

第八发送模块，用于在所述终端设备根据所述第七发送模块发送的所述第一提示信息确定用于身份验证的第一验证信息后，接收来自所述终端设备的第一验证信息；

第九发送模块，用于根据所述第九接收模块接收到的所述第一标识确定所述信息提供服务器，将所述第一验证信息、所述终端设备的用户在所述信息提供服务器注册的用户标识发送至所述信息提供服务器；
20

第一转发模块，用于在所述信息提供服务器对所述第九发送模块发送的所述第一验证信息验证通过并根据所述用户标识确定所述电子文件后，接收来自所述信息提供服务器的所述电子文件，将所述电子文件转发至所述终端设备，所述电子文件中的隐私信息
25 经过所述信息提供服务器的第一加密密钥加密。

根据本申请的第六方面，提出了一种获取电子文件的装置，应用在信息提供服务器上，包括：

第十六接收模块，用于接收来自平台服务器的第一验证信息、终端设备的用户在所述信息提供服务器注册的用户标识；

30 第三验证模块，用于对所述第十六接收模块接收到的所述第一验证信息进行验证，

在验证通过后根据所述用户标识确定所述电子文件；

第三加密模块，用于将所述电子文件中的隐私信息通过所述信息提供服务器的第一加密密钥加密；

第十五发送模块，用于将所述第三加密模块加密后的所述电子文件发送至所述平台服务器，以供所述平台服务器将所述电子文件转发至所述终端设备。

由以上技术方案可见，本申请通过对电子文件中的隐私信息通过第一加密密钥进行加密保护，由于平台服务器并没有信息提供服务器的第一加密密钥，因此即使电子文件在平台服务器时被窃取，窃取者也无法得到用户的真实的隐私信息，平台服务器侧的管理员也无法获取到用户的真实的隐私信息，从而有效地保护用户的隐私信息不被平台服务器泄露，确保用户的隐私安全。

附图说明

图 1 是根据一示例性实施例一示出的获取电子文件的方法的流程图；
图 2 是根据一示例性实施例二示出的获取电子文件的方法的流程图；
图 3 是根据一示例性实施例三示出的获取电子文件的方法的流程图；
图 4 是根据一示例性实施例四示出的获取电子文件的方法的流程图；
图 5 是根据又一示例性实施例一示出的获取电子文件的方法的流程图；
图 6 是根据又一示例性实施例二示出的获取电子文件的方法的流程图；
图 7 是根据又一示例性实施例三示出的获取电子文件的方法的流程图；
图 8 是根据又一示例性实施例四示出的获取电子文件的方法的流程图；
图 9 是根据另一示例性实施例一示出的获取电子文件的方法的流程图；
图 10 是根据另一示例性实施例二示出的获取电子文件的方法的流程图；
图 11 是根据另一示例性实施例三示出的获取电子文件的方法的流程图；
图 12 是根据另一示例性实施例四示出的获取电子文件的方法的流程图；
图 13 是根据一示例性实施例示出的获取电子文件的方法的场景图之一；
图 14 是根据一示例性实施例示出的获取电子文件的方法的场景图之二；
图 15 是根据一示例性实施例示出的获取电子文件的方法的场景图之三；
图 16 是根据一示例性实施例示出的获取电子文件的方法的场景图之四；
图 17 示出了根据本发明的一示例性实施例的终端设备的结构图；
图 18 示出了根据本发明的一示例性实施例的平台服务器的结构图；

图 19 示出了根据本发明的一示例性实施例的信息提供服务器的结构图；

图 20 是根据一示例性实施例一示出的获取电子文件的装置的结构示意图；

图 21 是根据一示例性实施例二示出的获取电子文件的装置的结构示意图；

图 22 是根据又一示例性实施例一示出的获取电子文件的装置的结构示意图；

5 图 23 是根据又一示例性实施例二示出的获取电子文件的装置的结构示意图；

图 24 是根据另一示例性实施例一示出的获取电子文件的装置的结构示意图；

图 25 是根据另一示例性实施例二示出的获取电子文件的装置的结构示意图。

具体实施方式

10 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述的实施方式并不代表与本发明相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本发明的一些方面相一致的装置和方法的例子。

在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在
15 本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不
20 脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

本申请通过对电子文件中的隐私信息通过第一加密密钥进行加密保护，由于平台服务器并没有信息提供服务器的第一加密密钥，因此即使电子文件在平台服务器时被窃取，
25 窃取者也无法得到用户的真实的隐私信息，平台服务器侧的管理员也无法获取到用户的真实的隐私信息，从而有效地保护用户的隐私信息不被平台服务器泄露，确保用户的隐私安全。

为对本申请进行进一步说明，提供下列实施例：

请参考图 1，为根据一示例性实施例一示出的获取电子文件的方法的流程图，本实
30 施例可以应用在终端设备上，在一实施例中，终端设备可以为智能手机、平板电脑、个

人计算机等，可以通过在终端设备上以应用程序或者浏览器的方式与平台服务器和信息提供服务器进行通信，如图 1 所示，包括如下步骤：

步骤 101，向平台服务器发送用于获取电子文件的第一请求消息，第一请求消息中携带有提供电子文件的信息提供服务器的第一标识。

5 步骤 102，接收来自平台服务器根据第一请求消息返回的第一提示信息。

步骤 103，根据第一提示信息确定用于身份验证的第一验证信息，向平台服务器发送第一验证信息。

10 步骤 104，在平台服务器根据第一标识确定信息提供服务器，以及根据终端设备的用户在平台服务器的第一登录信息确定用户在信息提供服务器注册的用户标识，并将第一验证信息、用户标识发送至信息提供服务器后，接收平台服务器转发的来自信息提供服务器的电子文件，电子文件中的隐私信息经过信息提供服务器的第一加密密钥加密。

在上述步骤 101 中，在一实施例中，平台服务器可以作为连接终端设备与信息提供服务器的网络平台，可以由电商平台提供，不同的终端设备与不同的信息提供服务器可以通过平台服务器进行电子文件的传输。在一实施例中，电子文件可以为电子处方，信息提供服务器可以为位于医院侧的医院信息系统（Hospital Information System，简称为 HIS），平台服务器可以为位于网络侧的电子处方平台（Electronic Prescription Platform，简称为 EPP），在另一实施例中，电子文件还可以为终端设备侧的用户的社保文件，信息提供服务器可以为社保中心侧的社保服务系统，平台服务器可以为位于网络侧的社保信息平台，在再一实施例中，电子文件还可以为终端设备侧的用户的住房公积金账单，
20 信息提供服务器可以为住房公积金管理中心侧的公积金服务系统，平台服务器可以为位于网络侧的公积金信息平台，由此可知，本申请不对电子文件的具体内容进行限制，只要是需要通过本申请进行加密保护的电子文件均为本申请中的电子文件。本实施例以电子文件具体为电子处方为例进行示例性说明，在一实施例中，第一请求消息中可以携带有第一标识，此时第一标识为终端设备的用户在 HIS 对应的医院代码 HIS_ID，如果第一
25 请求消息中未携带电子处方的处方号 P_ID（本申请中的第二标识），则 HIS 可以根据电子处方的开设时间确定用户需要最新的电子处方，如果携带有第二标识，HIS 可以为用户提供第二标识对应的电子处方。

在上述步骤 102 和步骤 103 中，在一实施例中，第一验证信息可以为用户在终端设备输入的第一原始验证信息通过第一加密密钥加密生成的，第一原始验证信息例如为用户的身份证号或者身份证号的最后四位、用户的名字等等。在一实施例中，可以根据第一
30

提示信息确定用户在终端设备输入的第一原始验证信息以及确定信息提供服务器的第一加密密钥，根据第一加密密钥对第一原始验证信息进行加密，得到用于身份验证的第一验证信息，第一验证信息通过信息提供服务器的第一加密密钥加密，可以使平台服务器侧获取不到用户的原始的验证信息，例如，如果根据第一提示信息需要确定的第一验证信息为用户的身份证号，通过对身份证号以第一加密密钥进行加密后，发送至平台服务器，则平台服务器是无法获取到用户的真实的身份证号的，从而确保用户的真实的验证信息在平台服务器上保密的。

在上述步骤 104 中，在一实施例中，电子文件中的隐私信息例如可以为用户的姓名、身份证号、手机号码、家庭住址等等，通过第一加密密钥对隐私信息进行加密，从而使平台服务器不能获取到电子文件中的用户的隐私信息。在一实施例中，如果信息提供服务器采用对称加密算法，则信息提供服务器上的第一加密密钥可以与信息提供服务器的第一解密密钥相同。对称加密算法可以为 DES (Data Encryption Standard)、3DES (Triple DES)、AES (Advanced Encryption Standard) 等。如果信息提供服务器采用非对称加密算法，第一加密密钥可以为信息提供服务器的公钥，信息提供服务器的第一解密密钥则为信息提供服务器的私钥。在一实施例中，信息提供服务器的采用的非对称加密算法可以为 RSA (Rivest Shamir Adleman)、Elgamal、背包算法、Rabin、D-H (Diffie-Hellman)、椭圆曲线加密算法 (ECC) 等。

本实施例中，通过对电子文件中的隐私信息通过第一加密密钥进行加密保护，由于平台服务器并没有信息提供服务器的第一加密密钥，因此即使电子文件在平台服务器时被窃取，窃取者也无法得到用户的真实的隐私信息，平台服务器侧的管理员也无法获取到用户的真实的隐私信息，从而有效地保护用户的隐私信息不被平台服务器泄露，确保用户的隐私安全。

请参考图 2，为根据一示例性实施例二示出的获取电子文件的方法的流程图，本实施例以用户需要通过终端设备登录到平台服务器为例进行示例性说明，包括如下步骤：

步骤 201，在用户未登录到平台服务器时，确定用户的第一登录信息，通过第一登录信息登录平台服务器。

步骤 202，通过第一手机号码接收来自信息提供服务器的第一验证码，第一验证码为平台服务器根据第二手机号码指示信息提供服务器发送第一手机号码的，第二手机号码由第一加密密钥对第一手机号码加密得到。

步骤 203，将第一验证码发送给平台服务器。

步骤 204, 在平台服务器对第一验证码与来自信息提供服务器的第二验证码进行验证后, 确定用户登录成功, 接收平台服务器返回的登录成功的第一响应消息。

在上述步骤 201 中, 在一实施例中, 第一登录信息可以包括用户在平台服务器的登录名和登录密码, 其中, 登录名可以为用户的真实的第一手机号码, 通过第一加密密钥对用户的真实的第一手机号码加密, 生成第一登录信息, 用户通过加密后的手机号码登录到平台服务器, 由此, 确保平台服务器不能够获取到用户的真实的手机号码。

在上述步骤 202 和步骤 203 中, 在一实施例中, 在用户通过第一登录信息登录到平台服务器之后, 可以基于第一登录信息确定用户在平台服务器注册时提供的经过第一加密密钥加密后的第二手机号码, 在另一实施例中, 如果第一登录信息中的登录名为第二手机号码, 可以通过第一登录信息中的登录名确定第二手机号码, 由此, 平台服务器可以向信息提供服务器请求向第二手机号码对应的终端设备发送第一验证码, 信息提供服务器在接收到第二手机号码后, 通过信息提供服务器的第一解密密钥对第二手机号码解密, 得到用户在信息提供服务器注册的原始的第一手机号码, 进而通过第一手机号码向终端设备发送第一验证码。在一实施例中, 第一验证码可以为短信验证码。

在上述步骤 204 中, 在一实施例中, 信息提供服务器在向终端设备发送第一验证码时, 可以向平台服务器发送第二验证码, 终端设备再将第一验证码发送给平台服务器。因此平台服务器在对第一验证码进行验证时, 可以比较第一验证码与第二验证码的内容是否相同, 如果相同, 则验证通过, 确定用户登录成功。

本实施例中, 在用户需要登录到平台服务器时, 通过第一加密密钥对用户的真实登录信息进行加密, 并通过加密后的第一登录信息登录到平台服务器, 在平台服务器上的数据遭到泄露时, 窃取者从平台服务器窃取到的第一登录信息是加密后的数据, 因此其无法获得用户的原始登录信息, 也无法通过从平台服务器上得到的登录信息登录到平台服务器, 从而有效地避免了窃取者通过其在平台服务器上窃取的登录信息非法登录到平台服务器, 确保用户登录信息的安全。

请参考图 3, 为根据一示例性实施例三示出的获取电子文件的方法的流程图, 本实施例以用户需要绑定用户在平台服务器的第一登录信息与用户在信息提供服务器上生成的用户标识为例进行示例性说明, 如图 3 所示, 包括如下步骤:

步骤 301, 在用户在平台服务器的第一登录信息与用户标识未绑定时, 向平台服务器发送关联请求, 关联请求中携带有信息提供服务器的第一标识。

步骤 302, 接收来自平台服务器根据关联请求返回的第二提示信息。

步骤 303, 根据第二提示信息确定用户在终端设备输入的第二原始验证信息。

步骤 304, 根据第一加密密钥对第二原始验证信息进行加密, 得到用于身份验证的第二验证信息, 向平台服务器发送第二验证信息, 平台服务器将绑定请求和第二验证信息转发至信息提供服务器, 以供信息提供服务器根据与第一加密密钥对应的第一解密密钥对第二验证信息进行解密, 根据解密后的第二验证信息确定用户在信息提供服务器的用户标识, 将用户标识返回平台服务器后, 以供平台服务器建立第一登录信息和用户标识之间的绑定关系。

在一实施例中, 用户标识可以为用户在信息提供服务器的唯一标识, 该用户标识不含有用户的隐私信息, 可以用于平台服务器在向信息提供服务器发起请求电子处方时作为索引, 避免信息提供服务器每次都要通过对来自平台服务器的第二手机号码进行解密得到第一手机号码, 之后将第一手机号码作为索引查找相应的电子文件。

本实施例以平台服务器为 EPP 和信息提供服务器为 HIS 为例进行说明, 终端设备通过第二手机号码登录到 EPP, 其中, 第二手机号码为原始的第一手机号码通过 HIS 信息提供服务器的第一加密密钥加密得到的; 终端设备向 EPP 发送关联请求, 该关联请求中携带有 HIS_ID, 终端设备的用户在根据 EPP 的提示输入身份证号后, 对身份证号通过第一加密密钥进行加密, 得到第二验证信息; EPP 向 HIS 发送第二手机号码、第二验证信息、EPP 的第二加密密钥, 请求 HIS 对第二验证信息进行验证; HIS 对第二验证信息验证通过后, 向 EPP 返回用户标识; EPP 存储第二验证信息, 并存储第二手机号和用户标识的关联关系。在一实施例中, HIS 可以基于第一手机号码生成用户标识。

本实施例中, 信息提供服务器通过对来自平台服务器的第二验证信息进行验证, 协助平台服务器实现了二次身份认证; 在平台服务器上, 由于第二验证信息是由信息提供服务器的第一加密密钥对第二原始验证信息进行加密后生成的, 因此平台服务器并不能获取到终端设备的用户的真实的验证信息, 从而可以防止窃听者窃取终端设备的用户的验证信息, 避免非法用户向平台服务器通过非法的关联请求绑定合法用户在平台服务器的第一登录信息和用户在信息提供服务器的用户标识。

请参考图 4, 为根据一示例性实施例四示出的获取电子文件的方法的流程图, 本实施例以用户在平台服务器和信息提供服务器上注册为例进行示例性说明, 如图 4 所示, 包括如下步骤:

步骤 401, 向平台服务器发送用于获取平台服务器的第二加密密钥的第二请求消息。

步骤 402, 接收平台服务器根据第二请求消息返回的第二加密密钥。

步骤 403, 在用户在平台服务器和信息提供服务器上未注册时, 通过平台服务器的第二加密密钥对终端设备的用户需要在信息提供服务器注册的第一注册信息进行加密。

步骤 404, 在用户通过第一手机号码登录到信息提供服务器后, 将通过第二加密密钥加密后的第一注册信息发送至信息提供服务器。

5 步骤 405, 在信息提供服务器根据第一手机号码生成用户标识后, 接收来自信息提供服务器的第一加密密钥、注册成功的第一响应消息以及第二手机号码, 第二手机号码由第一加密密钥对第一手机号码加密生成。

步骤 406, 通过第二手机号码向平台服务器注册。

10 步骤 407, 在平台服务器对第二手机号码注册后, 接收平台服务器返回的注册成功的第二响应消息。

在上述步骤 402 中, 在一实施例中, 如果平台服务器采用对称加密算法, 则平台服务器上的第二加密密钥可以与平台服务器的第二解密密钥相同。在一实施例中, 对称加密算法可以为 DES (Data Encryption Standard)、3DES (Triple DES)、AES (Advanced Encryption Standard) 等。在另一实施例中, 如果平台服务器采用非对称加密算法, 第二加密密钥可以为平台服务器的公钥, 平台服务器的第二解密密钥可以为平台服务器的私钥。在一实施例中, 平台服务器采用的非对称加密算法可以为 RSA (Rivest Shamir Adlemen)、Elgamal、背包算法、Rabin、D-H (Diffie-Hellman)、椭圆曲线加密算法 (ECC) 等。在一实施例中, 在平台服务器需要将第二加密密钥发送给信息提供服务器时, 可以将非对称加密算法的公钥作为第二加密密钥。对于对称密钥的传输, 可以通过安全传输

15

20 通道来进行, 或者是对对称密钥进行加密后再传输, 从而确保对称密钥的安全性。

在上述步骤 404 中, 终端设备可以向平台服务器发送第二手机号码, 接收来自信息提供服务器返回的第三验证码, 其中, 第三验证码可以为平台服务器根据第二手机号码请求信息提供服务器发送给终端设备的; 终端设备向平台服务器发送第三验证码; 在平台服务器根据第三验证码与信息提供服务器返回给平台服务器的第四验证码进行比较以

25

确定验证通过后, 接收平台服务器返回的注册成功的第二响应消息。由于信息提供服务器可以根据其第一解密密钥对第二手机号码进行解密, 并协助平台服务器发送短信验证码, 实现了对用户的二次验证。

本实施例中, 平台服务器在拿到通过信息提供服务器的第一加密密钥加密后的第二手机号码后, 由于没有相应的解密密钥, 因此并不能对第二手机号码进行解密获取到真实的

30

第一手机号码, 因此即使第二手机号码在平台服务器上被窃取, 在窃取者未获取到

信息提供服务器的第一解密密钥时窃取者会由于没有解密密钥不能对第二手机号码解密；同时，用户在信息提供服务器上注册的隐私数据通过平台服务器的第二加密密钥加密，因此信息提供服务器也不能对存储在平台服务器上的数据进行解密，由于窃取者同时攻破平台服务器和信息提供服务器的难度很高，因此本申请可以大大提高平台服务器和信息提供服务器的安全防护程度。

请参考图 5，为根据又一示例性实施例一示出的获取电子文件的方法的流程图；本实施例可以应用在平台服务器上，在一实施例中，平台服务器可以为电商平台的服务，如图 5 所示，包括如下步骤：

步骤 501，接收来自终端设备的用于获取电子文件的第一请求消息，第一请求消息中携带有提供电子文件的信息提供服务器的第一标识。

步骤 502，根据第一请求消息向终端设备返回第一提示信息。

步骤 503，在终端设备根据第一提示信息确定用于身份验证的第一验证信息后，接收来自终端设备的第一验证信息。

步骤 504，根据第一标识确定信息提供服务器，将第一验证信息、终端设备的用户在信息提供服务器注册的用户标识发送至信息提供服务器。

步骤 505，在信息提供服务器对第一验证信息验证通过并根据用户标识确定电子文件后，接收来自信息提供服务器的电子文件，将电子文件转发至终端设备，电子文件中的隐私信息经过信息提供服务器的第一加密密钥加密。

在上述步骤 501 中，关于第一请求消息以及电子文件的描述请参见上述步骤 101 的相关描述，在此不再详述。

在上述步骤 502 和步骤 503 中，第一验证信息以及第一原始验证信息的相关描述请参见上述步骤 102 和步骤 103 的相关描述，在此不再详述。

在上述步骤 504 中，在一实施例中，平台服务器可以作为中介平台为不同的终端设备与不同的信息提供服务器提供电子文件的转发和用户身份的认证，当平台服务器从第一请求消息中解析出第一标识后，根据第一标识确定相对应的信息提供服务器；通过将第一验证信息、终端设备的用户在信息提供服务器注册的用户标识发送至信息提供服务器，使信息提供服务器能够对第一验证信息进行验证，在验证通过后根据用户标识确定用户需要查看的电子文件。

在上述步骤 505 中，电子文件中的隐私信息的描述请参见上述步骤 104 的相关描述，在此不再详述。

本实施例中，平台服务器接收到来自终端设备的第一验证信息和第一请求消息之后，根据第一标识确定信息提供服务器，并将第一验证信息和用户标识发送至信息提供服务器，以供信息提供服务器确定用户标识相对应的电子文件，电子文件中的隐私信息通过信息提供服务器的第一加密密钥进行加密保护，由于平台服务器并没有信息提供服务器的第一解密密钥，因此即使电子文件在平台服务器侧被窃取，窃取者也无法通过电子文件得到用户的真实的隐私信息，平台服务器侧的管理员也无法通过电子文件获取到用户的真实的隐私信息，从而有效地保护用户的隐私信息不被平台服务器泄露，确保用户的隐私安全。

请参见图 6，为根据又一示例性实施例二示出的获取电子文件的方法的流程图；本实施例以用户需要通过终端设备登录到平台服务器为例进行示例性说明，如图 6 所示，包括如下步骤：

步骤 601，在用户未登录到平台服务器时，确定用户在平台服务器上的第一登录信息。

步骤 602，通过终端设备的用户在平台服务器注册的第二手机号码指示信息提供服务器向终端设备发送第一验证码，第二手机号码由第一加密密钥对第一手机号码加密得到，第一手机号码为用户注册在信息提供服务器的手机号码。

步骤 603，在信息提供服务器通过信息提供服务器的第一解密密钥对第二手机号码解密得到第一手机号码，通过第一手机号码向终端设备指示发送第一验证码后，接收来自终端设备的第一验证码以及接收来自信息提供服务器的第二验证码。

步骤 604，对第一验证码和第二验证码进行验证，在验证通过后确定用户登录成功。

步骤 605，向终端设备返回登录成功的第一响应消息。

在上述步骤 601 中，第一登录信息的描述可以参见上述步骤 201 的相关描述，在此不再详述。

在上述步骤 602 至步骤 604 中，信息提供服务器在向终端设备发送第一验证码时，可以向平台服务器发送第二验证码，因此平台服务器在对第一验证码进行验证时，可以比较第一验证码与第二验证码的内容是否相同，如果相同，则验证通过，确定用户登录成功。

本实施例中，在用户需要登录到平台服务器时，由于用户是通过加密后的第一登录信息登录到平台服务器，在平台服务器上的数据遭到泄露时，窃取者从平台服务器窃取到的第一登录信息是加密后的数据，因此其无法通过从平台服务器上得到的登录信息登

录到平台服务器，从而有效地避免了窃取者通过其在平台服务器上窃取的登录信息非法登录到平台服务器，确保用户登录信息的安全；通过比较第一验证码和第二验证码，实现对用户进行二次身份验证，从而提高了用户在登录平台服务器的过程中的安全性。

请参见图 7，为根据又一示例性实施例三示出的获取电子文件的方法的流程图，本实施例以用户需要绑定用户在平台服务器的第一登录信息与用户在信息提供服务器上生成的用户标识为例进行示例性说明，如图 7 所示，包括如下步骤：

步骤 701，在用户在平台服务器的第一登录信息和用户在信息提供服务器注册的用户标识未绑定时，接收来自终端设备的关联请求，关联请求中携带有第一标识。

步骤 702，根据关联请求向终端设备返回第二提示信息。

步骤 703，在终端设备根据第二提示信息确定用于身份验证的第二验证信息，接收来自终端设备根据第二提示信息返回的第二验证信息，第二验证信息经过第一加密密钥加密。

步骤 704，将绑定请求和经过第一加密密钥的第二验证信息转发至信息提供服务器，以供信息提供服务器对经过第一加密密钥加密的第二验证信息进行解密，根据解密后的第二验证信息确定用户在信息提供服务器注册的用户标识。

步骤 705，接收来自信息提供服务器返回的用户标识，建立第一登录信息和用户标识之间的绑定关系。

本实施例以平台服务器为 EPP 和信息提供服务器为 HIS 为例进行说明，终端设备通过第二手机号码登录到 EPP，其中，第二手机号码为原始的第一手机号码通过 HIS 信息提供服务器的第一加密密钥加密得到的；EPP 接收来自终端设备的关联请求，该关联请求中携带有 HIS_ID，EPP 接收到来自终端设备的第二验证信息后，向 HIS 发送第二手机号码、第二验证信息、EPP 的第二加密密钥，请求 HIS 对第二验证信息进行验证；HIS 对第二验证信息验证通过后，向 EPP 返回用户标识；EPP 存储第二验证信息，并存储第二手机号和用户标识的关联关系。在一实施例中，HIS 可以通过第一手机号码生成用户标识。

本实施例中，信息提供服务器通过对来自平台服务器的第二验证信息进行验证，协助平台服务器实现了二次身份认证；在平台服务器上，由于第二验证信息是由信息提供服务器的第一加密密钥对第二原始验证信息进行加密后生成的，因此平台服务器并不能获取到终端设备的用户的真实的验证信息，从而可以防止窃听者窃取终端设备的用户的验证信息，避免非法用户向平台服务器通过非法的关联请求绑定合法用户在平台服务器

的第一登录信息和用户在信息提供服务器的用户标识。

图 8 是根据又一示例性实施例四示出的获取电子文件的方法的流程图，本实施例以用户在平台服务器和信息提供服务器上注册为例进行示例性说明，如图 8 所示，包括如下步骤：

5 步骤 801，接收来自终端设备的用于获取平台服务器的第二加密密钥的第二请求消息。

步骤 802，根据第二请求消息向终端设备返回第二加密密钥。

步骤 803，在用户在平台服务器上未注册时，通过来自终端设备的第二注册信息进行注册。

10 步骤 804，根据第二注册信息向信息提供服务器获取第三验证码，指示信息提供服务器向第二手机号码对应的第一手机号码发送第四验证码。

步骤 805，接收来自终端设备的第四验证码。

步骤 806，对第三验证码和第四验证码进行验证。

15 步骤 807，在平台服务器对第三验证码和第四验证码验证通过后，向终端设备返回注册成功的第二响应消息。

本实施例中，平台服务器在拿到通过信息提供服务器的第一加密密钥加密后的第二手机号码后，由于没有相应的解密密钥，因此并不能对第二手机号码进行解密获取到真实的第一手机号码，因此即使第二手机号码在平台服务器上被窃取，在窃取者未获取到信息提供服务器的第一解密密钥时窃取者会由于没有解密密钥不能对第二手机号码解密；同时，用户在信息提供服务器上注册的隐私数据通过平台服务器的第二加密密钥加密，因此信息提供服务器也不能对存储在平台服务器上的数据进行解密，由于窃取者同时攻破平台服务器和信息提供服务器的难度很高，因此本申请可以大大提高平台服务器和信息提供服务器的安全防护程度。

25 请参见图 9，为根据另一示例性实施例一示出的获取电子文件的方法的流程图；本实施例可以应用在信息提供服务器上，在一实施例中，信息提供服务器可以为医院系统的服务器，通过信息提供服务器可以为终端设备的用户提供电子处方，如图 9 所示，包括如下步骤：

步骤 901，接收来自平台服务器的第一验证信息、终端设备的用户在信息提供服务器注册的用户标识。

30 步骤 902，对第一验证信息进行验证，在验证通过后根据用户标识确定电子文件。

步骤 903, 将电子文件中的隐私信息通过信息提供服务器的第一加密密钥加密。

步骤 904, 将电子文件发送至平台服务器, 以供平台服务器将电子文件转发至终端设备。

在上述步骤 902 中, 信息提供服务器可以通过信息提供服务器的第一解密密钥对第一验证信息进行解密, 通过平台服务器的第二加密密钥对解密后的第一验证信息进行加密, 得到第一加密字符串; 确定用户在信息提供服务器注册时生成的第二加密字符串, 第二加密字符串由第一验证信息通过平台服务器的第二加密密钥加密生成; 确定第一加密字符串和第二加密字符串是否相同, 如果相同, 则第一验证信息的验证通过。

本实施例中, 信息提供服务器在对来自平台服务器的第一验证信息进行验证并且验证通过后, 根据来自平台服务器的用户标识确定电子文件, 通过第一加密密钥将电子文件的隐私信息进行加密, 由于平台服务器并没有信息提供服务器的第一加密密钥, 因此即使电子文件在平台服务器侧被窃取, 窃取者也无法通过电子文件得到用户的真实的隐私信息, 平台服务器侧的管理员也无法通过电子文件获取到用户的真实的隐私信息, 从而有效地保护用户的隐私信息不被平台服务器泄露, 确保用户的隐私安全。

请参见图 10, 为根据另一示例性实施例二示出的获取电子文件的方法的流程图, 本实施例以用户需要通过终端设备登录到平台服务器为例进行示例性说明, 如图 10 所示, 包括如下步骤:

步骤 1001, 在用户未登录到平台服务器时, 接收来自平台服务器用于指示信息提供服务器向用户在平台服务器注册的第二手机号码发送第一验证码的指示消息, 其中, 第二手机号码由第一加密密钥对第一手机号码加密得到, 第一手机号码为用户注册在信息提供服务器的手机号码。

步骤 1002, 根据指示消息通过第一解密密钥对第二手机号码进行解密, 得到第一手机号码。

步骤 1003, 通过第一手机号码向终端设备发送第一验证码以及向平台服务器返回第二验证码, 以供平台服务器根据第一验证码和第二验证码对用户进行登录验证。

本实施例中, 在用户需要登录到平台服务器时, 信息提供服务器根据来自平台服务器的指示消息通过第一解密密钥对第二手机号码进行解密, 得到第一手机号码, 并通过第一手机号码向终端设备发送第一验证码以及向平台服务器返回第二验证码, 从而协助平台服务器对用户进行二次身份验证, 提高了用户在登录平台服务器的过程中的安全性。

请参见图 11, 为根据另一示例性实施例三示出的获取电子文件的方法的流程图, 本

实施例以用户需要绑定用户在平台服务器的第一登录信息与用户在信息提供服务器上生成的用户标识为例进行示例性说明，如图 11 所示，包括如下步骤：

步骤 1101，在用户在平台服务器的第一登录信息与用户标识未绑定时，接收来自平台服务器的第二验证信息和平台服务器的第二加密密钥，第二验证信息经过第一加密密钥加密。

步骤 1102，通过信息提供服务器的第一解密密钥对第二验证信息进行解密，通过第二加密密钥对解密后的第二原始验证信息进行加密，得到第三加密字符串。

步骤 1103，确定用户在信息提供服务器注册时生成的第四加密字符串，第四加密字符串由第二原始验证信息通过平台服务器的第二加密密钥加密生成。

步骤 1104，确定第三加密字符串和第四加密字符串是否相同。

步骤 1105，如果相同，向平台服务器返回终端设备的用户在信息提供服务器上注册的用户标识，以供平台服务器建立第一登录信息和用户标识的绑定关系。

作为一个示例性场景，信息提供服务器接收到的来自平台服务器的第二验证信息为字符串“AAAA&&&”和平台服务器的第二加密密钥“121212”，由于“AAAA&&&”经过第一加密密钥加密，因此信息提供服务器利用其第一解密密钥对“AAAA&&&”解密后，生成真实的验证信息“BBBB&&&”，通过第二加密密钥“121212”对“BBBB&&&”进行加密，得到第三加密字符串“CCCC&&&”，确定用户在信息提供服务器注册时生成的第四加密字符串“DDDD&&&”，第四加密字符串由第二验证信息 AAAA&&&通过平台服务器的第二加密密钥“121212”加密生成，由此可知，第三加密字符串“CCCC&&&”与第四加密字符串“DDDD&&&”应为内容相同的字符串，如果不相同，说明用户的关联请求非法或者非法用户请求关联。

本实施例中，信息提供服务器通过采用加密字符串的方式对来自平台服务器的第二验证信息进行验证，协助平台服务器实现了二次身份认证；在平台服务器上，由于第二验证信息是由信息提供服务器的第一加密密钥对第二原始验证信息进行加密后生成的，因此平台服务器并不能获取到终端设备的用户的真实的验证信息，而第四加密字符串由第二验证信息通过平台服务器的第二加密密钥加密生成，因此信息提供服务器侧只有在对用户进行验证时才能够得到真实的验证信息，从而可以防止窃听者窃取终端设备的用户在平台服务器和信息提供服务器上的验证信息，避免非法用户向平台服务器通过非法的关联请求绑定合法用户在平台服务器的第一登录信息和用户在信息提供服务器的用户标识。

请参见图 12，为根据另一示例性实施例四示出的获取电子文件的方法的流程图，本实施例以用户在平台服务器和信息提供服务器上注册为例进行示例性说明，如图 12 所示，包括如下步骤：

步骤 1201，在用户在信息提供服务器上未注册时，通过来自终端设备的第一注册信息
5 息进行注册。

步骤 1202，在用户通过第一手机号码登录到信息提供服务器后，将第一手机号码通过第一加密密钥进行加密，得到第二手机号码。

步骤 1203，将第二手机号码发送至终端设备，以供终端设备通过第二手机号码在平台服务器上注册。

10 步骤 1204，根据第一手机号码生成用户标识。

步骤 1205，接收来自平台服务器的第二手机号码。

步骤 1206，通过第一解密密钥对第二手机号码进行解密，得到第一手机号码；

步骤 1207，通过第一手机号码向终端设备返回第三验证码，第三验证码为平台服务器根据第二注册信息请求信息提供服务器发送给终端设备的；

15 步骤 1208，向平台服务器返回第四验证码，以供平台服务器对第三验证码和第四验证码进行比较以确定验证是否通过。

本实施例中，平台服务器在拿到通过信息提供服务器的第一加密密钥加密后的第二手机号码后，由于没有相应的解密密钥，因此并不能对第二手机号码进行解密获取到真实的第一手机号码，因此即使第二手机号码在平台服务器上被窃取，在窃取者未获取到
20 信息提供服务器的第一解密密钥时窃取者会由于没有解密密钥不能对第二手机号码解密；同时，用户在信息提供服务器上注册的隐私数据通过平台服务器的第二加密密钥加密，因此信息提供服务器也不能对存储在平台服务器上的数据进行解密，由于窃取者同时攻破平台服务器和信息提供服务器的难度很高，因此本申请可以大大提高平台服务器和信息提供服务器的安全防护程度。

25 请参见图 13，为根据一示例性实施例示出的获取电子文件的方法的场景图之一，本实施例以电子文件为电子处方、平台服务器为 EPP 以及信息提供服务器为 HIS 为例，描述用户如何从 HIS 获取到电子处方的，其中，HIS 和 EPP 均采用非对称加密算法，相应地，HIS 侧的公钥为第一加密密钥，私钥为第一解密密钥，EPP 侧的公钥为第二加密密钥，私钥为第二解密密钥；如图 13 所示，包括如下步骤：

30 步骤 1301，患者通过终端设备使用经过 HIS 的公钥加密后的登录名、登录密码登录

EPP，其中，登录的方式可以通过图案方式登录，也可以通过输入登录名、密码登录的方式登录。

步骤 1302，EPP 向终端设备返回登录成功的第一响应消息。

步骤 1303，终端设备向 EPP 发送获取电子处方的第一请求消息，请求查看患者在指定医院的电子处方，该第一请求消息中携带医院标识 HIS_ID（也可称为第一标识）。

步骤 1304，EPP 根据第一请求消息向终端设备返回第一提示消息，提示用户输入第一验证信息。

步骤 1305，终端设备根据第一提示信息确定用户在终端设备输入的第一原始验证信息以及确定信息提供服务器的第一加密密钥，根据第一加密密钥对第一原始验证信息进行加密，得到用于身份验证的第一验证信息。

步骤 1306，向 EPP 发送第一验证信息。

步骤 1307，EPP 通过患者的登录名查找到患者在指定医院的用户标识（PatientID），将该用户标识、第二手机号码、第一验证信息，EPP 的第二加密密钥发送至 HIS。

步骤 1308，HIS 通过其第一解密密钥对第二手机号码进行解密，得到第一手机号码，通过第一手机号查找患者在 HIS 的用户标识。

步骤 1309，HIS 通过 HIS 的第一解密密钥对第一验证信息进行解密，通过 EPP 的第二加密密钥对解密后的第一验证信息进行加密，得到第一加密字符串。

步骤 1310，HIS 确定患者在 HIS 注册时生成的第二加密字符串，第二加密字符串由第一验证信息通过 EPP 的第二加密密钥加密生成，比较第一加密字符串和第二加密字符串是否相同，如果相同，则第一验证信息的验证通过。

步骤 1311，HIS 确定电子处方，通过第一加密密钥对电子处方中的隐私信息进行加密，将加密后的电子处方发送至 EPP。

步骤 1312，EPP 向终端设备返回电子处方。

本实施例中，由于患者需要查看的电子处方是患者的诊治记录、药方、服药说明等，因此通过 HIS 的第一加密密钥对电子处方中的隐私信息进行去隐私保护并不会影响患者的用户体验。由于 HIS 仅对电子处方中的隐私信息通过第一加密密钥加密，而对非隐私信息不用加密，因此可以降低 HIS 侧的计算复杂度。

请参见图 14，为根据一示例性实施例示出的获取电子文件的方法的场景图之二，本实施例以电子文件为电子处方、平台服务器为 EPP 以及信息提供服务器为 HIS 为例，描述用户如何通过第二手机号码登录到 EPP 的；如图 14 所示，包括如下步骤：

步骤 1401, 患者通过终端设备向 EPP 发起登录请求时, 终端设备将用户的真实的第一手机号码通过 HIS 的第一加密密钥进行加密, 得到第二手机号码, 通过第二手机号码进行登录。

步骤 1402, EPP 向 HIS 基于第二手机号码, 向 HIS 请求向终端设备发送第一验证码。

5 步骤 1403, HIS 基于第二手机号码通过其对应的第一解密密钥对第二手机号码解密, 得到第一手机号, 通过第一手机号码向终端设备发送第一验证码。

步骤 1404, HIS 向 EPP 返回第二验证码。

步骤 1405, EPP 接收来自终端设备的第一验证码。

10 步骤 1406, EPP 比较第一验证码和第二验证码, 在确定二者相同时, 确定患者登录成功, 向终端设备返回登录成功的第一响应消息。

本实施例中, 在用户需要登录到 EPP 时, 通过第一加密密钥对用户的真实登录信息进行加密, 并通过加密后的第一登录信息登录到平台服务器, 在平台服务器上的数据遭到泄露时, 窃取者从平台服务器窃取到的第一登录信息是加密后的数据, 因此其无法通过从平台服务器上得到的登录信息登录到平台服务器, 从而有效地避免了窃取者通过其在平台服务器上窃取的登录信息非法登录到平台服务器, 确保用户登录信息的安全。HIS 通过其第一解密秘钥对第二手机号码解密得到第一手机号码, 并分别向终端设备和 EPP 发送第一验证码和第二验证码, 从而协助 EPP 完成了二次身份验证。

15

请参见图 15, 为根据一示例性实施例示出的获取电子文件的方法的场景图之三, 本实施例以电子文件为电子处方、平台服务器为 EPP 以及信息提供服务器为 HIS 为例, 描述如何对用户在 EPP 的第一登录信息中的登录名与用户在 HIS 的用户标识进行绑定的; 如图 15 所示, 包括如下步骤:

20

步骤 1501, 终端应用使用第二手机号 (即对原始的第一手机号通过 HIS 的第一解密密钥加密得到的)、登录密码登录 EPP。

步骤 1502, EPP 向终端设备返回登录成功的第一响应消息。

25 步骤 1503, 终端设备向 EPP 发送关联请求, 该关联请求中携带有医院标识。

步骤 1504, EPP 向终端设备返回第二提示信息, 以提示用户通过终端设备输入第二原始验证信息。

步骤 1505, 用户根据第二提示信息输入第二原始验证信息 (例如, 身份证号), 并通过 HIS 的第一加密密钥对第二原始验证信息进行加密, 生成的第二验证信息。

30 步骤 1506, 终端设备向 EPP 发送第二验证信息。

步骤 1507, EPP 将第二手机号、第二验证信息、EPP 的第二加密密钥以及 EPP 所采用的加密算法的名称发送给 HIS, 请求 HIS 对第二验证信息进行验证。

步骤 1508, HIS 通过其第一解密密钥采用相应的加密算法对第二手机号码解密, 得到第一手机号码, 根据第一手机号码查找用户标识, 通过信息提供服务器的第一解密密钥对第二验证信息进行解密, 得到第二原始验证信息, 通过第二加密密钥对第二原始验证信息进行加密, 得到第三加密字符串。

步骤 1509, 确定用户在信息提供服务器注册时生成的第四加密字符串, 第四加密字符串由第二原始验证信息通过平台服务器的第二加密密钥加密生成。

步骤 1510, HIS 比较第三加密字符串和第四加密字符串是否相同, 进行验证。

10 步骤 1511, 如果相同, HIS 验证通过, 向 EPP 返回用户标识。

步骤 1512, EPP 存储第二验证信息, 并存储第二手机号和用户标识的关联关系。

在本实施例所述的流程中, HIS 通过得到来自 EPP 的第二验证信息, 通过 HIS 的第一解密密钥得到第一加密密钥加密后的第二原始验证信息, 通过 EPP 的第二加密密钥对第二原始验证信息加密得到第三加密字符串, 从而实现了身份认证的目的。在将第一登录信息与用户标识进行绑定的过程中, 除了用于索引的第一手机号码和用于验证的第二验证信息之外, HIS 侧的其它数据均为机密的, 而 EPP 平台侧的用户的登录信息也是机密的, 从而达到了隐私保护的目的。

请参见图 16, 为根据一示例性实施例示出的获取电子文件的方法的场景图之四, 本实施例以电子文件为电子处方、平台服务器为 EPP 以及信息提供服务器为 HIS 为例, 描述用户如何在 EPP 和 HIS 侧注册的; 如图 16 所示, 包括如下步骤:

步骤 1601, 患者通过终端设备向 EPP 请求 EPP 的第二加密密钥。

步骤 1602, EPP 向终端设备返回 EPP 的第二加密密钥, 并向终端设备发送数字签名。

步骤 1603, 终端设备使用第一手机号码(即原始的手机号)在 HIS 注册, 使用 EPP 的第二加密密钥, 对需要注册的信息通过第二加密密钥进行加密。其中, 需要在 HIS 注册的信息包括: 姓名、病历卡号、身份证号、手机号码家庭住址、药物过敏记录、过往病史等。

步骤 1604, HIS 保存第一手机号码, 生成患者标识(PatientID), 并保存基于 EPP 的第二加密密钥加密后的验证信息(例如, 身份证号等)。

步骤 1605, HIS 向终端设备返回注册成功的第二响应消息, 并向终端设备返回 HIS 的第一加密密钥, 以及使用 HIS 的第一加密密钥对第一手机号码加密后生成的第二手机

号码。

步骤 1606, 终端设备使用第二手机号码向 EPP 注册。

步骤 1607, EPP 将第二手机号码发送到 HIS, 请求 HIS 向终端设备发送短信验证码。

5 步骤 1608, HIS 通过 HIS 的第一加密密钥对第二手机号码进行解密, 得到第一手机号码。

步骤 1609, HIS 向 EPP 返回第三验证码。

步骤 1610, HIS 基于第一手机号码向终端设备返回第四验证码。

步骤 1611, 终端设备向 EPP 上报第四验证码。

10 步骤 1612, EPP 比较终端设备上报的第四验证码和 HIS 返回的第三验证码, 如果一致, 则验证通过, 并存储第二手机号。

步骤 1613, EPP 向终端设备返回注册成功的第二响应消息。

步骤 1614, 终端设备可以通过第二手机号码设置登录到 EPP 的登录密码。

步骤 1615, EPP 向终端设备平台返回设置成功的响应。

15 在本实施例的流程中, EPP 在拿到通过 HIS 的第一加密密钥加密后的第二手机号码后, 由于没有相应的解密密钥, 因此并不能对第二手机号码进行解密获取到真实的第一手机号码, 因此即使第二手机号码在平台服务器上被窃取, 在窃取者未获取到 HIS 的第一解密密钥时窃取者会由于没有解密密钥不能对第二手机号码解密; 同时, 用户在 HIS 上注册的隐私数据通过 EPP 的第二加密密钥加密, 因此 HIS 也不能对存储在 EPP 上的数据进行解密, 由于窃取者同时攻破 EPP 和 HIS 的难度很高, 因此本申请可以大大提高
20 EPP 和 HIS 的安全防护程度。此外, HIS 可以根据自己的第一解密密钥解密得到第一手机号码, 从而可以协助 EPP 发送短信验证码, 完成二次验证。

对应于上述的获取电子文件的方法, 本申请还提出了图 17 所示的根据本申请的一示例性实施例的终端设备的示意结构图。请参考图 17, 在硬件层面, 该服务器包括处理器、内部总线、网络接口、内存以及非易失性存储器, 当然还可能包括其他业务所需要的硬件。
25 件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行, 在逻辑层面上形成获取电子文件的装置。当然, 除了软件实现方式之外, 本申请并不排除其他实现方式, 比如逻辑器件抑或软硬件结合的方式等等, 也就是说以下处理流程的执行主体并不限定于各个逻辑单元, 也可以是硬件或逻辑器件。

对应于上述的获取电子文件的方法, 本申请还提出了图 18 所示的根据本申请的一示例性实施例的平台服务器的示意结构图。请参考图 18, 在硬件层面, 该服务器包括处理
30

器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成获取电子文件的装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

对应于上述的获取电子文件的方法，本申请还提出了图 19 所示的根据本申请的一示例性实施例的信息提供服务器的示意结构图。请参考图 19，在硬件层面，该服务器包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成获取电子文件的装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

请参考图 20，为根据一示例性实施例一示出的获取电子文件的装置的结构示意图；在软件实施方式中，该获取电子文件的装置可以包括：第一发送模块 2001、第一接收模块 2202、第一确定模块 2203、第二接收模块 2204；其中：

第一发送模块 2001，用于向平台服务器发送用于获取电子文件的第一请求消息，第一请求消息中携带有提供电子文件的信息提供服务器的第一标识；

第一接收模块 2002，用于接收来自平台服务器根据第一发送模块 2001 发送的第一请求消息返回的第一提示信息；

第一确定模块 2003，用于根据第一接收模块 2002 接收到的第一提示信息确定用于身份验证的第一验证信息，向平台服务器发送第一验证信息；

第二接收模块 2004，用于在平台服务器根据第一标识确定信息提供服务器，以及根据终端设备的用户在平台服务器的第一登录信息确定用户在信息提供服务器注册的用户标识，并将第一确定模块 2003 确定的第一验证信息、用户标识发送至信息提供服务器后，接收平台服务器转发的来自信息提供服务器的电子文件，电子文件中的隐私信息经过信息提供服务器的第一加密密钥加密。

请参见图 21，为根据一示例性实施例二示出的获取电子文件的装置的结构示意图，在上述图 20 所示实施例的基础上，第一确定模块 2003 可包括：

第一确定单元 20031，用于根据第一提示信息确定用户在终端设备输入的第一原始

验证信息以及确定信息提供服务器的第一加密密钥；

第一加密单元 20032，用于根据第一确定单元 20031 确定的第一加密密钥对第一原始验证信息进行加密，得到用于身份验证的第一验证信息。

在一实施例中，装置还可包括：

- 5 第二确定模块 2005，用于在用户未登录到平台服务器时，确定用户的第一登录信息，通过第一登录信息登录平台服务器；

第三接收模块 2006，用于在第二确定模块 2005 确定用户登录成功后，接收平台服务器返回的登录成功的第一响应消息。

在一实施例中，装置还可包括：

- 10 第四接收模块 2007，用于通过第一手机号码接收来自信息提供服务器的第一验证码，第一验证码为平台服务器根据第二手机号码指示信息提供服务器发送第一手机号码的，第二手机号码由第一加密密钥对第一手机号码加密得到；

第二发送模块 2008，用于将第四接收模块 2007 接收到的第一验证码通过第二手机号码发送给平台服务器；

- 15 第三确定模块 2009，用于在平台服务器对第二发送模块 2008 发送的第一验证码与来自信息提供服务器的第二验证码进行验证后，确定用户登录成功，第三接收模块 2006 执行接收平台服务器返回的登录成功的第一响应消息的步骤。

在一实施例中，装置还可包括：

- 20 第三发送模块 2010，用于在用户在平台服务器的第一登录信息与用户标识未绑定时，向平台服务器发送关联请求，关联请求中携带有信息提供服务器的第一标识；

第五接收模块 2011，用于接收来自平台服务器根据第三发送模块 2010 发送的关联请求返回的第二提示信息；

第四确定模块 2012，用于根据第五接收模块 2011 接收到的第二提示信息确定用户在终端设备输入的第二原始验证信息；

- 25 第一加密模块 2013，用于根据第一加密密钥对第四确定模块 2012 确定的第二原始验证信息进行加密，得到用于身份验证的第二验证信息；

- 30 第四发送模块 2014，用于向平台服务器发送第一加密模块 2013 加密的第二验证信息，平台服务器将绑定请求和第二验证信息转发至信息提供服务器，以供信息提供服务器根据与第一加密密钥对应的第一解密密钥对经过第二验证信息进行解密，根据解密后的第二验证信息确定用户在信息提供服务器的用户标识，将用户标识返回平台服务器后，

以供平台服务器建立第一登录信息和用户标识之间的绑定关系。

在一实施例中，装置还可包括：

第二加密模块 2015，用于在用户在平台服务器和信息提供服务器上未注册时，通过平台服务器的第二加密密钥对终端设备的用户需要在信息提供服务器注册的第一注册信息
5 信息进行加密；

第五发送模块 2016，用于在用户通过第一手机号码登录到信息提供服务器后，将通过第一加密密钥加密后的第一注册信息发送至信息提供服务器；

第六接收模块 2017，用于在信息提供服务器根据第一手机号码生成用户标识后，接收来自信息提供服务器的第一加密密钥、注册成功的第一响应消息以及第二手机号码，
10 第二手机号码由第一加密密钥对第一手机号码加密生成；

第一注册模块 2018，用于通过第二手机号码向平台服务器注册；

第七接收模块 2019，用于在平台服务器对第二手机号码注册后，接收平台服务器返回的注册成功的第二响应消息。

在一实施例中，装置还包括：

第六发送模块 2020，用于向平台服务器发送用于获取平台服务器的第二加密密钥的第二请求消息；
15

第八接收模块 2021，用于接收平台服务器根据第六发送模块 39 发送的第二请求消息返回的第二加密密钥。

在一实施例中，第一注册模块 2018 可包括：

第一发送单元 20181，用于向平台服务器发送第二手机号码；
20

第一接收单元 20182，用于接收来自信息提供服务器返回的第三验证码，第三验证码为平台服务器根据第一发送单元发送的第二手机号码请求信息提供服务器发送给终端设备的；

第二发送单元 20183，用于向平台服务器发送第一接收单元 20182 接收到的第三验证码；
25

在平台服务器根据第三验证码与信息提供服务器返回给平台服务器的第四验证码进行比较以确定验证通过后，第七接收模块 2019 执行接收平台服务器返回的注册成功的第二响应消息的步骤。

图 22 是根据又一示例性实施例一示出的获取电子文件的装置的结构示意图；在软件实施方式中，该获取电子文件的装置可以包括：第九接收模块 2201、第七发送模块 2202、
30

第八发送模块 2203、第九发送模块 2204、第一转发模块 2205；其中：

第九接收模块 2201，用于接收来自终端设备的用于获取电子文件的第一请求消息，第一请求消息中携带有提供电子文件的信息提供服务器的第一标识；

5 第七发送模块 2202，用于根据第九接收模块 2201 接收到的第一请求消息向终端设备返回第一提示信息；

第八发送模块 2203，用于在终端设备根据第七发送模块 2202 发送的第一提示信息确定用于身份验证的第一验证信息后，接收来自终端设备的第一验证信息；

第九发送模块 2204，用于根据第九接收模块 2201 接收到的第一标识确定信息提供服务器，将第八发送模块 2203 接收到的第一验证信息、终端设备的用户在信息提供服务
10 器注册的用户标识发送至信息提供服务器；

第一转发模块 2205，用于在信息提供服务器对第九发送模块 2204 发送的第一验证信息验证通过并根据用户标识确定电子文件后，接收来自信息提供服务器的电子文件，将电子文件转发至终端设备，电子文件中的隐私信息经过信息提供服务器的第一加密密钥加密。

15 图 23 是根据又一示例性实施例二示出的获取电子文件的装置的结构示意图；在上述图 22 所示实施例的基础上，第一验证信息为用户在终端设备输入的原始验证信息通过第一加密密钥加密生成的。

在一实施例中，装置还可包括：

第五确定模块 2206，用于在用户未登录到平台服务器时，确定用户在平台服务器上
20 的第一登录信息；

第十发送模块 2207，用于在第五确定模块 2206 确定用户登录成功后，向终端设备返回登录成功的第一响应消息。

在一实施例中，装置还可包括：

第十一发送模块 2208，用于通过终端设备的用户在平台服务器注册的第二手机号码
25 指示信息提供服务器向终端设备发送第一验证码，第二手机号码由第一加密密钥对第一手机号码加密得到，第一手机号码为用户注册在信息提供服务器的手机号码；

第十接收模块 2209，用于在信息提供服务器通过信息提供服务器的第一解密密钥对第二手机号码解密得到第一手机号码，通过第一手机号码向终端设备指示发送第一验证码后，接收来自终端设备的第一验证码以及接收来自信息提供服务器的第二验证码；

30 第一验证模块 2210，用于对第一验证码和第二验证码进行验证，在验证通过后确定

用户登录成功，第十发送模块 2209 执行向终端设备返回登录成功的第一响应消息的步骤。

在一实施例中，装置还可包括：

第十一接收模块 2211，用于在用户在平台服务器的第一登录信息和用户在信息提供
5 服务器注册的用户标识未绑定时，接收来自终端设备的关联请求，关联请求中携带有第一标识；

第十二发送模块 2212，用于根据关联请求向终端设备返回第二提示信息；

第十二接收模块 2213，用于在终端设备根据第二提示信息确定用于身份验证的第二
10 验证信息，接收来自终端设备根据第二提示信息返回的第二验证信息，第二验证信息经
过第一加密密钥加密；

第二转发模块 2214，用于将绑定请求和经过第一加密密钥的第二验证信息转发至信息
提供服务器，以供信息提供服务器对经过第一加密密钥加密的第二验证信息进行解密，
根据解密后的第二验证信息确定用户在信息提供服务器注册的用户标识；

第十三接收模块 2215，用于接收来自信息提供服务器返回的用户标识，建立第一登
15 录信息和用户标识之间的绑定关系。

在一实施例中，装置还可包括：

第二注册模块 2216，用于在用户在平台服务器上未注册时，通过来自终端设备的第
二注册信息进行注册；

第一获取模块 2217，用于根据第二注册模块 2216 注册的第二注册信息向信息提供
20 服务器获取第三验证码，指示信息提供服务器向第二手机号码对应的第一手机号码发送
第四验证码；

第十四接收模块 2218，用于接收来自终端设备的第四验证码；

第二验证模块 2219，用于对第三验证码和第四验证码进行验证；

第十三发送模块 2220，用于在第二验证模块 2219 对第三验证码和第四验证码验证通
25 过后，向终端设备返回注册成功的第二响应消息。

在一实施例中，装置还可包括：

第十五接收模块 2221，用于接收来自终端设备的用于获取平台服务器的第二加密密
钥的第二请求消息；

第十四发送模块 2222，用于根据第十五接收模块 2221 接收到的第二请求消息向终
30 端设备返回第二加密密钥。

图 24 是根据另一示例性实施例一示出的获取电子文件的装置的结构示意图；在软件实施方式中，该获取电子文件的装置可以包括：第十六接收模块 2401、第三验证模块 2402、第三加密模块 2403、第十五发送模块 2404；其中：

第十六接收模块 2401，用于接收来自平台服务器的第一验证信息、终端设备的用户
5 在信息提供服务器注册的用户标识；

第三验证模块 2402，用于对第十六接收模块 2401 接收到的第一验证信息进行验证，在验证通过后根据用户标识确定电子文件；

第三加密模块 2403，用于将第三验证模块 2402 确定的电子文件中的隐私信息通过信息提供服务器的第一加密密钥加密；

10 第十五发送模块 2404，用于将第三加密模块 2403 加密后的电子文件发送至平台服务器，以供平台服务器将电子文件转发至终端设备。

图 25 是根据另一示例性实施例二示出的获取电子文件的装置的结构示意图，在上述图 24 所示实施例的基础上，第三验证模块 2402 包括：

15 第一解密单元 24021，用于通过信息提供服务器的第一解密密钥对第一验证信息进行解密；

第一加密单元 24022，用于通过平台服务器的第二加密密钥对第一解密单元解密后的第一验证信息进行加密，得到第一加密字符串；

第一确定单元 24023，用于确定用户在信息提供服务器注册时生成的第二加密字符串，第二加密字符串由第一验证信息通过平台服务器的第二加密密钥加密生成；

20 第二确定单元 24024，用于确定第一加密单元 24022 得到的第一加密字符串和第一确定单元 24023 确定的第二加密字符串是否相同，如果相同，则第一验证信息的验证通过。

在一实施例中，装置还可包括：

25 第十七接收模块 2405，用于在用户未登录到平台服务器时，接收来自平台服务器用于指示信息提供服务器向用户在平台服务器注册的第二手机号码发送第一验证码的指示消息，其中，第二手机号码由第一加密密钥对第一手机号码加密得到，第一手机号码为用户注册在信息提供服务器的手机号码；

第一解密模块 2406，用于根据第十七接收模块 2405 接收到的指示消息通过第一解密密钥对第二手机号码进行解密，得到第一手机号码；

30 第十六发送模块 2407，用于通过第一手机号码向终端设备发送第一验证码以及向平

台服务器返回第二验证码，以供平台服务器根据第一验证码和第二验证码对用户进行登录验证。

在一实施例中，装置还可包括：

第十八接收模块 2408，用于在用户在平台服务器的第一登录信息与用户标识未绑定时，接收来自平台服务器的第二验证信息和平台服务器的第二加密密钥，第二验证信息经过第一加密密钥加密；

第二解密模块 2409，用于通过信息提供服务器的第一解密密钥对第二验证信息进行解密，通过第二加密密钥对解密后的第二原始验证信息进行加密，得到第三加密字符串；

第六确定模块 2410，用于确定用户在信息提供服务器注册时生成的第四加密字符串，第四加密字符串由第二原始验证信息通过平台服务器的第二加密密钥加密生成；

第七确定模块 2411，用于确定第三加密字符串和第四加密字符串是否相同；

第十七发送模块 2412，用于如果第七确定模块 2411 确定相同，向平台服务器返回终端设备的用户在信息提供服务器上注册的用户标识，以供平台服务器建立第一登录信息和用户标识的绑定关系。

在一实施例中，装置还可包括：

第三注册模块 2413，用于在用户在信息提供服务器上未注册时，通过来自终端设备的第一注册信息进行注册；

第四加密模块 2414，用于在用户通过第一手机号码登录到信息提供服务器后，将第一手机号码通过第一加密密钥进行加密，得到第二手机号码；

第十八发送模块 2415，用于将第二手机号码发送至终端设备，以供终端设备通过第二手机号码在平台服务器上注册；

标识生成模块 2416，用于根据第一手机号码生成用户标识。

在一实施例中，装置还可包括：

第十九接收模块 2417，用于接收来自平台服务器的第二手机号码；

第三解密模块 2418，用于通过第一解密密钥对第二手机号码进行解密，得到第一手机号码；

第十九发送模块 2419，用于通过第一手机号码向终端设备返回第三验证码，第三验证码为平台服务器根据第二注册信息请求信息提供服务器发送给终端设备的；

第二十发送模块 2420，用于向平台服务器返回第四验证码，以供平台服务器对第三验证码和第四验证码进行比较以确定验证是否通过。

由上述实施例可见，用户需要在信息提供服务器注册时，使用平台服务器的第二加密密钥对用户的相关信息进行加密；而在平台服务器注册时，使用信息提供服务器的第一加密密钥对用户的相关信息（包括电子文件中的隐私信息）进行加密；在进行关联请求、查看电子文件时，平台服务器均需要将加密后的信息发给信息提供服务器进行解密之后再进行验证，或者是信息提供服务器对信息进行解密后发回平台服务器进行验证，在信息提供服务器上的隐私数据遭到泄露时，可以使窃取者无法得到原始数据；同样，即使平台服务器上的数据遭到泄露，窃取者也无法得到原始数据。此外，平台服务器还可以在信息提供服务器的协助下，完成身份认证，既有效地保护了用户的隐私信息，又实现了身份认证。

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

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，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

权 利 要 求 书

1、一种获取电子文件的方法，应用在终端设备上，其特征在于，所述方法包括：

向平台服务器发送用于获取电子文件的第一请求消息，所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识；

5 接收来自所述平台服务器根据所述第一请求消息返回的第一提示信息；

根据所述第一提示信息确定用于身份验证的第一验证信息，向所述平台服务器发送所述第一验证信息；

在所述平台服务器根据所述第一标识确定所述信息提供服务器，以及根据所述终端设备的用户在所述平台服务器的第一登录信息确定所述用户在所述信息提供服务器注册的用户标识，并将所述第一验证信息、所述用户标识发送至所述信息提供服务器后，
10 接收所述平台服务器转发的来自所述信息提供服务器的所述电子文件，所述电子文件中的隐私信息经过所述信息提供服务器的第一加密密钥加密。

2、根据权利要求 1 所述的方法，其特征在于，所述根据所述第一提示信息确定用于身份验证的第一验证信息的步骤，包括：

15 根据所述第一提示信息确定所述用户在所述终端设备输入的第一原始验证信息以及确定所述信息提供服务器的所述第一加密密钥；

根据所述第一加密密钥对所述第一原始验证信息进行加密，得到用于身份验证的第一验证信息。

3、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

20 在所述用户未登录到所述平台服务器时，确定所述用户的第一登录信息，通过所述第一登录信息登录所述平台服务器；

在所述用户登录成功后，接收所述平台服务器返回的登录成功的第一响应消息。

4、根据权利要求 3 所述的方法，其特征在于，所述方法还包括：

通过第一手机号码接收来自所述信息提供服务器的第一验证码，所述第一验证码为
25 所述平台服务器根据第二手机号码指示所述信息提供服务器发送所述第一手机号码的，所述第二手机号码由所述第一加密密钥对所述第一手机号码加密得到；

将所述第一验证码通过第二手机号码发送给所述平台服务器；

在所述平台服务器对所述第一验证码与来自所述信息提供服务器的第二验证码进行验证后，确定所述用户登录成功，执行所述接收所述平台服务器返回的登录成功的第一
30 一响应消息的步骤。

5、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

在所述用户在所述平台服务器的第一登录信息与所述用户标识未绑定时，向所述平台服务器发送关联请求，所述关联请求中携带有所述信息提供服务器的第一标识；

接收来自所述平台服务器根据所述关联请求返回的第二提示信息；

5 根据所述第二提示信息确定所述用户在所述终端设备输入的第二原始验证信息；

根据所述第一加密密钥对所述第二原始验证信息进行加密，得到用于身份验证的第二验证信息，向所述平台服务器发送所述第二验证信息，所述平台服务器将所述绑定请求和所述第二验证信息转发至所述信息提供服务器，以供所述信息提供服务器根据与所述第一加密密钥对应的第一解密密钥对经过所述第二验证信息进行解密，根据解密后的
10 所述第二验证信息确定所述用户在所述信息提供服务器的用户标识，将所述用户标识返回所述平台服务器后，以供所述平台服务器建立所述第一登录信息和所述用户标识之间的绑定关系。

6、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

在所述用户在所述平台服务器和所述信息提供服务器上未注册时，通过所述平台服务器的第二加密密钥对所述终端设备的用户需要在所述信息提供服务器注册的第一注册信息进行加密；
15

在所述用户通过第一手机号码登录到所述信息提供服务器后，将通过所述第一加密密钥加密后的所述第一注册信息发送至所述信息提供服务器；

在所述信息提供服务器根据所述第一手机号码生成用户标识后，接收来自所述信息提供服务器的所述第一加密密钥、注册成功的第一响应消息以及所述第二手机号码，所述
20 所述第二手机号码由所述第一加密密钥对所述第一手机号码加密生成；

通过所述第二手机号码向所述平台服务器注册；

在所述平台服务器对所述第二手机号码注册后，接收所述平台服务器返回的注册成功的第二响应消息。

25 7、根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

向所述平台服务器发送用于获取所述平台服务器的第二加密密钥的第二请求消息；

接收所述平台服务器根据所述第二请求消息返回的第二加密密钥。

8、根据权利要求 6 所述的方法，其特征在于，所述通过所述第二手机号码向所述平台服务器注册的步骤，包括：

30 向所述平台服务器发送所述第二手机号码；

接收来自所述信息提供服务器返回的第三验证码,所述第三验证码为所述平台服务器根据所述第二手机号码请求所述信息提供服务器发送给所述终端设备的;

向所述平台服务器发送所述第三验证码;

在所述平台服务器根据所述第三验证码与所述信息提供服务器返回给所述平台服务器的第四验证码进行比较以确定验证通过后,执行所述接收所述平台服务器返回的注册成功的第二响应消息的步骤。

9、一种获取电子文件的方法,应用在平台服务器上,其特征在于,所述方法包括:

接收来自终端设备的用于获取电子文件的第一请求消息,所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识;

10 根据所述第一请求消息向所述终端设备返回第一提示信息;

在所述终端设备根据所述第一提示信息确定用于身份验证的第一验证信息后,接收来自所述终端设备的第一验证信息;

根据所述第一标识确定所述信息提供服务器,将所述第一验证信息、所述终端设备的用户在所述信息提供服务器注册的用户标识发送至所述信息提供服务器;

15 在所述信息提供服务器对所述第一验证信息验证通过并根据所述用户标识确定所述电子文件后,接收来自所述信息提供服务器的所述电子文件,将所述电子文件转发至所述终端设备,所述电子文件中的隐私信息经过所述信息提供服务器的第一加密密钥加密。

20 10、根据权利要求9所述的方法,其特征在于,所述第一验证信息为所述用户在所述终端设备输入的原始验证信息通过所述第一加密密钥加密生成的。

11、根据权利要求9所述的方法,其特征在于,所述方法还包括:

在所述用户未登录到所述平台服务器时,确定所述用户在所述平台服务器上的第一登录信息;

在所述用户登录成功后,向所述终端设备返回登录成功的第一响应消息。

25 12、根据权利要求11所述的方法,其特征在于,所述方法还包括:

通过所述终端设备的用户在所述平台服务器注册的第二手机号码指示所述信息提供服务器向所述终端设备发送第一验证码,所述第二手机号码由所述第一加密密钥对第一手机号码加密得到,所述第一手机号码为所述用户注册在所述信息提供服务器的手机号码;

30 在所述信息提供服务器通过所述信息提供服务器的第一解密密钥对所述第二手机

号码解密得到所述第一手机号码,通过所述第一手机号码向所述终端设备指示发送第一验证码后,接收来自所述终端设备的所述第一验证码以及接收来自所述信息提供服务器的第二验证码;

5 对所述第一验证码和所述第二验证码进行验证,在验证通过后确定所述用户登录成功,执行所述向所述终端设备返回登录成功的第一响应消息的步骤。

13、根据权利要求9所述的方法,其特征在于,所述方法还包括:

在所述用户在所述平台服务器的第一登录信息和所述用户在所述信息提供服务器注册的用户标识未绑定时,接收来自所述终端设备的关联请求,所述关联请求中携带有所述第一标识;

10 根据所述关联请求向所述终端设备返回第二提示信息;

在所述终端设备根据所述第二提示信息确定用于身份验证的第二验证信息,接收来自所述终端设备根据所述第二提示信息返回的所述第二验证信息,所述第二验证信息经过所述第一加密密钥加密;

15 将所述绑定请求和经过所述第一加密密钥的所述第二验证信息转发至所述信息提供服务器,以供所述信息提供服务器对经过所述第一加密密钥加密的所述第二验证信息进行解密,根据解密后的所述第二验证信息确定所述用户在所述信息提供服务器注册的用户标识;

接收来自所述信息提供服务器返回的所述用户标识,建立所述第一登录信息和所述用户标识之间的绑定关系。

20 14、根据权利要求9所述的方法,其特征在于,所述方法还包括:

在所述用户在所述平台服务器上未注册时,通过来自所述终端设备的第二注册信息进行注册;

根据所述第二注册信息向所述信息提供服务器获取第三验证码,指示所述信息提供服务器向所述第二手机号码对应的第一手机号码发送第四验证码;

25 接收来自所述终端设备的所述第四验证码;

对所述第三验证码和所述第四验证码进行验证;

在所述平台服务器对所述第三验证码和所述第四验证码验证通过后,向所述终端设备返回注册成功的第二响应消息。

15、根据权利要求14所述的方法,其特征在于,所述方法还包括:

30 接收来自所述终端设备的用于获取所述平台服务器的第二加密密钥的第二请求消

息；

根据所述第二请求消息向所述终端设备返回所述第二加密密钥。

16、一种获取电子文件的方法，应用在信息提供服务器上，其特征在于，所述方法包括：

5 接收来自平台服务器的第一验证信息、终端设备的用户在所述信息提供服务器注册的用户标识；

 对所述第一验证信息进行验证，在验证通过后根据所述用户标识确定所述电子文件；

 将所述电子文件中的隐私信息通过所述信息提供服务器的第一加密密钥加密；

10 将所述电子文件发送至所述平台服务器，以供所述平台服务器将所述电子文件转发至所述终端设备。

 17、根据权利要求 16 所述的方法，其特征在于，所述对所述第一验证信息进行验证的步骤，包括：

 通过所述信息提供服务器的所述第一解密密钥对所述第一验证信息进行解密；

15 通过所述平台服务器的第二加密密钥对所述解密后的所述第一验证信息进行加密，得到第一加密字符串；

 确定所述用户在所述信息提供服务器注册时生成的第二加密字符串，所述第二加密字符串由所述第一验证信息通过所述平台服务器的第二加密密钥加密生成；

20 确定所述第一加密字符串和所述第二加密字符串是否相同，如果相同，则所述第一验证信息的验证通过。

 18、根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

 在所述用户未登录到所述平台服务器时，接收来自所述平台服务器用于指示所述信息提供服务器向所述用户在所述平台服务器注册的第二手机号码发送第一验证码的指示消息，其中，所述第二手机号码由所述第一加密密钥对第一手机号码加密得到，所述
25 第一手机号码为所述用户注册在所述信息提供服务器的手机号码；

 根据所述指示消息通过所述第一解密密钥对所述第二手机号码进行解密，得到所述第一手机号码；

 通过所述第一手机号码向所述终端设备发送第一验证码以及向所述平台服务器返回第二验证码，以供所述平台服务器根据所述第一验证码和所述第二验证码对所述用户
30 进行登录验证。

19、根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

在所述用户在所述平台服务器的第一登录信息与所述用户标识未绑定时，接收来自所述平台服务器的第二验证信息和所述平台服务器的第二加密密钥，所述第二验证信息经过所述第一加密密钥加密；

5 通过所述信息提供服务器的第一解密密钥对所述第二验证信息进行解密，通过所述第二加密密钥对解密后的所述第二原始验证信息进行加密，得到第三加密字符串；

确定所述用户在所述信息提供服务器注册时生成的第四加密字符串，所述第四加密字符串由所述第二原始验证信息通过所述平台服务器的第二加密密钥加密生成；

确定所述第三加密字符串和所述第四加密字符串是否相同；

10 如果相同，向所述平台服务器返回所述终端设备的用户在所述信息提供服务器上注册的用户标识，以供所述平台服务器建立所述第一登录信息和所述用户标识的绑定关系。

20、根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

15 在所述用户在所述信息提供服务器上未注册时，通过来自所述终端设备的第一注册信息进行注册；

在所述用户通过第一手机号码登录到所述信息提供服务器后，将所述第一手机号码通过所述第一加密密钥进行加密，得到第二手机号码；

将所述第二手机号码发送至所述终端设备，以供所述终端设备通过所述第二手机号码在所述平台服务器上注册；

20 根据所述第一手机号码生成用户标识。

21、根据权利要求 20 所述的方法，其特征在于，所述方法还包括：

接收来自平台服务器的第二手机号码；

通过所述第一解密密钥对所述第二手机号码进行解密，得到所述第一手机号码；

25 通过所述第一手机号码向所述终端设备返回第三验证码，所述第三验证码为所述平台服务器根据所述第二注册信息请求所述信息提供服务器发送给所述终端设备的；

向所述平台服务器返回第四验证码，以供所述平台服务器对所述第三验证码和所述第四验证码进行比较以确定验证是否通过。

22、一种获取电子文件的装置，应用在终端设备上，其特征在于，所述装置包括：

30 第一发送模块，用于向平台服务器发送用于获取电子文件的第一请求消息，所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识；

第一接收模块,用于接收来自所述平台服务器根据所述第一发送模块发送的所述第一请求消息返回的第一提示信息;

第一确定模块,用于根据所述第一接收模块接收到的所述第一提示信息确定用于身份验证的第一验证信息,向所述平台服务器发送所述第一验证信息;

5 第二接收模块,用于在所述平台服务器根据所述第一标识确定所述信息提供服务器,以及根据所述终端设备的用户在所述平台服务器的第一登录信息确定所述用户在所述信息提供服务器注册的用户标识,并将所述第一确定模块确定的所述第一验证信息、所述用户标识发送至所述信息提供服务器后,接收所述平台服务器转发的来自所述信息提供服务器的所述电子文件,所述电子文件中的隐私信息经过所述信息提供服务器的第一加密密钥加密。

23、根据权利要求 22 所述的装置,其特征在于,所述第一确定模块包括:

第一确定单元,用于根据所述第一提示信息确定所述用户在所述终端设备输入的第一原始验证信息以及确定所述信息提供服务器的所述第一加密密钥;

15 第一加密单元,用于根据所述第一确定单元确定的所述第一加密密钥对所述第一原始验证信息进行加密,得到用于身份验证的第一验证信息。

24、根据权利要求 22 所述的装置,其特征在于,所述装置还包括:

第二确定模块,用于在所述用户未登录到所述平台服务器时,确定所述用户的第一登录信息,通过所述第一登录信息登录所述平台服务器;

20 第三接收模块,用于在所述第二确定模块确定所述用户登录成功后,接收所述平台服务器返回的登录成功的第一响应消息。

25、根据权利要求 24 所述的装置,其特征在于,所述装置还包括:

25 第四接收模块,用于通过第一手机号码接收来自所述信息提供服务器的第一验证码,所述第一验证码为所述平台服务器根据第二手机号码指示所述信息提供服务器发送所述第一手机号码的,所述第二手机号码由所述第一加密密钥对所述第一手机号码加密得到;

第二发送模块,用于将所述第四接收模块接收到的所述第一验证码通过第二手机号码发送给所述平台服务器;

30 第三确定模块,用于在所述平台服务器对所述第二发送模块发送的所述第一验证码与来自所述信息提供服务器的第二验证码进行验证后,确定所述用户登录成功,所述第三接收模块执行所述接收所述平台服务器返回的登录成功的第一响应消息的步骤。

26、根据权利要求 22 所述的装置，其特征在于，所述装置还包括：

第三发送模块，用于在所述用户在所述平台服务器的第一登录信息与所述用户标识未绑定时，向所述平台服务器发送关联请求，所述关联请求中携带有所述信息提供服务器的第一标识；

5 第五接收模块，用于接收来自所述平台服务器根据所述第三发送模块发送的所述关联请求返回的第二提示信息；

第四确定模块，用于根据所述第五接收模块接收到的所述第二提示信息确定所述用户在所述终端设备输入的第二原始验证信息；

10 第一加密模块，用于根据所述第一加密密钥对所述第四确定模块确定的所述第二原始验证信息进行加密，得到用于身份验证的第二验证信息；

第四发送模块，用于向所述平台服务器发送所述第一加密模块加密的所述第二验证信息，所述平台服务器将所述绑定请求和所述第二验证信息转发至所述信息提供服务器，以供所述信息提供服务器根据与所述第一加密密钥对应的第一解密密钥对经过所述第二验证信息进行解密，根据解密后的所述第二验证信息确定所述用户在所述信息提供服务器的用户标识，将所述用户标识返回所述平台服务器后，以供所述平台服务器建立所述

15 所述第一登录信息和所述用户标识之间的绑定关系。

27、根据权利要求 22 所述的装置，其特征在于，所述装置还包括：

20 第二加密模块，用于在所述用户在所述平台服务器和所述信息提供服务器上未注册时，通过所述平台服务器的第二加密密钥对所述终端设备的用户需要在所述信息提供服务器注册的第一注册信息进行加密；

第五发送模块，用于在所述用户通过第一手机号码登录到所述信息提供服务器后，将通过所述第一加密密钥加密后的所述第一注册信息发送至所述信息提供服务器；

25 第六接收模块，用于在所述信息提供服务器根据所述第一手机号码生成用户标识后，接收来自所述信息提供服务器的所述第一加密密钥、注册成功的第一响应消息以及所述第二手机号码，所述第二手机号码由所述第一加密密钥对所述第一手机号码加密生成；

第一注册模块，用于通过所述第二手机号码向所述平台服务器注册；

第七接收模块，用于在所述平台服务器对所述第二手机号码注册后，接收所述平台服务器返回的注册成功的第二响应消息。

30 28、根据权利要求 27 所述的装置，其特征在于，所述装置还包括：

第六发送模块，用于向所述平台服务器发送用于获取所述平台服务器的第二加密密钥的第二请求消息；

第八接收模块，用于接收所述平台服务器根据所述第六发送模块发送的所述第二请求消息返回的第二加密密钥。

5 29、根据权利要求 27 所述的装置，其特征在于，所述第一注册模块包括：

第一发送单元，用于向所述平台服务器发送所述第二手机号码；

第一接收单元，用于接收来自所述信息提供服务器返回的第三验证码，所述第三验证码为所述平台服务器根据所述第一发送单元发送的所述第二手机号码请求所述信息提供服务器发送给所述终端设备的；

10 第二发送单元，用于向所述平台服务器发送所述第一接收单元接收到的所述第三验证码；

在所述平台服务器根据所述第三验证码与所述信息提供服务器返回给所述平台服务器的第四验证码进行比较以确定验证通过后，所述第七接收模块执行所述接收所述平台服务器返回的注册成功的第二响应消息的步骤。

15 30、一种获取电子文件的装置，应用在平台服务器上，其特征在于，所述装置包括：

第九接收模块，用于接收来自终端设备的用于获取电子文件的第一请求消息，所述第一请求消息中携带有提供所述电子文件的信息提供服务器的第一标识；

第七发送模块，用于根据所述第九接收模块接收到的所述第一请求消息向所述终端设备返回第一提示信息；

20 第八发送模块，用于在所述终端设备根据所述第七发送模块发送的所述第一提示信息确定用于身份验证的第一验证信息后，接收来自所述终端设备的第一验证信息；

第九发送模块，用于根据所述第九接收模块接收到的所述第一标识确定所述信息提供服务器，将所述第一验证信息、所述终端设备的用户在所述信息提供服务器注册的用户标识发送至所述信息提供服务器；

25 第一转发模块，用于在所述信息提供服务器对所述第九发送模块发送的所述第一验证信息验证通过并根据所述用户标识确定所述电子文件后，接收来自所述信息提供服务器的所述电子文件，将所述电子文件转发至所述终端设备，所述电子文件中的隐私信息经过所述信息提供服务器的第一加密密钥加密。

30 31、根据权利要求 30 所述的装置，其特征在于，所述第一验证信息为所述用户在所述终端设备输入的原始验证信息通过所述第一加密密钥加密生成的。

32、根据权利要求 30 所述的装置，其特征在于，所述装置还包括：

第五确定模块，用于在所述用户未登录到所述平台服务器时，确定所述用户在所述平台服务器上的第一登录信息；

第十发送模块，用于在所述第五确定模块确定所述用户登录成功后，向所述终端设备返回登录成功的第一响应消息。

33、根据权利要求 32 所述的装置，其特征在于，所述装置还包括：

第十一发送模块，用于通过所述终端设备的用户在所述平台服务器注册的第二手机号码指示所述信息提供服务器向所述终端设备发送第一验证码，所述第二手机号码由所述第一加密密钥对第一手机号码加密得到，所述第一手机号码为所述用户注册在所述信息提供服务器的手机号码；

第十接收模块，用于在所述信息提供服务器通过所述信息提供服务器的第一解密密钥对所述第二手机号码解密得到所述第一手机号码，通过所述第一手机号码向所述终端设备指示发送第一验证码后，接收来自所述终端设备的所述第一验证码以及接收来自所述信息提供服务器的第二验证码；

第一验证模块，用于对所述第一验证码和所述第二验证码进行验证，在验证通过后确定所述用户登录成功，所述第十发送模块执行所述向所述终端设备返回登录成功的第一响应消息的步骤。

34、根据权利要求 30 所述的装置，其特征在于，所述装置还包括：

第十一接收模块，用于在所述用户在所述平台服务器的第一登录信息和所述用户在所述信息提供服务器注册的用户标识未绑定时，接收来自所述终端设备的关联请求，所述关联请求中携带有所述第一标识；

第十二发送模块，用于根据所述关联请求向所述终端设备返回第二提示信息；

第十二接收模块，用于在所述终端设备根据所述第二提示信息确定用于身份验证的第二验证信息，接收来自所述终端设备根据所述第二提示信息返回的所述第二验证信息，所述第二验证信息经过所述第一加密密钥加密；

第二转发模块，用于将所述绑定请求和经过所述第一加密密钥的所述第二验证信息转发至所述信息提供服务器，以供所述信息提供服务器对经过所述第一加密密钥加密的所述第二验证信息进行解密，根据解密后的所述第二验证信息确定所述用户在所述信息提供服务器注册的用户标识；

第十三接收模块，用于接收来自所述信息提供服务器返回的所述用户标识，建立所

述第一登录信息和所述用户标识之间的绑定关系。

35、根据权利要求 30 所述的装置，其特征在于，所述装置还包括：

第二注册模块，用于在所述用户在所述平台服务器上未注册时，通过来自所述终端设备的第二注册信息进行注册；

5 第一获取模块，用于根据所述第二注册模块注册的所述第二注册信息向所述信息提供服务器获取第三验证码，指示所述信息提供服务器向所述第二手机号码对应的第一手机号码发送第四验证码；

第十四接收模块，用于接收来自所述终端设备的所述第四验证码；

第二验证模块，用于对所述第三验证码和所述第四验证码进行验证；

10 第十三发送模块，用于在所述第二验证模块对所述第三验证码和所述第四验证码验证通过后，向所述终端设备返回注册成功的第二响应消息。

36、根据权利要求 35 所述的装置，其特征在于，所述装置还包括：

第十五接收模块，用于接收来自所述终端设备的用于获取所述平台服务器的第二加密密钥的第二请求消息；

15 第十四发送模块，用于根据所述第十五接收模块接收到的所述第二请求消息向所述终端设备返回所述第二加密密钥。

37、一种获取电子文件的装置，应用在信息提供服务器上，其特征在于，所述装置包括：

20 第十六接收模块，用于接收来自平台服务器的第一验证信息、终端设备的用户在所述信息提供服务器注册的用户标识；

第三验证模块，用于对所述第十六接收模块接收到的所述第一验证信息进行验证，在验证通过后根据所述用户标识确定所述电子文件；

第三加密模块，用于将所述电子文件中的隐私信息通过所述信息提供服务器的第一加密密钥加密；

25 第十五发送模块，用于将所述第三加密模块加密后的所述电子文件发送至所述平台服务器，以供所述平台服务器将所述电子文件转发至所述终端设备。

38、根据权利要求 37 所述的装置，其特征在于，所述第三验证模块包括：

第一解密单元，用于通过所述信息提供服务器的所述第一解密密钥对所述第一验证信息进行解密；

30 第一加密单元，用于通过所述平台服务器的第二加密密钥对所述第一解密单元解密

后的所述第一验证信息进行加密，得到第一加密字符串；

第一确定单元，用于确定所述用户在所述信息提供服务器注册时生成的第二加密字符串，所述第二加密字符串由所述第一验证信息通过所述平台服务器的第二加密密钥加密生成；

- 5 第二确定单元，用于确定所述第一加密单元得到的所述第一加密字符串和所述第一确定单元确定的所述第二加密字符串是否相同，如果相同，则所述第一验证信息的验证通过。

39、根据权利要求 37 所述的装置，其特征在于，所述装置还包括：

- 10 第十七接收模块，用于在所述用户未登录到所述平台服务器时，接收来自所述平台服务器用于指示所述信息提供服务器向所述用户在所述平台服务器注册的第二手机号码发送第一验证码的指示消息，其中，所述第二手机号码由所述第一加密密钥对第一手机号码加密得到，所述第一手机号码为所述用户注册在所述信息提供服务器的手机号码；

- 15 第一解密模块，用于根据所述第十七接收模块接收到的所述指示消息通过所述第一解密密钥对所述第二手机号码进行解密，得到所述第一手机号码；

第十六发送模块，用于通过所述第一手机号码向所述终端设备发送第一验证码以及向所述平台服务器返回第二验证码，以供所述平台服务器根据所述第一验证码和所述第二验证码对所述用户进行登录验证。

40、根据权利要求 37 所述的装置，其特征在于，所述装置还包括：

- 20 第十八接收模块，用于在所述用户在所述平台服务器的第一登录信息与所述用户标识未绑定时，接收来自所述平台服务器的第二验证信息和所述平台服务器的第二加密密钥，所述第二验证信息经过所述第一加密密钥加密；

- 25 第二解密模块，用于通过所述信息提供服务器的第一解密密钥对所述第二验证信息进行解密，通过所述第二加密密钥对解密后的所述第二原始验证信息进行加密，得到第三加密字符串；

第六确定模块，用于确定所述用户在所述信息提供服务器注册时生成的第四加密字符串，所述第四加密字符串由所述第二原始验证信息通过所述平台服务器的第二加密密钥加密生成；

第七确定模块，用于确定所述第三加密字符串和所述第四加密字符串是否相同；

- 30 第十七发送模块，用于如果所述第七确定模块确定相同，向所述平台服务器返回所

述终端设备的用户在所述信息提供服务器上注册的用户标识，以供所述平台服务器建立所述第一登录信息和所述用户标识的绑定关系。

41、根据权利要求 37 所述的装置，其特征在于，所述装置还包括：

5 第三注册模块，用于在所述用户在所述信息提供服务器上未注册时，通过来自所述终端设备的第一注册信息进行注册；

第四加密模块，用于在所述用户通过第一手机号码登录到所述信息提供服务器后，将所述第一手机号码通过所述第一加密密钥进行加密，得到第二手机号码；

第十八发送模块，用于将所述第二手机号码发送至所述终端设备，以供所述终端设备通过所述第二手机号码在所述平台服务器上注册；

10 标识生成模块，用于根据所述第一手机号码生成用户标识。

42、根据权利要求 41 所述的装置，其特征在于，所述装置还包括：

第十九接收模块，用于接收来自平台服务器的第二手机号码；

第三解密模块，用于通过所述第一解密密钥对所述第二手机号码进行解密，得到所述

15 第十九发送模块，用于通过所述第一手机号码向所述终端设备返回第三验证码，所述第三验证码为所述平台服务器根据所述第二注册信息请求所述信息提供服务器发送给所述终端设备的；

第二十发送模块，用于向所述平台服务器返回第四验证码，以供所述平台服务器对所述第三验证码和所述第四验证码进行比较以确定验证是否通。

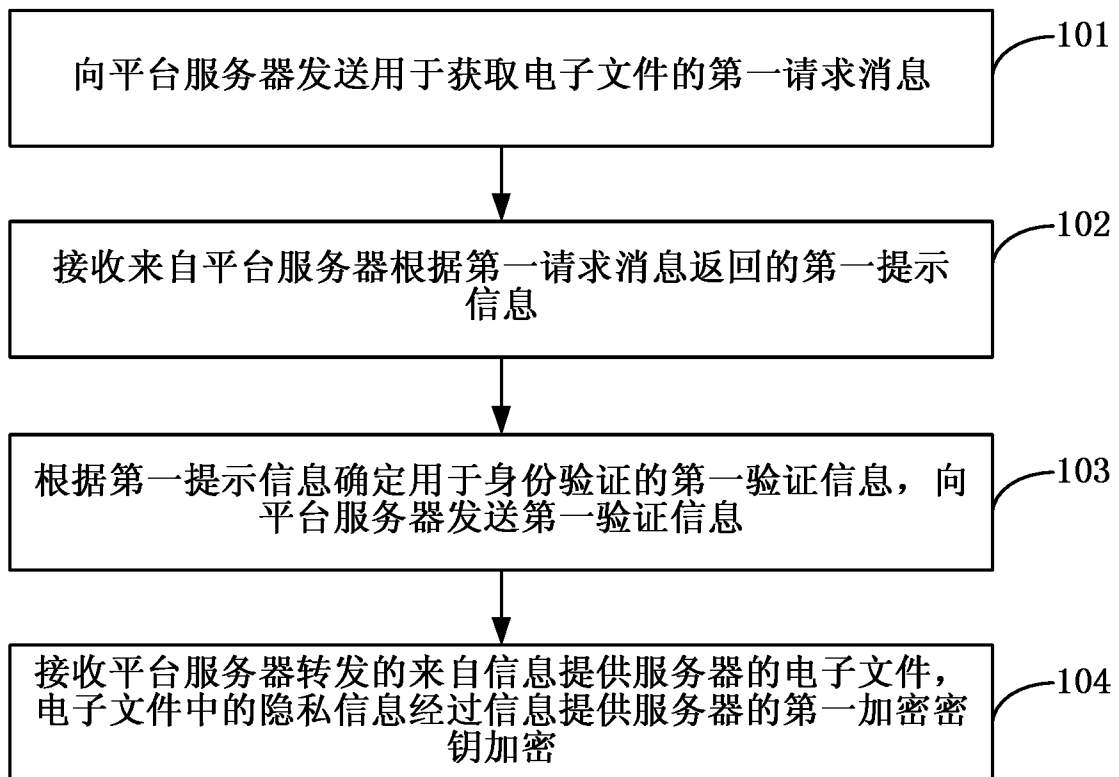


图 1

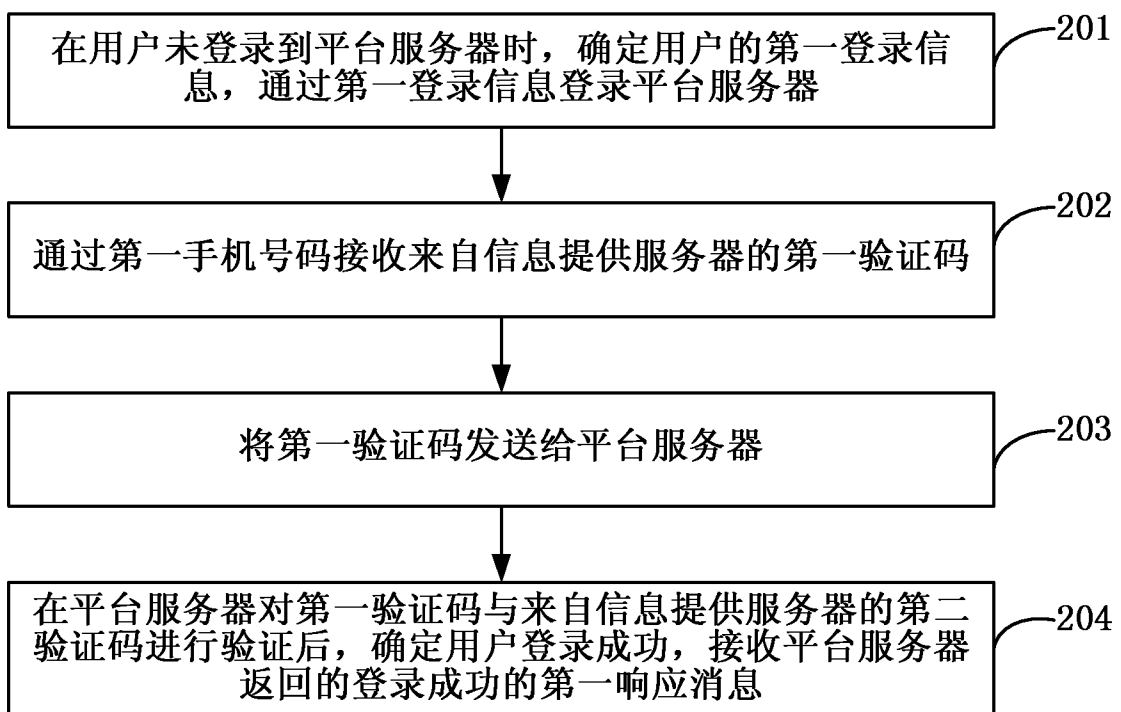


图 2

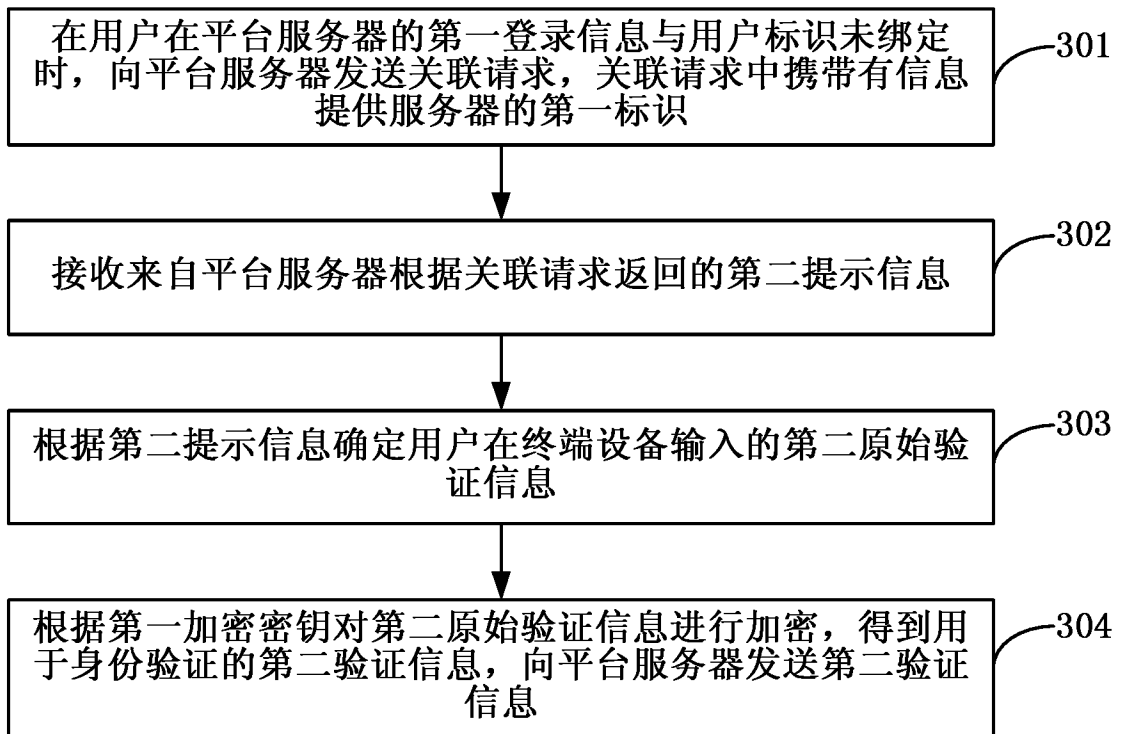


图 3

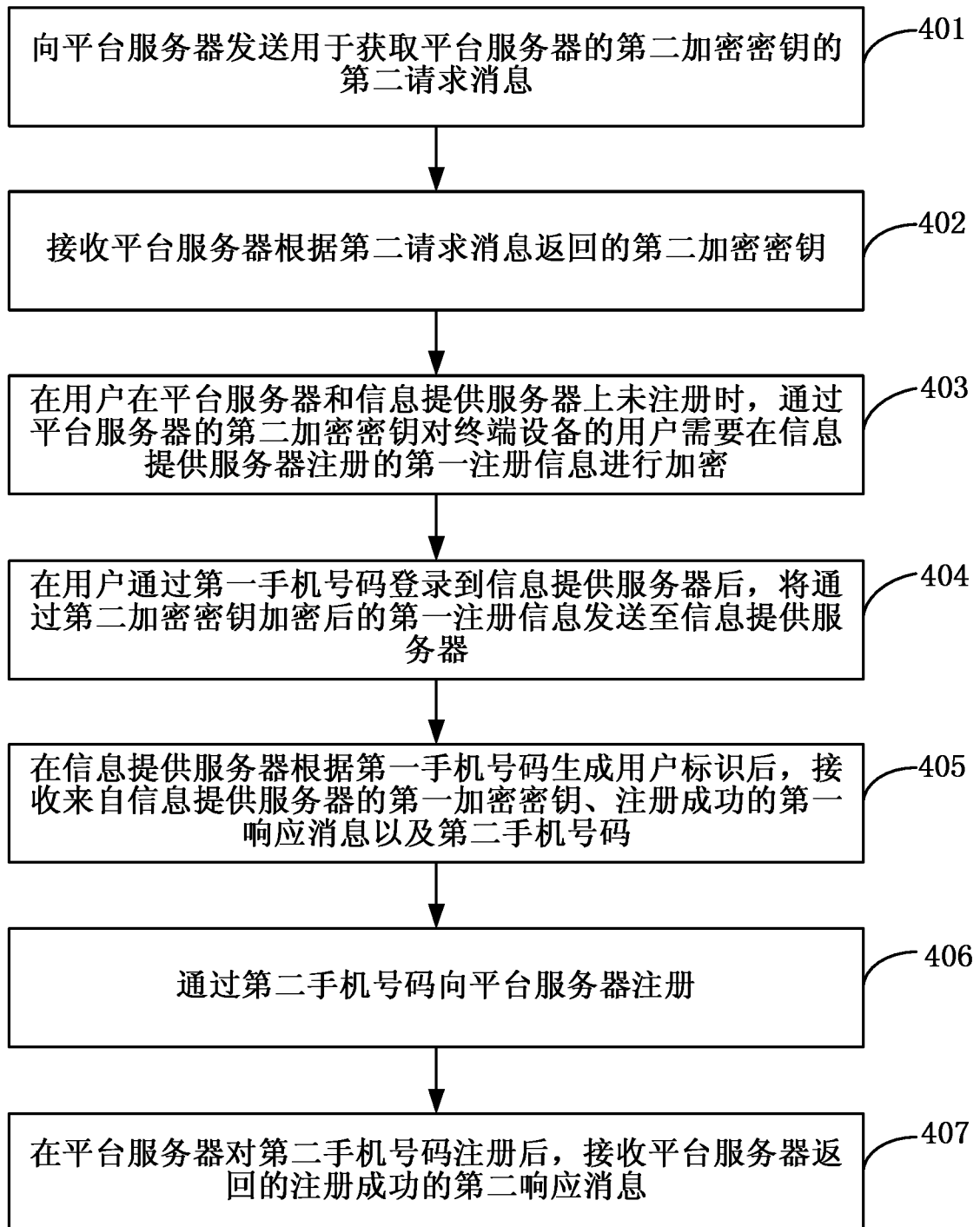


图 4

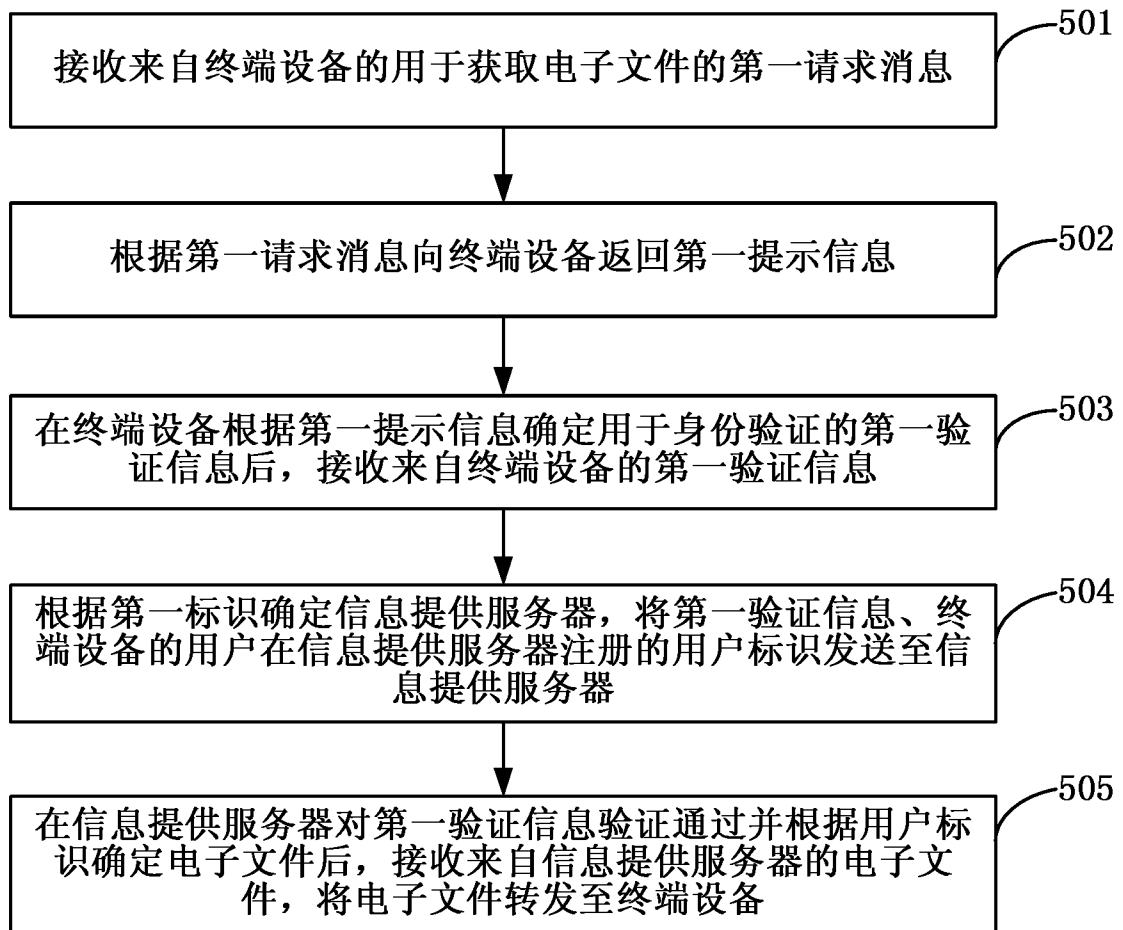


图 5

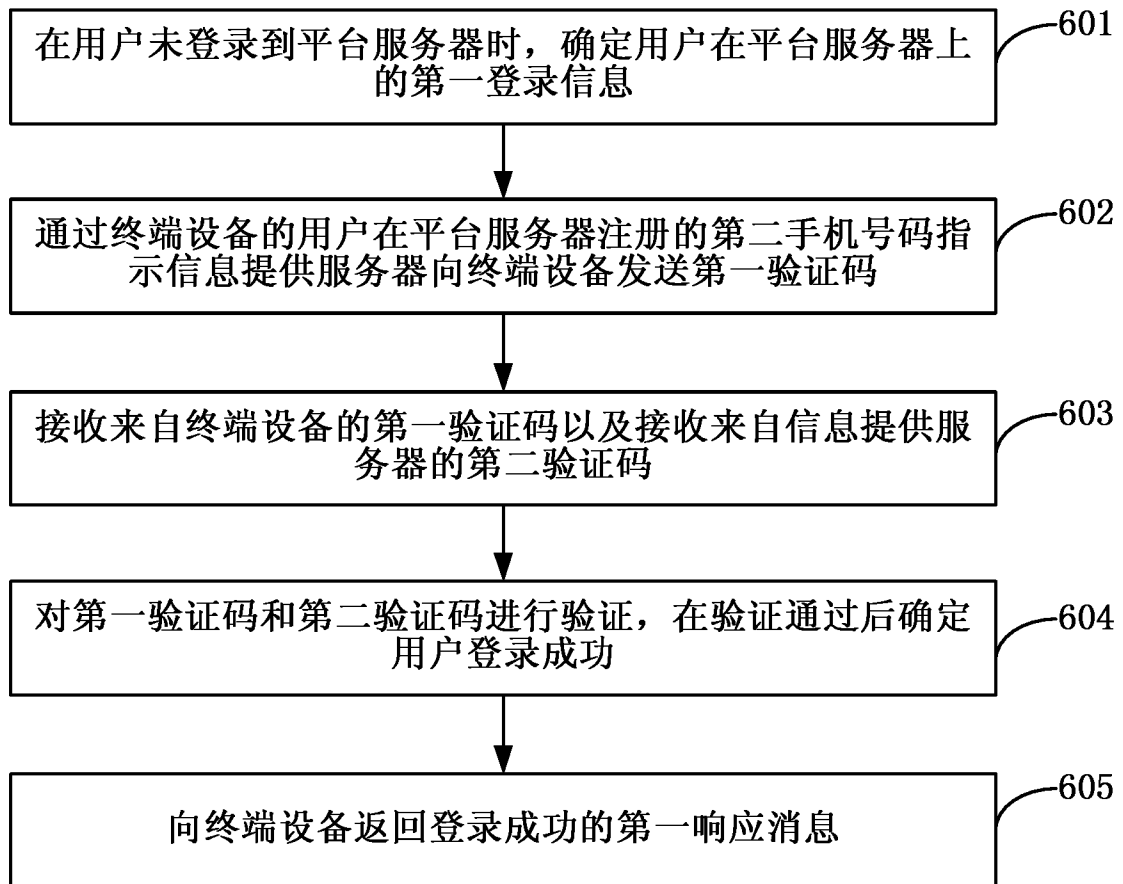


图 6

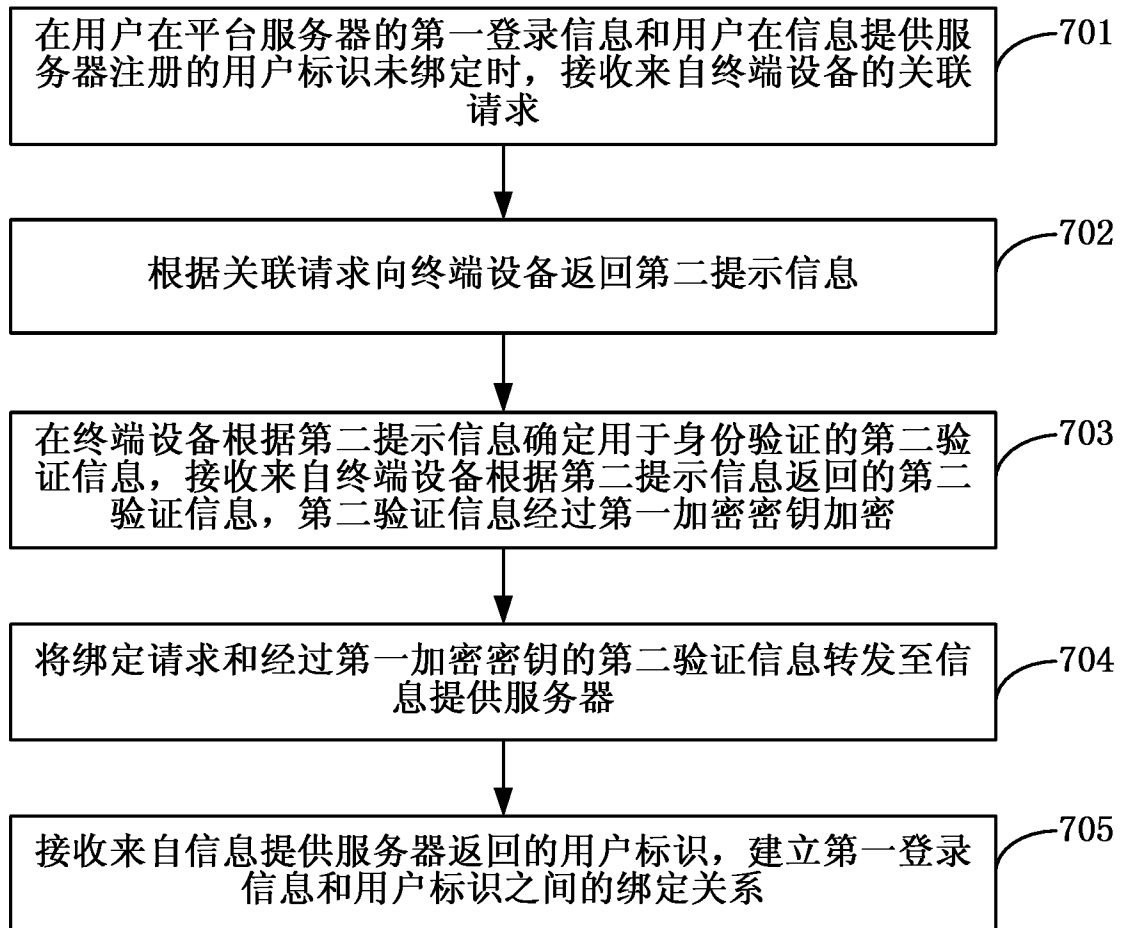


图 7

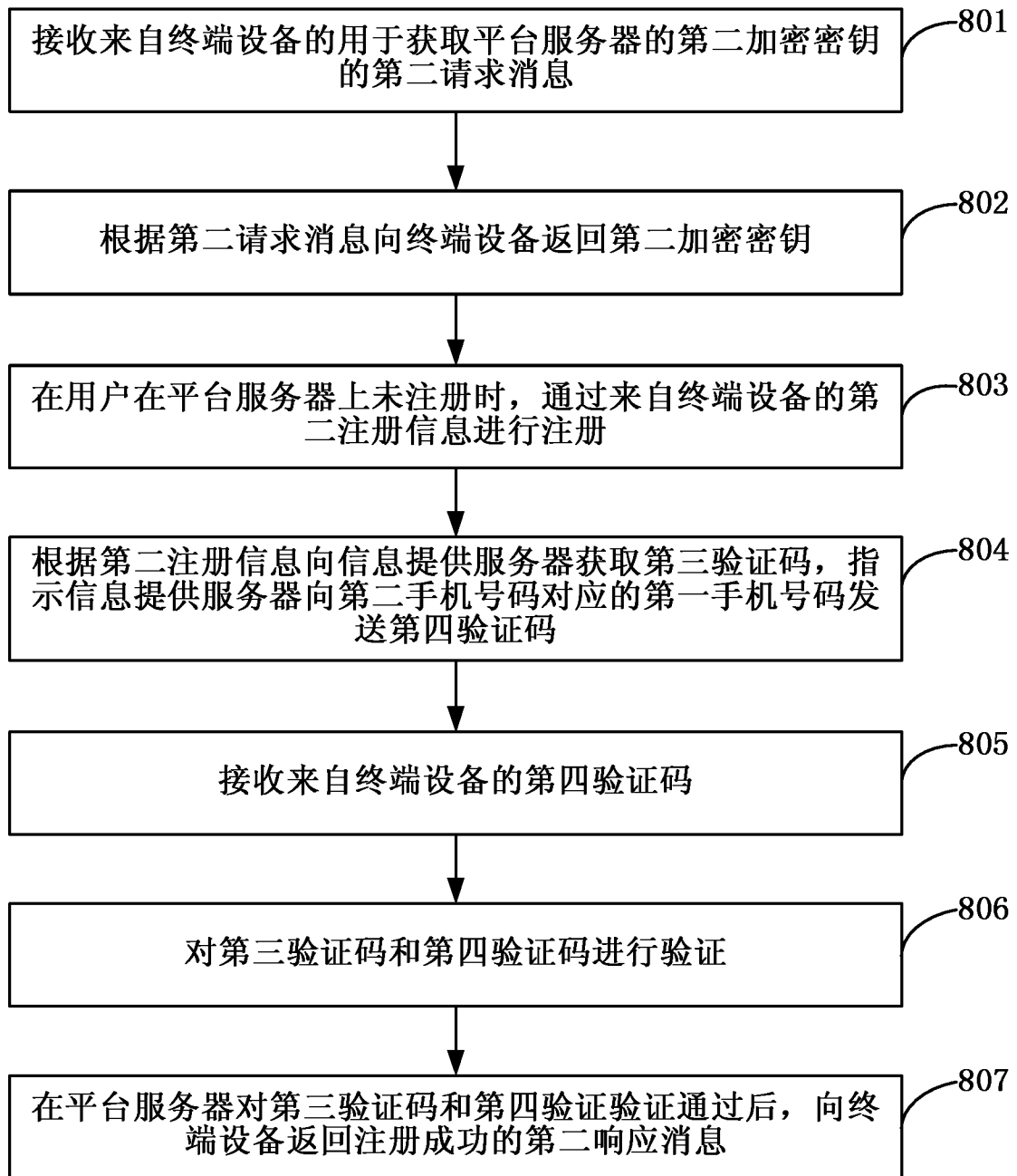


图 8

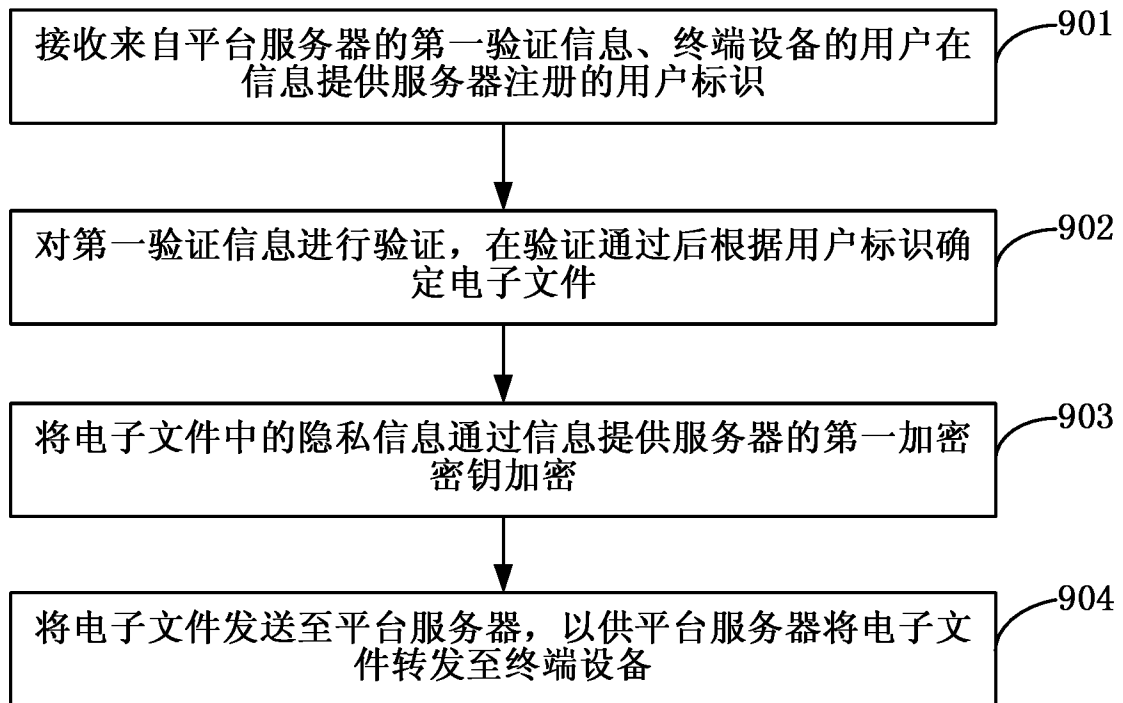


图 9

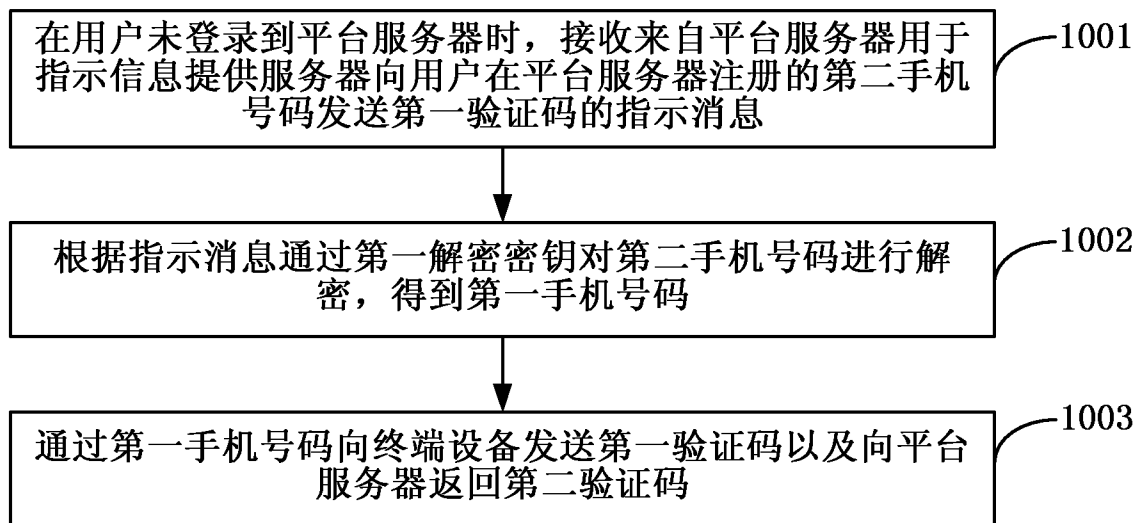


图 10

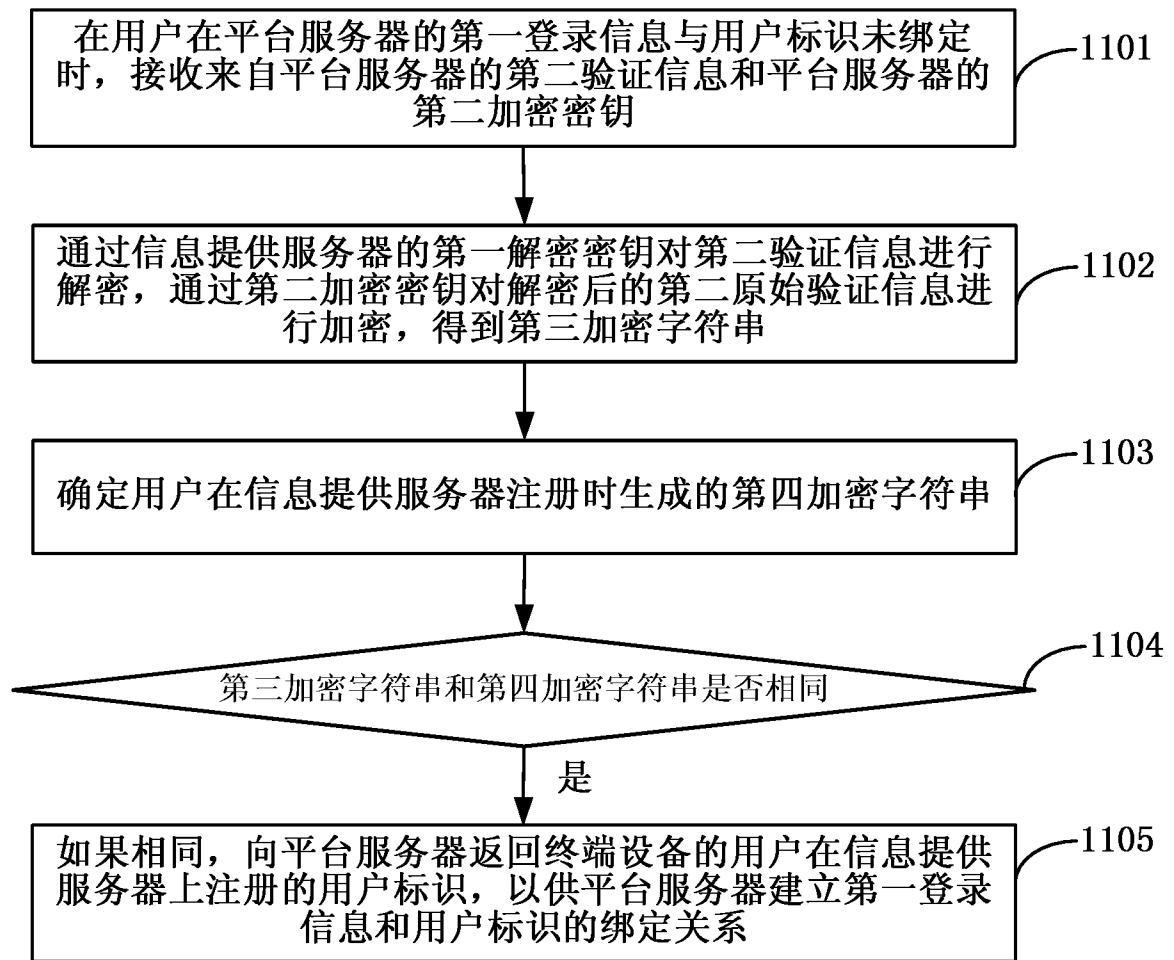


图 11

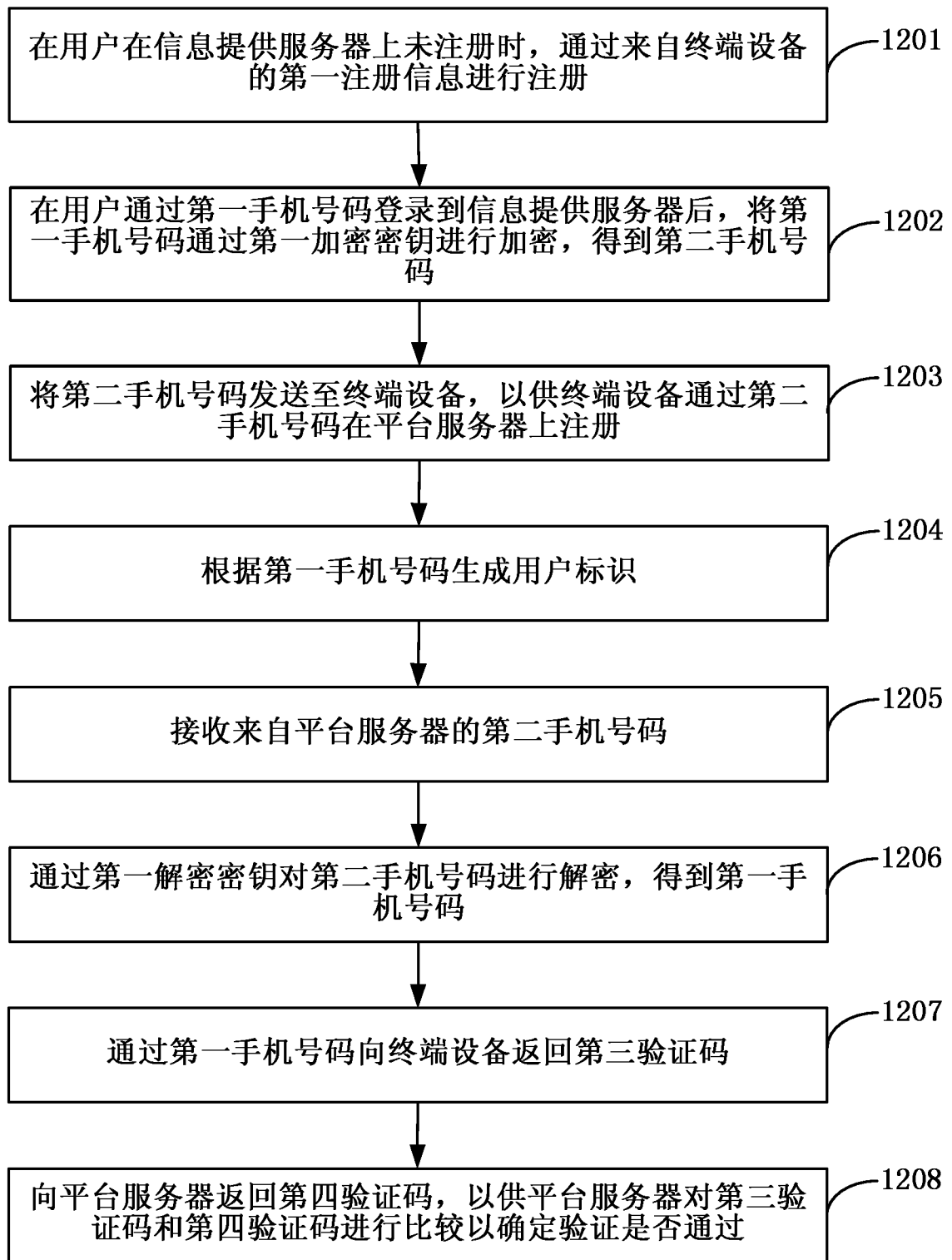


图 12

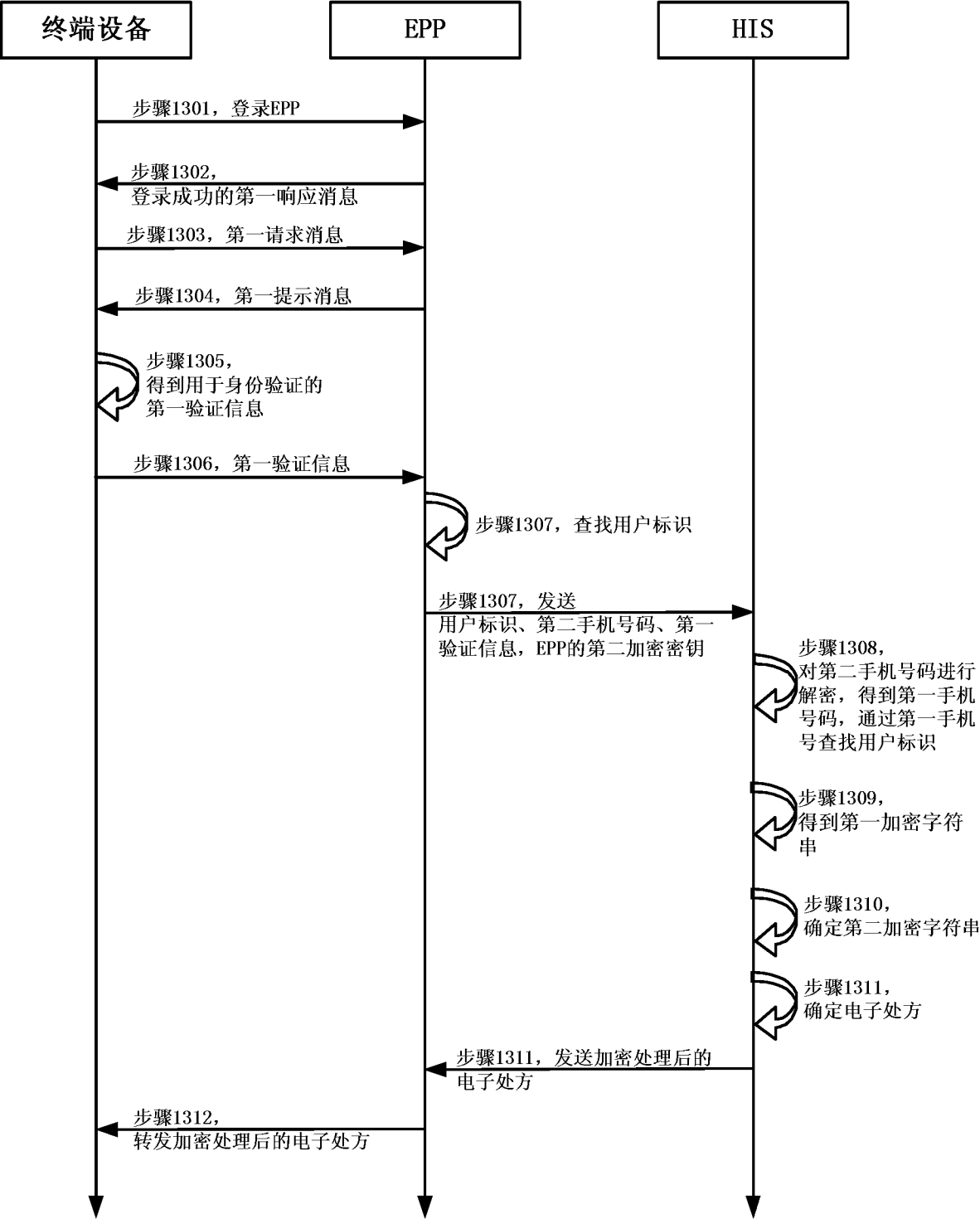


图 13

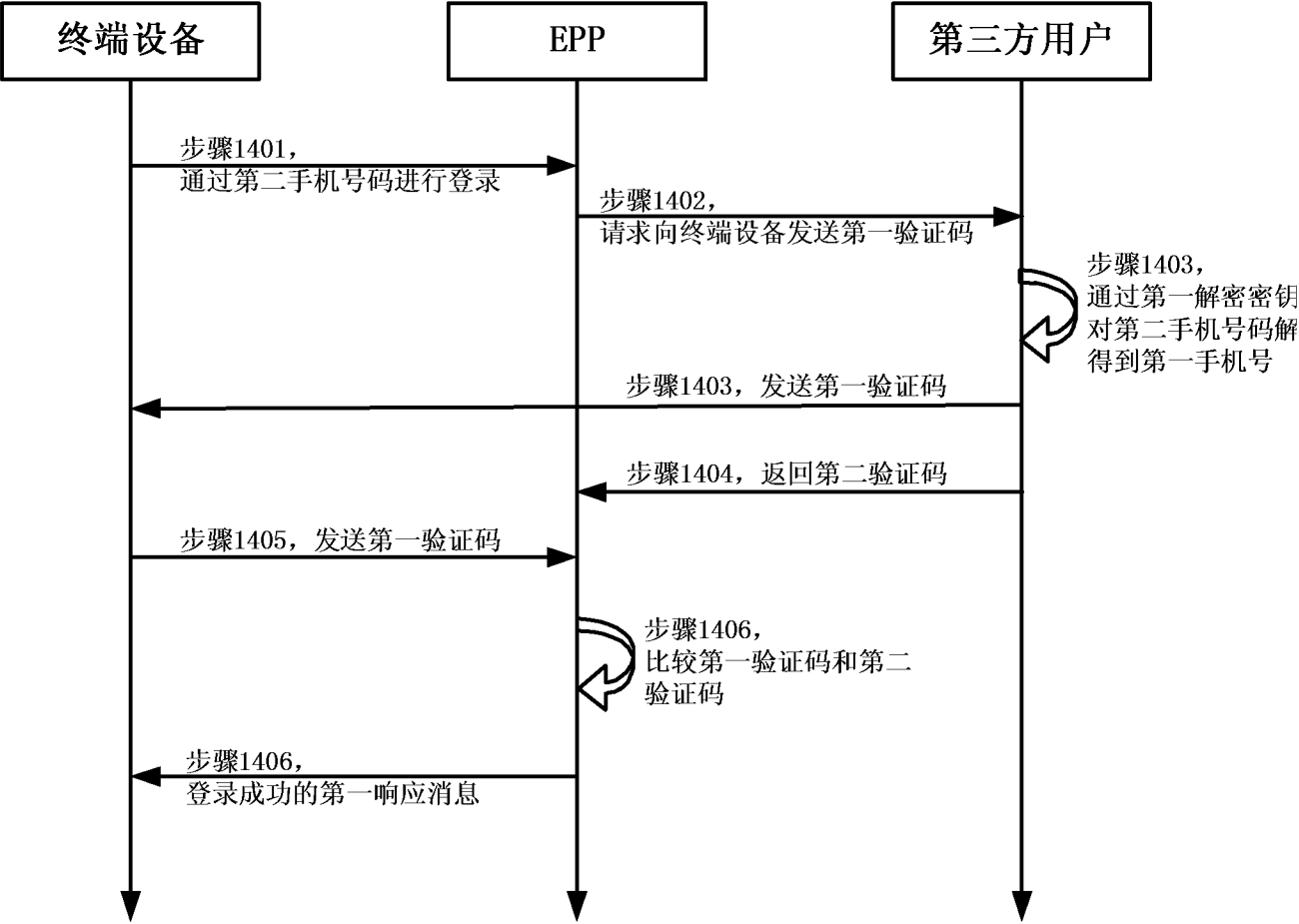


图 14

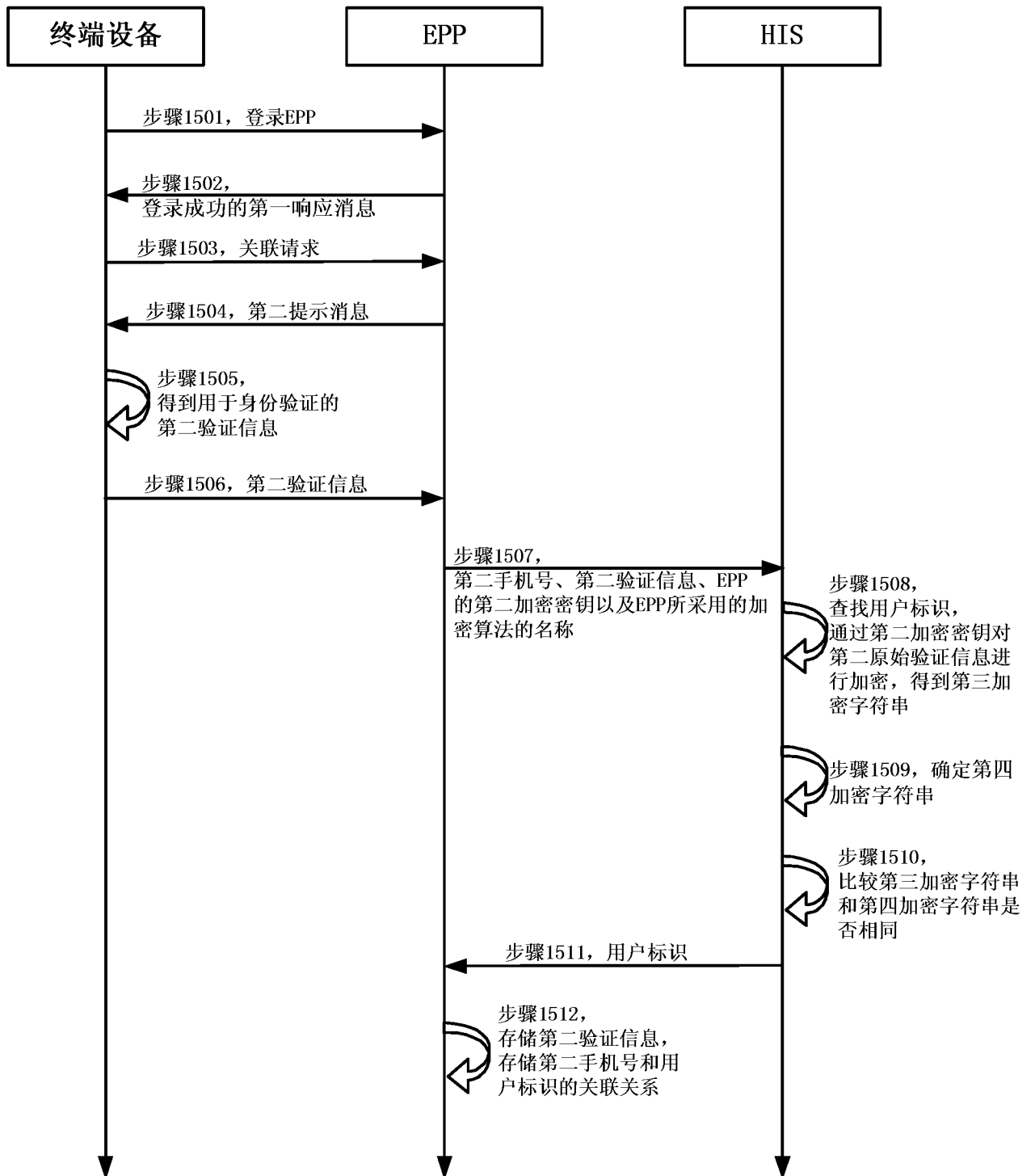


图 15

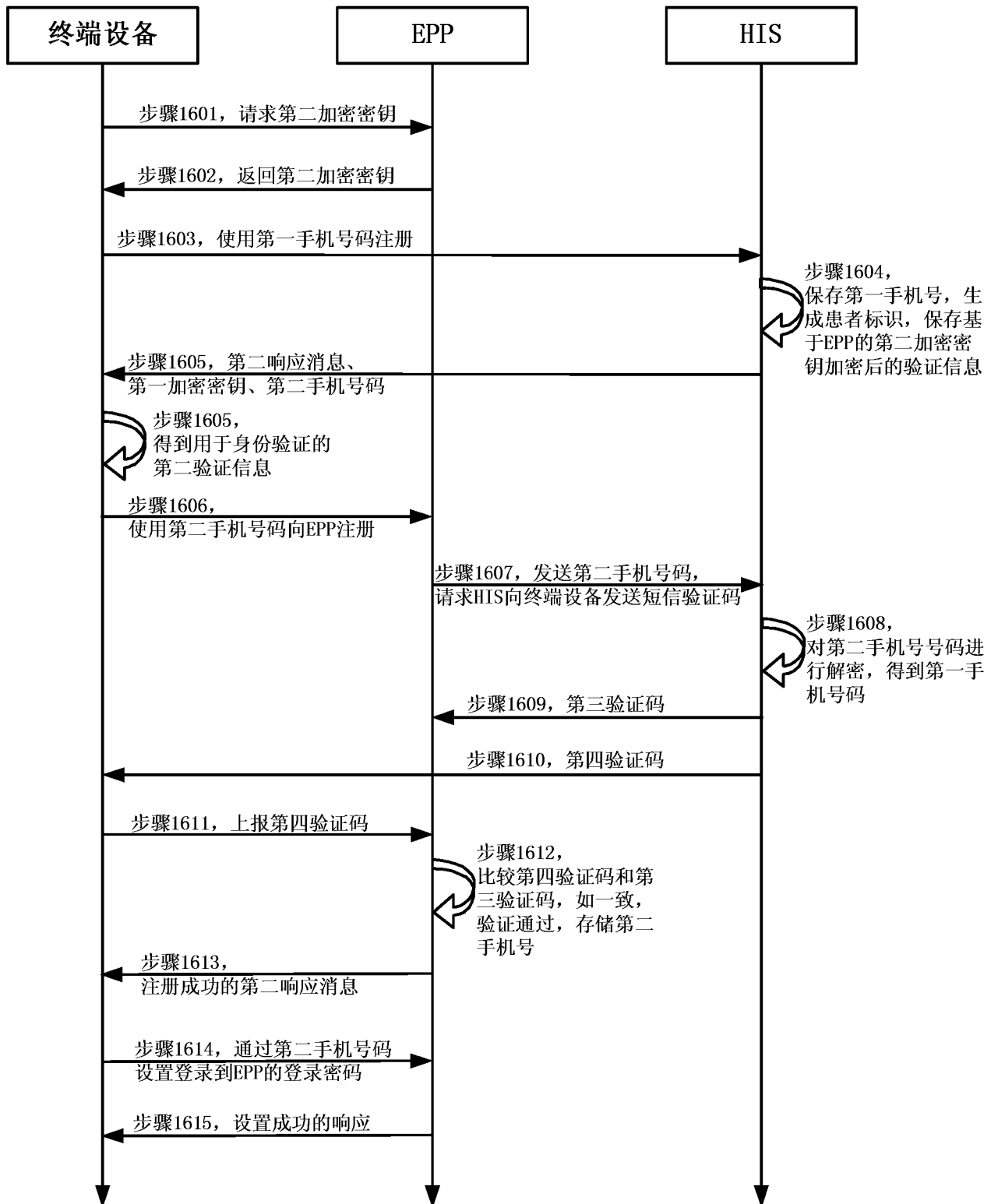


图 16

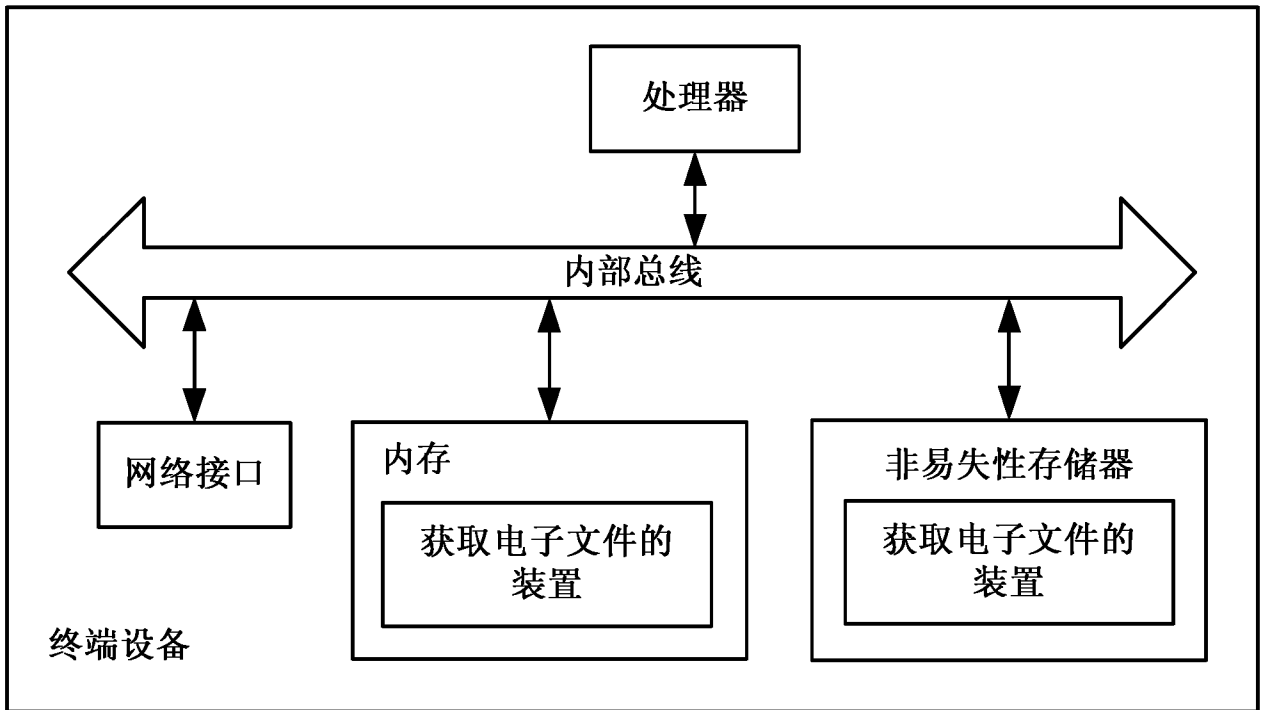


图 17

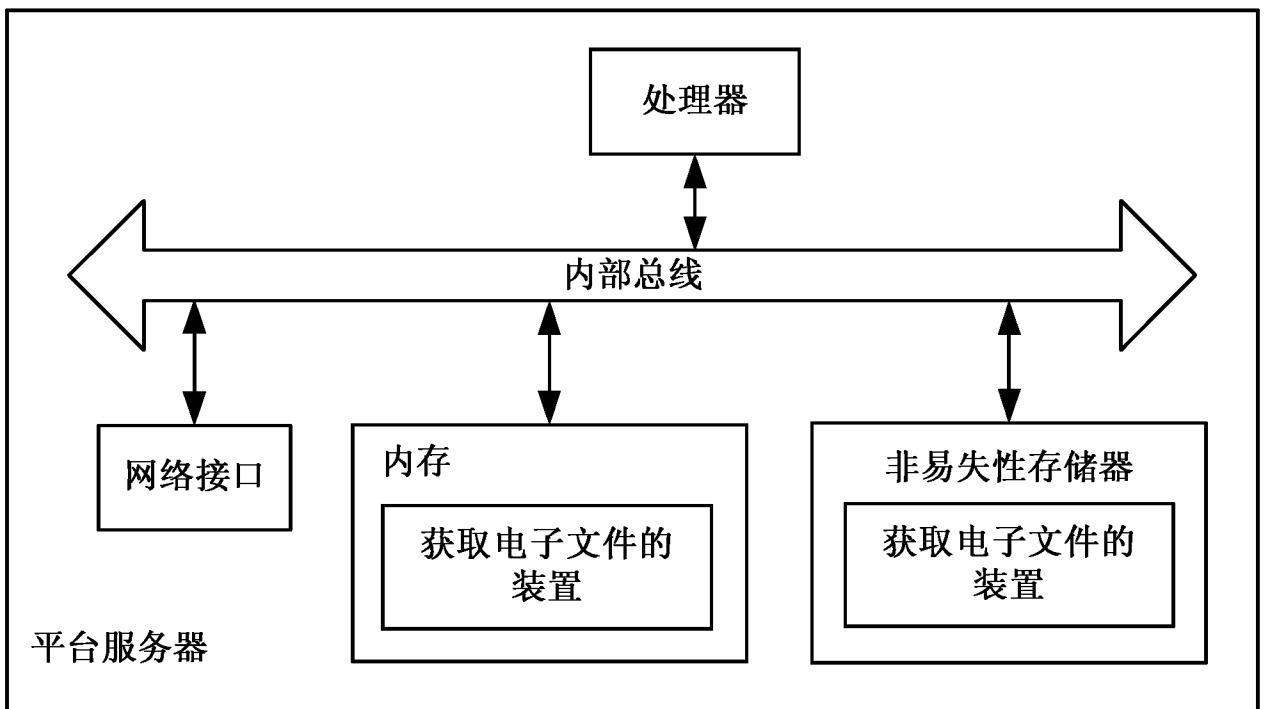


图 18

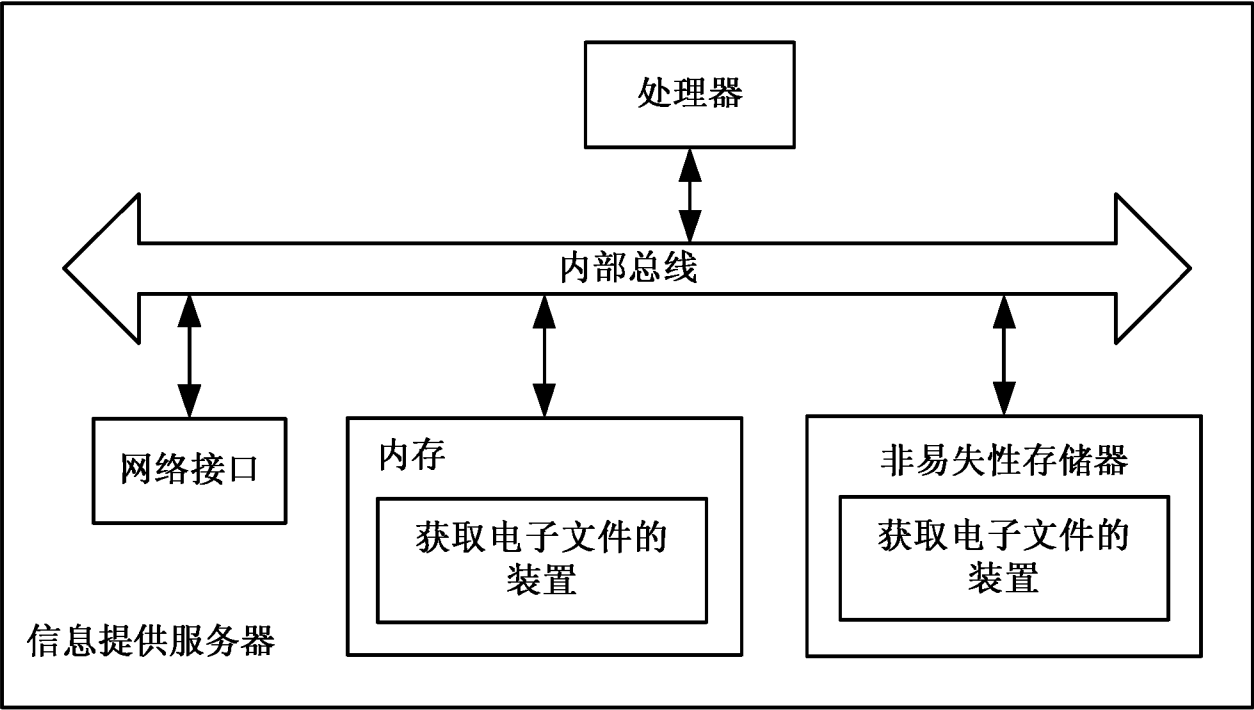


图 19

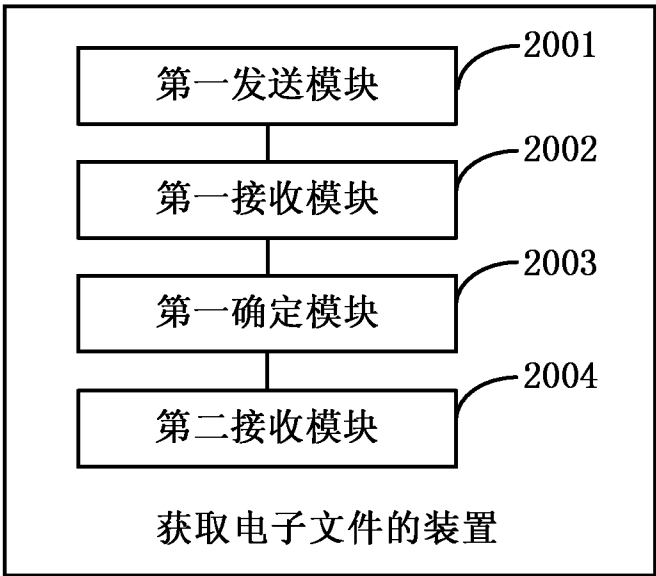


图 20

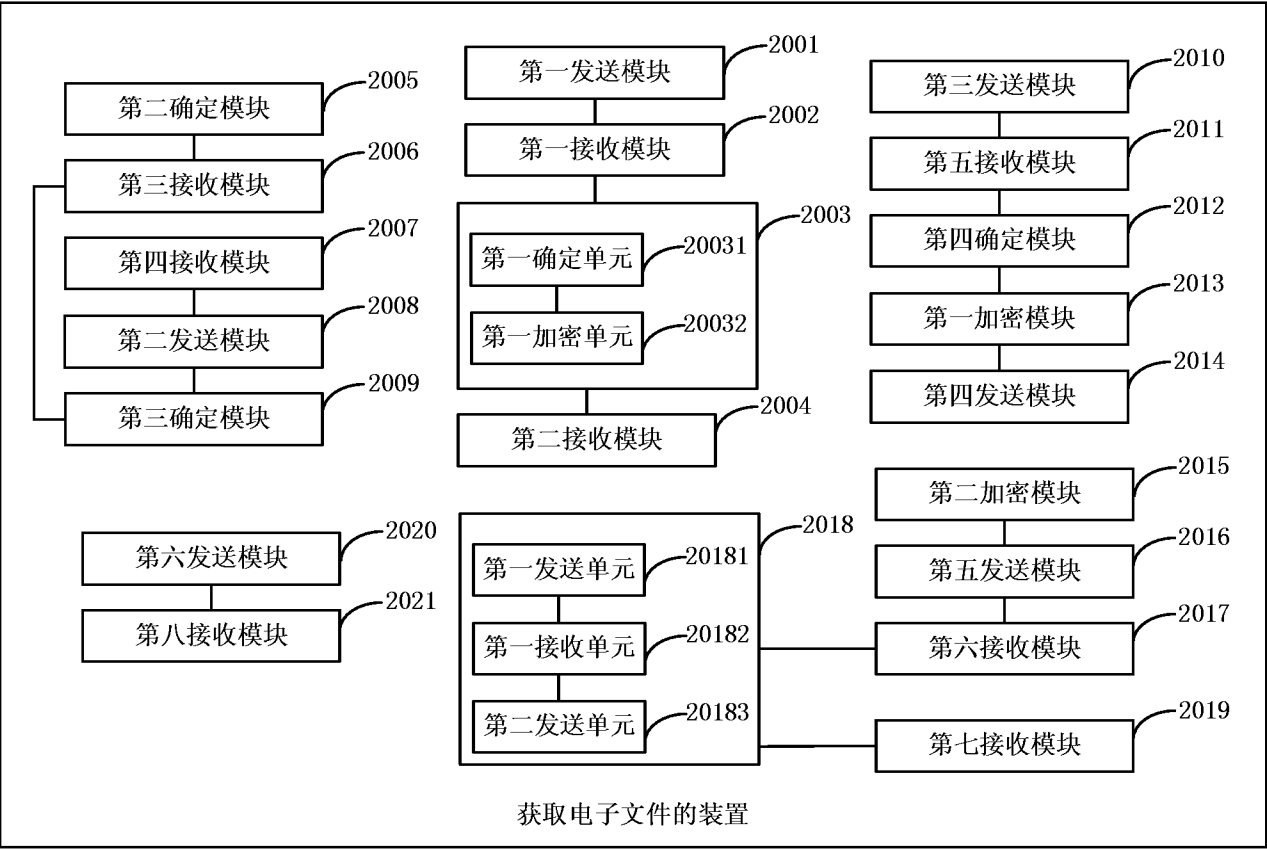


图 21

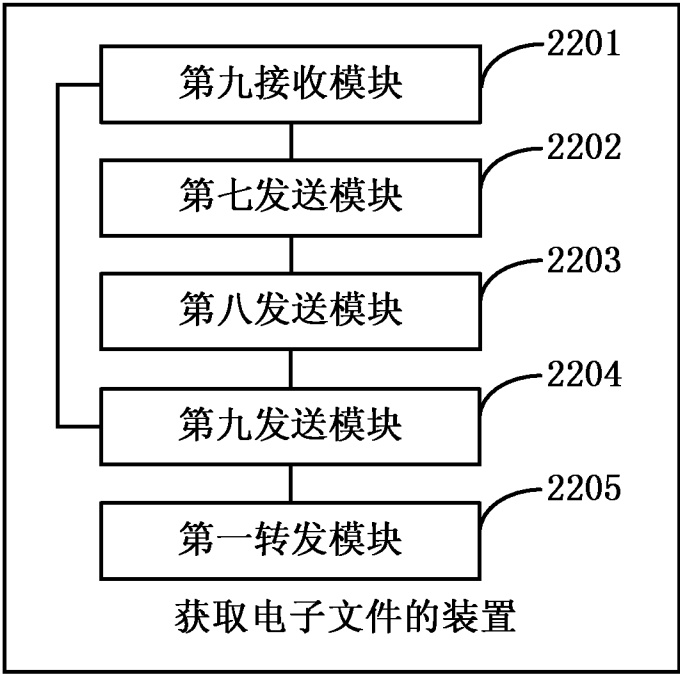


图 22

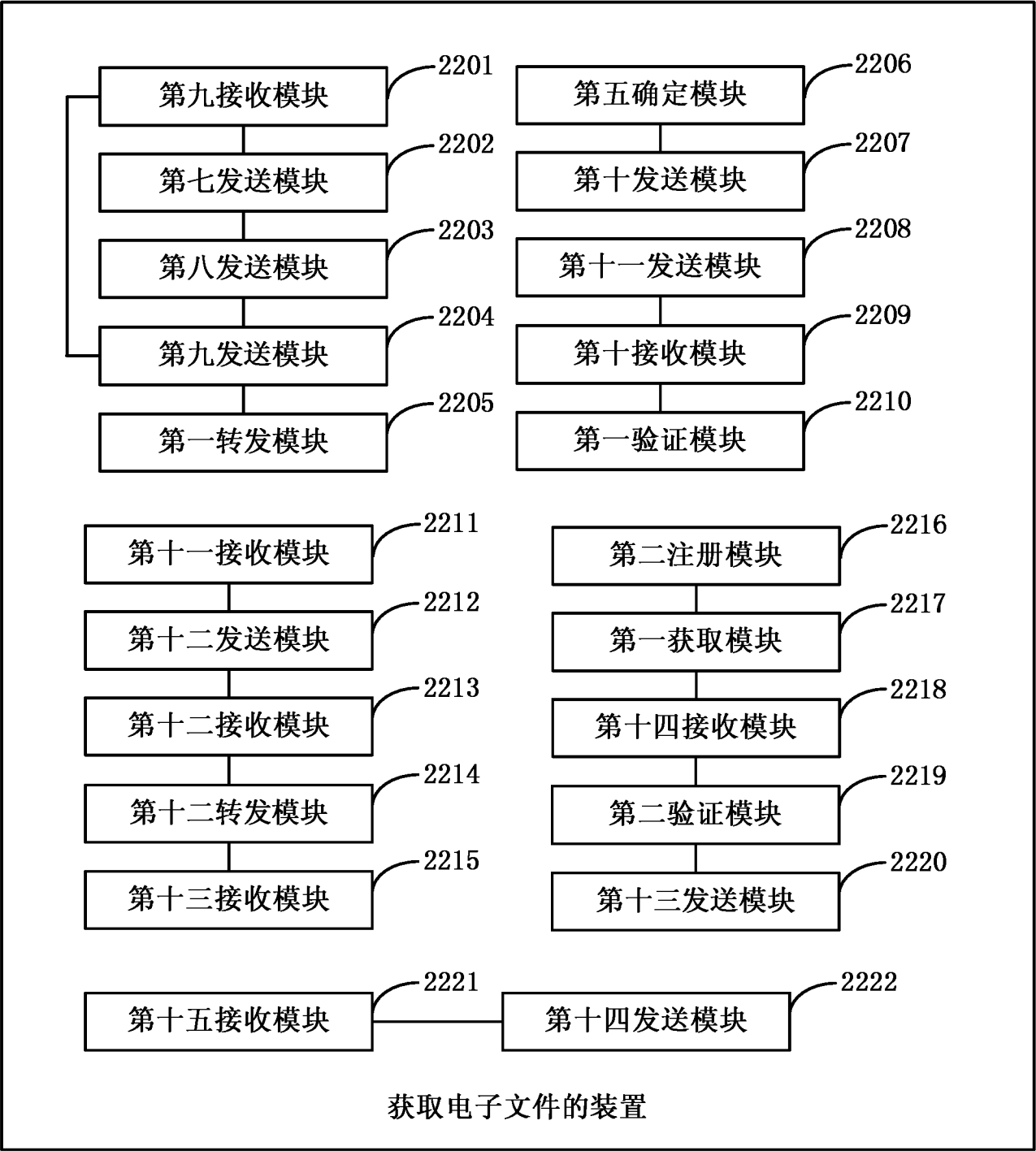


图 23

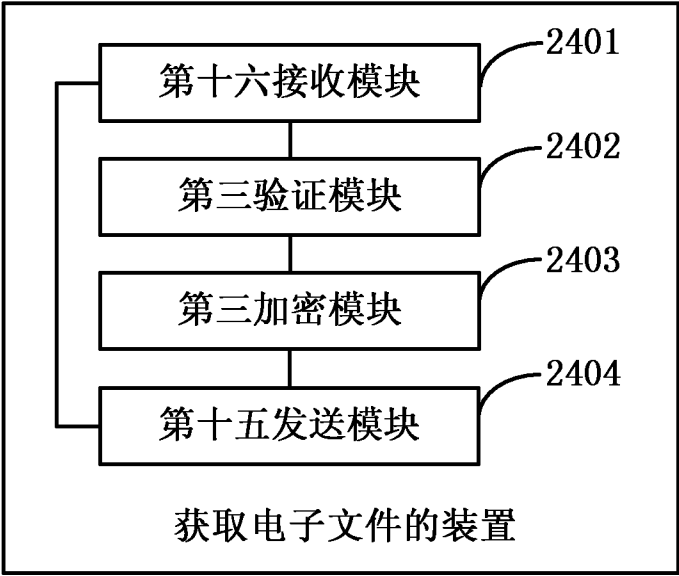


图 24

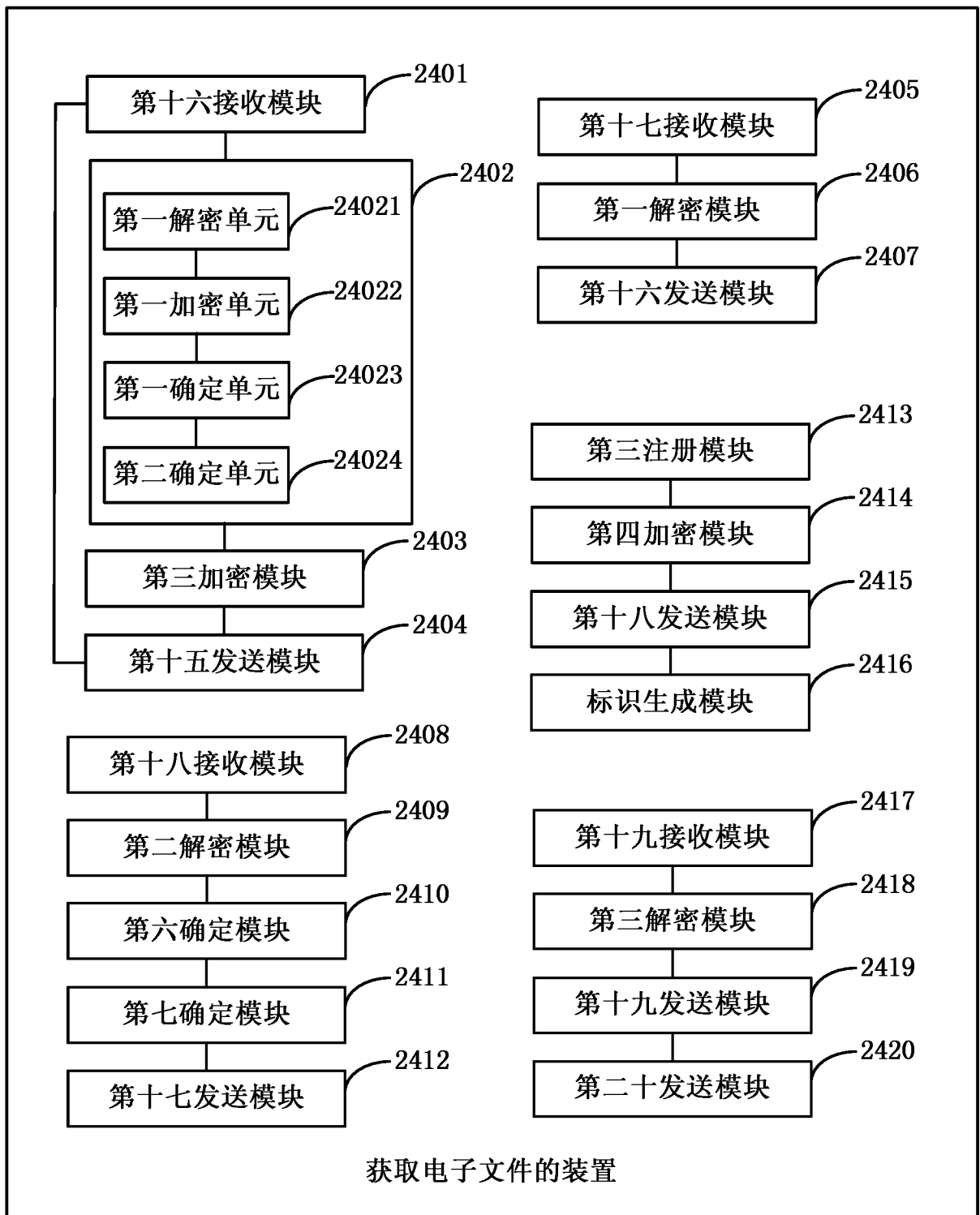


图 25

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/085216

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, EPODOC, WPI, IEEE, Google: document, server, file?, content?, service?, terminal?, encrypt+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102930225 A (INSTITUTE 706, THE SECOND ACADEMY OF CHINESE AEROSPACE SCIENCE AND INDUSTRY CORP.), 13 February 2013 (13.02.2013), description, paragraphs [0064]-[0069], and figure 2	1-42
A	CN 104104657 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 15 October 2014 (15.10.2014), the whole document	1-42
A	CN 104660557 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 27 May 2015 (27.05.2015), the whole document	1-42
A	CN 102663844 A (LI, Kai), 12 September 2012 (12.09.2012), the whole document	1-42
A	CN 103824031 A (JIANGSU AGILE TECHNOLOGY CO., LTD.), 28 May 2014 (28.05.2014), the whole document	1-42
A	US 2014344943 A1 (HAND HELD PROD., INC.), 20 November 2014 (20.11.2014), the whole document	1-42

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 06 September 2016 (06.09.2016)	Date of mailing of the international search report 20 September 2016 (20.09.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LIU, Tianfei Telephone No.: (86-10) 62414060

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/085216

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102930225 A	13 February 2013	None	
CN 104104657 A	15 October 2014	None	
CN 104660557 A	27 May 2015	HK 1206506 A1	08 January 2016
		TW 201520917 A	01 June 2015
		WO 2015074443 A1	28 May 2015
		TW I528301 B	01 April 2016
		US 2015143475 A1	21 May 2015
CN 102663844 A	12 September 2012	None	
CN 103824031 A	28 May 2014	None	
US 2014344943 A1	20 November 2014	US 2016080150 A1	17 March 2016
		US 9195844 B2	24 November 2015

国际检索报告

国际申请号

PCT/CN2016/085216

A. 主题的分类

G06F 21/62 (2013.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

G06F; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNPAT, CNKI, EPODOC, WPI, IEEE, Google: 文件, 文档, 服务器, 终端, 加密, file?, content?, service?, terminal?, encrypt+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 102930225 A (中国航天科工集团第二研究院七〇六所) 2013年 2月 13日 (2013 - 02 - 13) 说明书第[0064]-[0069]段, 附图2	1-42
A	CN 104104657 A (腾讯科技深圳有限公司) 2014年 10月 15日 (2014 - 10 - 15) 全文	1-42
A	CN 104660557 A (腾讯科技深圳有限公司) 2015年 5月 27日 (2015 - 05 - 27) 全文	1-42
A	CN 102663844 A (李凯) 2012年 9月 12日 (2012 - 09 - 12) 全文	1-42
A	CN 103824031 A (江苏敏捷科技股份有限公司) 2014年 5月 28日 (2014 - 05 - 28) 全文	1-42
A	US 2014344943 A1 (HAND HELD PROD., INC.) 2014年 11月 20日 (2014 - 11 - 20) 全文	1-42

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 9月 6日

国际检索报告邮寄日期

2016年 9月 20日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10) 62019451

授权官员

刘天飞

电话号码 (86-10) 62414060

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/085216

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	102930225	A	2013年 2月 13日	无			
CN	104104657	A	2014年 10月 15日	无			
CN	104660557	A	2015年 5月 27日	HK	1206506	A1	2016年 1月 8日
				TW	201520917	A	2015年 6月 1日
				WO	2015074443	A1	2015年 5月 28日
				TW	I528301	B	2016年 4月 1日
				US	2015143475	A1	2015年 5月 21日
CN	102663844	A	2012年 9月 12日	无			
CN	103824031	A	2014年 5月 28日	无			
US	2014344943	A1	2014年 11月 20日	US	2016080150	A1	2016年 3月 17日
				US	9195844	B2	2015年 11月 24日

表 PCT/ISA/210 (同族专利附件) (2009年7月)