(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
2015 年 12 月 3 日 (03.12.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/180689 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01)

(21) 国际申请号: PCT/CN2015/080315

(22) 国际申请日: 2015 年 5 月 29 日 (29.05.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410240511.0 2014 年 5 月 30 日 (30.05.2014) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **胡宇光 (HU, Yuguang)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: **北京市隆安律师事务所 (BEIJING LONGAN LAW FIRM)**; 中国北京市朝阳区建国门外大街 21 号北京国际俱乐部 188 室, Beijing 100020 (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。

(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,

[见续页]

(54) **Title**: METHOD AND APPARATUS FOR ACQUIRING VERIFICATION INFORMATION

(54) **发明名称** : 验证信息的获取方法及装置

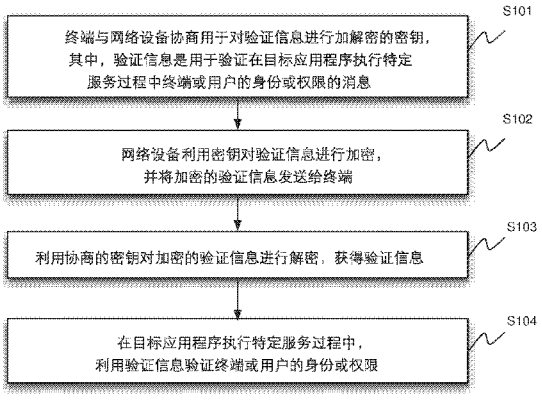

图 1 / Fig.1

S101 A terminal negotiates with a network device on a key used for decrypting the verification information, the verification information being a message used for verifying an identity or right of the terminal or a user when a target application program executes a specific service

S102 The network device encrypts the verification information by using the key, and sends the encrypted verification information to the terminal

S103 Decrypt the encrypted verification information by using the negotiated key, and acquire the verification information

S104 Verify, by using the verification information, the identity or the right of the terminal or the user when the target application program executes the specific service

(57) Abstract: Disclosed are a method and an apparatus for acquiring verification information. The method for acquiring verification information comprises: a terminal negotiates with a network device on a key used for decrypting the verification information, the verification information being a message used for verifying an identity or right of the terminal or a user when a target application program executes a specific service; the network device encrypts the verification information by using the key, and sends the encrypted verification information to the terminal; the terminal decrypts the encrypted verification information by using the negotiated key, and acquires the verification information; and verify, by using the verification information, the identity or the right of the terminal or the user when the target application program executes the specific service. The present invention can effectively ensure the security when payment and other services are operated on an application program.

(57) 摘要: 本发明公开了一种验证信息的获取方法及装置，其中的验证信息的获取方法包括：终端与网络设备协商用于对所述验证信息进行加解密的密钥，其中，所述验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息；所述网络设备利用所述密钥对验证信息进行加密，并将加密的验证信息发送给所述终端；所述终端利用协商的密钥对加密的验证信息进行解密，获得验证信息；在所述目标应用程序执行特定服务过程中，利用所述验证信息验证终端或用户的身份或权限。本发明可有效保证在应用程序上进行支付等业务操作的安全性。

WO 2015/180689 A1

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))。

验证信息的获取方法及装置

技术领域

本发明涉及网络安全技术领域，具体涉及验证信息的获取方法及装置。

背景技术

现有移动业务中，常常需要用户利用验证信息进行操作，以保证业务的安全性。用户可以通过短信或邮件等方式获取验证信息。例如，用手机注册帐号或进行支付时，需要服务端向当前手机号下发短信进行身份验证，且短信都以明文形式下发。但是目前一些操作系统（例如 Android）平台比较开放，任意软件在注册短信权限后都可随意读取短信内容，在安全方面造成极大的隐患。

在许多认证，尤其是支付过程中，手机短信验证都是最后一道安全措施。通常而言是由服务器（服务提供商，例如支付宝）通过短信网关给用户此前绑定的手机号发送一个包含数字或字符的验证码的短信。用户收到短信之后将短信中的验证码通过手机 APP 或者认证或支付的 WEB 页面并提交给服务器。服务器根据提交的验证码判断是否的确是该用户在进行验证或者支付操作。

问题在于，作为私人物品的手机，其短信并不像服务提供商以及用户所理解的那么安全。随便打开一个手机并查看每一个安装的应用，就会发现，许多看似完全无关的应用都会要求阅读短信甚至是发送短信的权限。由此可见，用户是根本不会在意安装的应用拥有一些权限。一个恶意的木马应用完全可以悄无声息的读到前面所述的验证码。Android4.4 以前的系统（目前市场上绝大部分 Android 手机），木马甚至可以在无 Root 的情况下在偷窃了验证码短信之后删除该短信，在用户毫无察觉的情况下就盗走验证码。

除了恶意的木马可能盗取验证码短信之外，还有一个严重的问题是手机可能丢失。在手机丢失的情况，获得手机的人可以很容易的利用短信找回密码的功能进行非常多的操作，包括修改用户登录密码、支付、转账等等。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的验证信息的获取方法及装置。

依据本发明的一个方面，提供一种验证信息的获取方法，包括：终端与网络设备协商用于对所述验证信息进行加解密的密钥，其中，所述验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息；所述网络设备利用所述密钥对验证信息进行加密，并将加密的验证信息发送给所述终端；所述终端利用协商的密钥对加密的验证信息进行解密，获得验证信

息；在所述目标应用程序执行特定服务过程中，利用所述验证信息验证终端或用户的身份或权限。

依据本发明的另一个方面，提供一种验证信息的获取装置，包括：密钥协商单元，用于在终端与网络设备之间协商用于对验证信息进行加解密的密钥，其中，所述验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息；加密验证信息获取单元，用于接收所述网络设备利用所述密钥对验证信息进行加密的验证信息；解密单元，用于利用协商的密钥对加密的验证信息进行解密，获得验证信息；服务执行单元，用于在所述目标应用程序执行特定服务过程中，利用所述验证信息验证终端或用户的身份或权限。

依据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在终端上运行时，导致所述终端执行前项所述验证信息的获取的方法。

依据据本发明的再一个方面，提供了一种计算机可读介质，其中存储了前项所述的计算机程序。

由上述实施例可以看出，与现有技术相比，本发明的有益效果在于：通过应用程序与网络设备之间的密钥协商，对验证信息加密处理，并且应用程序直接读取加密的验证信息，从而利用解密的验证信息进行业务等操作，也就是，只有这个应用程序才能对密文形式的验证信息进行解密，对于木马等恶意应用程序，即使能获取到验证信息，但由于验证信息是密文形式的，也无从利用，有效保证了在应用程序上进行支付等业务操作的安全性。

另外，本发明对于 GSM（Global System for Mobile Communications，全球移动通信系统）信号窃听，sim（Subscriber Identity Module，客户识别模块）卡复制等攻击手段具有很好的防御效果，因为通过本发明的加密验证信息方式，GSM 信号窃听、sim 卡复制等方案的攻击者都只能获取到密文，是没办法得到明文的，当然也就无法继续攻击。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的验证信息的获取方法流程图；

图 2 示出了根据本发明一个实施例的验证信息的获取方法实例一流程图；

图 3 示出了根据本发明一个实施例的验证信息的获取方法实例二流程图；

图 4 示出了根据本发明一个实施例的验证信息的获取方法实例三流程图；

图 5 示出了根据本发明一个实施例的验证信息的获取装置结构示意图；

图 6 示出了用于执行根据本发明的验证信息的获取方法的终端的框图；以及

图 7 示出了用于保持或者携带实现根据本发明的验证信息的获取方法的程序代码的存储单元。

具体实施例

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

参见图 1，为本发明实施例提供的验证信息的获取方法的流程图。包括以下步骤：

S101：终端与网络设备协商用于对验证信息进行加解密的密钥，其中，所述验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息；

S102：网络设备利用密钥对验证信息进行加密，并将加密的验证信息发送给终端；

S103：终端利用协商的密钥对加密的验证信息进行解密，获得验证信息；

S104：在目标应用程序执行特定服务过程中，利用验证信息验证终端或用户的身份或权限。

本发明中，终端是指具有通信功能的终端，例如，智能手机等。网络设备是指发送用于目标应用程序的业务的验证信息的服务器、网关或代理服务器。目标应用程序是指需要对验证信息进行验证从而进行服务（业务）的应用程序，包括但不限于通信软件、支付软件或电商软件，例如现在流行的支付宝软件、微信等等。在目标应用程序上执行特定服务是指利用验证信息通过终端或者用户的身份或权限的验证之后，在目标应用程序上执行支付、登录、下载等业务。上述步骤 S101 和 S103 可以由目标应用程序执行，也可以由安全应用程序执行，后续实施例会有详细介绍。

可以理解的是，验证信息就是目标应用程序服务器发起的用于在目标应用

程序上进行用户身份验证的信息。验证信息的获取方式不限，现在常用的是通过短信方式获取验证信息，但是本发明对此不作限制，对于通过邮件或者即时通信工具等方式获取验证信息的方式都是可行的。

本发明实施例一个实现条件在于，应用程序是具有访问获取验证信息的通信方式的权限的，例如，终端通过短信接收验证信息，那么，应用程序就具有访问验证短信的权限，此后，应用程序利用自身具有的访问短信的权限，直接访问短信获取加密的验证信息。由此，才能执行步骤 S103，对加密的短信进行解密，从而最终获得解密的验证信息。

本发明方案中，通过应用程序和网络设备之间的密钥协商，确定密钥，并利用协商的密钥对验证信息进行加密。本领域技术人员了解，密钥可分为对称密钥和非对称密钥。对称密钥加密，又称私钥加密或会话密钥加密算法，即信息的发送方和接收方使用同一个密钥去加密和解密数据。它的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。非对称密钥加密系统，又称公钥密钥加密。它需要使用不同的密钥来分别完成加密和解密操作，一个公开发布，即公开密钥或称为公钥，另一个由用户自己秘密保存，即私用密钥或称为私钥。信息发送者用公开密钥去加密，而信息接收者则用私用密钥去解密。公钥机制灵活，但加密和解密速度却比对称密钥加密慢得多。本发明中，密钥可以是对称密钥，也可以是非对称密钥。当采用对称密钥方式时，网络设备与应用程序使用同一个密钥对验证信息进行加密和解密；当采用非对称密钥时，网络设备使用公钥对验证信息进行加密，应用程序使用私钥对加密的验证信息进行解密。

可见，本发明通过应用程序与网络设备之间的密钥协商，对验证信息加密处理，并且应用程序直接读取加密的验证信息，从而利用解密的验证信息进行业务等操作，也就是，只有这个应用程序才能对密文形式的验证信息进行解密，对于木马等恶意应用程序，即使能获取到验证信息，但由于验证信息是密文形式的，也无从利用，有效保证了在应用程序上进行支付等业务操作的安全性。

另外，本发明对于 GSM 信号窃听，sim 卡复制等攻击手段具有很好的防御效果，因为通过本发明的加密验证信息方式，GSM 信号窃听、sim 卡复制等方案的攻击者都只能获取到密文，是没办法得到明文的，当然也就无法继续攻击。

下面以几个实例对本发明实施例进行详细介绍。

实例一

参见图 2，为实例一提供的验证信息的获取方法的流程图，包括：

S201：终端的目标应用程序与网络设备协商用于验证信息的密钥；

S202：网络设备利用密钥对验证信息进行加密，并将加密的验证信息发送给终端；

S203：目标应用程序利用协商的密钥对加密的验证信息进行解密，获得验证信息。

其中，目标应用程序是指需要验证所述验证信息从而进行业务的应用程序；那么可以理解，网络设备是指发送用于目标应用程序的业务的验证信息的服务器、网关或代理服务器。

下面以通过手机短信方式获取验证信息的例子进行说明。

首先，安装在用户手机的 APP（目标 APP）和网络设备基于某种方式协商一个密钥。网络设备是指位于网络侧的与验证信息对应的功能实体，可有多种形式。具体地，APP 可以与 APP 服务器直接协商密钥、发送密文短信，也可以与短信网关协商密钥以及发送密文短信，还可以通过短信网关的代理服务器，由代理服务器负责协商密钥及发送密文短信。本领域技术人员了解，短信业务是由运营商控制的，那么，如果 APP 服务器要给终端发送 APP 业务的验证短信，一般都是借助运营商的短信业务线路进行发送，因此，一般情况下，需要借助短信网关或者短信网关代理服务器进行密钥协商，当然也可以如上所述的通过与 APP 服务器进行密钥协商。

然后，网络设备给用户手机发送短信时用协商的密钥进行加密。

最后，用户在手机上收到加密的验证短信，该 APP 在后台自动获取该短信并解密获得真正的验证码。

例如，本实例中的 APP 是指支付宝软件，那么，手机上的支付宝软件首先需要与网络设备（支付宝服务器、短信网关或者短信网关代理服务器）协商验证码密钥；在用户进行支付等业务时，需要验证码，此时，网络设备利用预先约定的密钥对验证码进行加密并发送到该用户手机上；最后，用户在手机上通过短信接收到的是一条密文形式的验证短信，而手机上的支付宝软件从后台直接读取该密文短信，并利用预先约定的密钥进行读取，获取到解密的验证码，最终进行验证并完成业务。

可见，因为手机收到的是加密短信，除了目标 APP 是无法读取验证信息的，有效地解决了验证短信被木马等恶意软件窃取的问题。

实例二

参见图 3，为实例二提供的验证信息的获取方法的流程图，包括：

S301：安全应用程序与网络设备协商用于验证信息的密钥，其中，验证信息是在目标应用程序的业务中需要被验证的信息；

S302：网络设备利用密钥对验证信息进行加密，并将加密的验证信息发送给终端；

S303：安全应用程序利用协商的密钥对加密的验证信息进行解密，获得验

证信息;

S304：安全应用程序将验证信息提供给所述目标应用程序，和／或，安全应用程序将验证信息展示给用户。

其中，目标应用程序是指需要验证所述验证信息从而进行业务的应用程序;那么可以理解，网络设备是指发送用于目标应用程序的业务的验证信息的服务器、网关或代理服务器。

该实例二与上述实例一区别在于，通过引入一个安全应用程序，为各个目标应用程序统一管理验证信息。具体的，由这个安全应用程序与网络设备进行密钥协商，并且仅由这个安全应用程序可以读取并解密验证信息，并且由这个安全应用程序将解密的验证信息提供给目标应用程序。

下面以通过手机短信方式获取验证信息的例子进行说明。

与实例一区别在于，用户手机上需要安装一个安全 APP。

首先，安全 APP 和网络设备进行密钥协商。网络设备是指位于网络侧的与验证信息对应的功能实体，可有多种形式。具体地，安全 APP 可以与目标 APP 服务器直接协商密钥、发送密文短信，也可以与短信网关协商密钥以及发送密文短信，还可以通过短信网关的代理服务器，由代理服务器负责协商密钥及发送密文短信。本领域技术人员了解，短信业务是由运营商控制的，那么，如果目标 APP 服务器要给终端发送目标 APP 业务的验证短信，一般都是借助运营商的短信业务线路进行发送，因此，一般情况下，需要借助短信网关或者短信网关代理服务器进行密钥协商，当然也可以如上所述的通过与目标 APP 服务器进行密钥协商。

然后，网络设备给用户手机发送短信时用协商的密钥进行加密。

接着，用户在手机上收到加密的验证短信，仅有这个安全 APP 可以解密并且显示给用户。

最后，目标 APP 通过安全 APP 提供的接口获得解密的验证短信。

可见，其他 APP 如果需要读取对应的短信，则不再通过手机操作系统的短信接口获取短信，而是通过该安全 APP 提供的接口获取。安全 APP 负责验证试图调用该接口的 APP 的合法性（验证该 APP 的签名，以及判断该短信的确是属于该 APP。比如仅有微信 APP 可以读微信服务器发来的验证码短信），只有目标 APP 合法时，才将验证信息提供给目标 APP。

其中，安全 APP 验证目标 APP 的合法性包括：通过目标 APP 的签名判断目标 APP 是否合法，和／或，判断目标 APP 是否具有读取验证信息的权限。具体的，判断目标 APP 是否合法包括：根据目标 APP 的签名判断目标 APP 是否属于安全 APP（白 APP），或者，根据所述目标 APP 的签名判断目标 APP 是否属于恶意 APP（黑 APP），如果目标 APP 属于安全 APP 或者不属于恶意 APP，

则确定目标 APP 合法。可以理解，白 APP 和黑 APP 名单是预先获取并存储在手机上的，获取方式可以是手动设置或者网络抓取等等。具体的，判断目标 APP 是否具有读取验证信息的权限包括：判断目标 APP 是否是与提供验证信息的网络设备对应的应用程序，如果是，则确定目标 APP 具有读取验证信息的权限。具体地，通过判断验证信息携带的标识是否与提供验证信息的网络设备对应。比如，通过发送短信的号码进行判断。

例如，本实例中的目标 APP 是指微信软件，那么，手机上的安全 APP（例如，360 安全通讯录）首先需要与网络设备（微信服务器、短信网关或者短信网关代理服务器）协商验证码密钥；在用户进行支付等业务时，需要验证码，此时，网络设备利用预先约定的密钥对验证码进行加密并发送到该用户手机上；接着，用户在手机上通过短信接收到的是一条密文形式的验证短信，而手机上的安全 APP 从后台直接读取该密文短信，并利用预先约定的密钥进行读取，获取到解密的验证码，并将明文的验证码展示给用户；最后，如果需要，微信从安全 APP 提供的接口获取到该明文的验证码。

可见，因为手机收到的是加密短信，除了安全 APP 是无法读取验证信息的，而且安全 APP 是在验证目标 APP 合法性基础上才向 APP 提供验证短信，有效地解决了验证短信被木马等恶意软件窃取的问题。而且，与实例一相比，本实例二还可以向用户展示明文的验证信息，这就可以满足通过 PC 浏览器发送验证码的情况，也就是，适用于在 PC 机上通过目标 APP 进行操作的情况。

实例三

参见图 4，为实例三提供的验证信息的获取方法的流程图，包括：

S401：安全应用程序与网络设备协商用于验证信息的密钥，其中，验证信息是在目标应用程序的业务中需要被验证的信息；

S402：网络设备利用密钥对验证信息进行加密，并将加密的验证信息发送给终端；

S403：安全应用程序利用协商的密钥对加密的验证信息进行解密，获得验证信息；

S404：获取用户输入的密码，根据与用户预先约定密码确定用户输入的密码是否正确；

S405：在用户输入密码正确情况下，安全应用程序将验证信息提供给目标应用程序，和／或，安全应用程序将验证信息展示给用户。

其中，目标应用程序是指需要验证所述验证信息从而进行业务的应用程序；那么可以理解，网络设备是指发送用于目标应用程序的业务的验证信息的服务器、网关或代理服务器。

该实例三与上述实例二类似，通过引入一个安全应用程序，为各个目标应

用程序统一管理验证信息。具体的，由这个安全应用程序与网络设备进行密钥协商，并且仅由这个安全应用程序可以读取并解密验证信息，并且由这个安全应用程序将解密的验证信息提供给目标应用程序。与实例二区别在于，在向用户展示验证信息之前或者在向目标应用程序提供验证信息之前，需要用户输入与安全应用程序事先约定的密码。

下面以通过手机短信方式获取验证信息的例子进行说明。

用户手机上需要安装一个安全 APP。

首先，安全 APP 和网络设备进行密钥协商。网络设备是指位于网络侧的与验证信息对应的功能实体，可有多种形式。具体地，安全 APP 可以与目标 APP 服务器直接协商密钥、发送密文短信，也可以与短信网关协商密钥以及发送密文短信，还可以通过短信网关的代理服务器，由代理服务器负责协商密钥及发送密文短信。本领域技术人员了解，短信业务是由运营商控制的，那么，如果目标 APP 服务器要给终端发送目标 APP 业务的验证短信，一般都是借助运营商的短信业务线路进行发送，因此，一般情况下，需要借助短信网关或者短信网关代理服务器进行密钥协商，当然也可以如上所述的通过与目标 APP 服务器进行密钥协商。

然后，网络设备给用户手机发送短信时用协商的密钥进行加密。

接着，用户在手机上收到加密的验证短信，安全 APP 进行解密。

继而，用户在需要查看解密的验证短信时，或者目标 APP 需要读取该验证短信时，需要用户输入与安全 APP 预先约定的密码。

最后，目标 APP 向用户展示解密的验证短信，或者，目标 APP 通过安全 APP 提供的接口获得解密的验证短信。

可见，其他 APP 如果需要读取对应的短信，则不再通过手机操作系统的短信接口获取短信，而是通过该安全 APP 提供的接口获取。安全 APP 负责验证试图调用该接口的 APP 的合法性（验证该 APP 的签名，以及判断该短信的确是属于该 APP。比如仅有微信 APP 可以读微信服务器发来的验证码短信），只有目标 APP 合法时，才将验证信息提供给目标 APP。

其中，安全 APP 验证目标 APP 的合法性包括：通过目标 APP 的签名判断目标 APP 是否合法，和／或，判断目标 APP 是否具有读取验证信息的权限。具体的，判断目标 APP 是否合法包括：根据目标 APP 的签名判断目标 APP 是否属于安全 APP（白 APP），或者，根据所述目标 APP 的签名判断目标 APP 是否属于恶意 APP（黑 APP），如果目标 APP 属于安全 APP 或者不属于恶意 APP，则确定目标 APP 合法。可以理解，白 APP 和黑 APP 名单是预先获取并存储在手机上的，获取方式可以是手动设置或者网络抓取等等。具体的，判断目标 APP 是否具有读取验证信息的权限包括：判断目标 APP 是否是与提供验证信息的网

络设备对应的应用程序，如果是，则确定目标 APP 具有读取验证信息的权限。具体地，通过判断验证信息携带的标识是否与提供验证信息的网络设备对应。比如，通过发送短信的号码进行判断。

例如，本实例中的目标 APP 是指亚马逊链接到的银行支付平台，那么，手机上的安全 APP（例如 360 安全通讯录）首先需要与网络设备（银行支付平台服务器、短信网关或者短信网关代理服务器）协商验证码密钥；在用户进行支付等业务时，需要验证码，此时，网络设备利用预先约定的密钥对验证码进行加密并发送到该用户手机上；接着，用户在手机上通过短信接收到的是一条密文形式的验证短信，而手机上的安全 APP 从后台直接读取该密文短信，并利用预先约定的密钥进行读取，获取到解密的验证码；在用户输入正确的密码后，将明文的验证码展示给用户；最后，如果需要，银行支付平台从安全 APP 提供的接口获取到该明文的验证码。

可见，因为手机收到的是加密短信，除了安全 APP 是无法读取验证信息的，而且安全 APP 是在验证目标 APP 合法性基础上才向 APP 提供验证短信，有效地解决了验证短信被木马等恶意软件窃取的问题。而且，同实例二类似，实例三还可以向用户展示明文的验证信息，这就可以满足通过 PC 浏览器发送验证码的情况，也就是，适用于在 PC 机上通过目标 APP 进行操作的情况。另外，与实例二相比，本实例三在用户输入正确密码之后才向用户展示验证信息或者提供给目标 APP，也就是又进一步保证了验证信息的安全性，通过密文验证信息以及用户密码的双重保险，即使在手机丢失的情况下，也能保证验证信息的安全性。

与上述方法相对应，本发明还提供一种验证信息的获取装置。该装置可以通过硬件、软件或软硬件结合方式实现。该装置可以是指终端内部的功能模块，也可以是指终端本身，只要终端包括实现该装置的功能即可。参见图 5，该装置包括：

密钥协商单元 501，用于在终端与网络设备之间协商用于对验证信息进行加解密的密钥，其中，所述验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息；

加密验证信息获取单元 502，用于接收所述网络设备利用所述密钥对验证信息进行加密的验证信息；

解密单元 503，用于利用协商的密钥对加密的验证信息进行解密，获得验证信息；

服务执行单元 504，用于在所述目标应用程序执行特定服务过程中，利用所述验证信息验证终端或用户的身份或权限。

优选的，一种方案中，由所述目标应用程序执行密钥协商单元 501 以及解密单元 503 的功能，即，由所述目标应用程序执行所述与网络设备协商用于验

证信息的密钥以及所述利用协商的密钥对加密的验证信息进行解密。

优选地，另一种方案中，由一个安全应用程序执行密钥协商单元 501 以及解密单元 503 的功能，即，由安全应用程序执行所述与网络设备协商用于验证信息的密钥以及所述利用协商的密钥对加密的验证信息进行解密；所述密钥协商单元 501 具体用于：利用所述安全应用程序与网络设备协商用于验证信息的密钥，其中，所述验证信息是在目标应用程序的业务中需要被验证的信息；所述装置还包括：验证信息提供单元 505，用于利用所述安全应用程序将所述验证信息提供给所述目标应用程序。

其中，所述目标应用程序调用所述安全应用程序提供的接口，从所述安全应用程序获取所述验证信息。

可选的，装置还包括：目标合法性验证单元 506，用于利用所述安全应用程序验证所述目标应用程序的合法性；此情况下，所述验证信息提供单元 505 只有所述目标应用程序合法时，才将所述验证信息提供给所述目标应用程序。

其中，所述目标合法性验证单元 506 具体用于：通过所述目标应用程序的签名判断所述目标应用程序是否合法，和／或，判断所述目标应用程序是否具有读取所述验证信息的权限。

具体地，所述目标合法性验证单元 506 具体用于：根据所述目标应用程序的签名判断所述目标应用程序是否属于安全应用程序，或者，根据所述目标应用程序的签名判断所述目标应用程序是否属于恶意应用程序，如果所述目标应用程序属于安全应用程序或者不属于恶意安全程序，则确定所述目标应用程序合法。

具体地，所述目标合法性验证单元 506 具体用于：判断所述目标应用程序是否是与提供所述验证信息的网络设备对应的应用程序，如果是，则确定所述目标应用程序具有读取所述验证信息的权限。

具体地，所述目标合法性验证单元 506 具体用于：判断所述验证信息携带的标识是否与提供所述验证信息的网络设备对应。

优选地，另一种方案中，装置还包括：密码验证单元 507，用于获取用户输入的密码，根据与用户预先约定密码确定用户输入的密码是否正确；所述验证信息提供单元 505 在用户输入的密码正确时，才将所述验证信息提供给所述目标应用程序。

其中，所述与用户预先约定密码是指安全应用程序与用户之间约定的密码。

优选地，另一种方案中，所述应用程序是指安全应用程序；所述密钥协商单元 501 具体用于：利用所述安全应用程序与网络设备协商用于验证信息的密钥；所述装置还包括：验证信息展示单元 508，用于利用所述安全应用程序将解密后的验证信息展示给用户。

可选的，所述装置还包括：密码验证单元 507，用于获取用户输入的密码，根据与用户预先约定密码确定用户输入的密码是否正确；所述验证信息展示单元 508，在用户输入的密码正确时，才将所述验证信息展示给所述用户。

其中，所述与用户预先约定密码是指安全应用程序与用户之间约定的密码。

其中，所述目标应用程序包括即时通信软件、支付软件或电商软件。

其中，所述网络设备是指发送验证信息的服务器、网关或代理服务器。

其中，所述网络设备通过预先获得的有关所述终端验证信息的协商参数，获知所述终端支持密文验证信息。

其中，所述密钥是指对称密钥，所述网络设备与所述应用程序使用同一个密钥对验证信息进行加密和解密；或者，所述密钥是指非对称密钥，所述网络设备使用公钥对验证信息进行加密，所述应用程序使用私钥对加密的验证信息进行解密。

其中，所述终端通过短信、邮件或者即时通信工具的通信方式从所述网络设备获取所述加密的验证信息。

优选地，所述装置还包括：权限访问单元 509，用于支持所述应用程序利用自身具有的访问所述通信方式的权限，直接访问所述通信方式获取所述加密的验证信息。

需要说明的是：

在此提供的算法和显示不与任何特定计算机、虚拟装置或者其它设备固有相关。各种通用装置也可以与基于在此的示教一起使用。根据上面的描述，构造这类装置所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的实现验证信息获取的装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 6 示出了可以实现根据本发明的验证信息的获取方法的终端，例如智能终端。该终端传统上包括处理器 610 和以存储器 620 形式的计算机程序产品或者计算机可读介质。存储器 620 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 620 具有用于执行上述方法中的任何方法步骤的程序代码631的存储空间630。例如，用于程序代码的存储空间 630 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 631。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 7 所述的便携式或者固定存储单元。该存储单元可以具有与图 6 的终端中的存储器 620 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 631'，即可以由例如诸如 610 之类的处理器读取的代码，这些代码当由终端运行时，导致该终端执行上面所描述的方法中的各个步骤。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

权利要求书

1、一种验证信息的获取方法，其特征在于，包括:

终端与网络设备协商用于对所述验证信息进行加解密的密钥，其中，所述验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息;

所述网络设备利用所述密钥对验证信息进行加密，并将加密的验证信息发送给所述终端;

所述终端利用协商的密钥对加密的验证信息进行解密，获得验证信息;

在所述目标应用程序执行特定服务过程中，利用所述验证信息验证终端或用户的身份或权限。

2、如权利要求 1 所述的方法，其特征在于，由所述终端上的所述目标应用程序执行所述与网络设备协商用于验证信息的密钥以及所述利用协商的密钥对加密的验证信息进行解密的步骤。

3、如权利要求 1 所述的方法，其特征在于，由所述终端上的安全应用程序执行与网络设备协商用于验证信息的密钥以及所述利用协商的密钥对加密的验证信息进行解密的步骤;

所述终端与网络设备协商用于验证信息的密钥包括:

所述安全应用程序与网络设备协商用于验证信息的密钥;

在所述终端利用协商的密钥对加密的验证信息进行解密，获得验证信息之后，还包括:

所述安全应用程序将所述验证信息提供给所述目标应用程序。

4、如权利要求 3 所述的方法，其特征在于，所述目标应用程序调用所述安全应用程序提供的接口，从所述安全应用程序获取所述验证信息。

5、如权利要求 3 所述的方法，其特征在于，所述方法还包括:

所述安全应用程序验证所述目标应用程序的合法性，只有所述目标应用程序合法时，才将所述验证信息提供给所述目标应用程序。

6、如权利要求 5 所述的方法，其特征在于，所述安全应用程序验证所述目标应用程序的合法性包括:

通过所述目标应用程序的签名判断所述目标应用程序是否合法，和 / 或，判断所述目标应用程序是否具有读取所述验证信息的权限。

7、如权利要求 6 所述的方法，其特征在于，所述判断所述目标应用程序是否合法包括:

根据所述目标应用程序的签名判断所述目标应用程序是否属于安全应用程

序，或者，根据所述目标应用程序的签名判断所述目标应用程序是否属于恶意应用程序，如果所述目标应用程序属于安全应用程序或者不属于恶意安全程序，则确定所述目标应用程序合法。

8、如权利要求 6 所述的方法，其特征在于，所述判断所述目标应用程序是否具有读取所述验证信息的权限包括:

判断所述目标应用程序是否是与提供所述验证信息的网络设备对应的应用程序，如果是，则确定所述目标应用程序具有读取所述验证信息的权限。

9、如权利要求 8 所述的方法，其特征在于，所述判断所述目标应用程序是否是与提供所述验证信息的网络设备对应的应用程序包括:

判断所述验证信息携带的标识是否与提供所述验证信息的网络设备对应。

10、如权利要求 3 所述的方法，其特征在于，在所述安全应用程序将所述验证信息提供给所述目标应用程序之前，还包括:

获取用户输入的密码，根据与用户预先约定密码确定用户输入的密码是否正确;

在用户输入的密码正确时，所述安全应用程序才将所述验证信息提供给所述目标应用程序。

11、如权利要求 10 所述的方法，其特征在于，所述与用户预先约定密码是指安全应用程序与用户之间约定的密码。

12、如权利要求 1 所述的方法，其特征在于，由所述终端上的安全应用程序执行与网络设备协商用于验证信息的密钥以及所述利用协商的密钥对加密的验证信息进行解密的步骤;

所述终端与网络设备协商用于验证信息的密钥包括:

所述安全应用程序与网络设备协商用于验证信息的密钥;

在所述终端利用协商的密钥对加密的验证信息进行解密，获得验证信息之后，还包括:

所述安全应用程序将解密后的验证信息展示给用户。

13、如权利要求 12 所述的方法，其特征在于，在所述安全应用程序将解密后的验证信息展示给用户之前，还包括:

获取用户输入的密码，根据与用户预先约定密码确定用户输入的密码是否正确;

在用户输入的密码正确时，所述安全应用程序才将所述验证信息展示给所述用户。

14、如权利要求 13 所述的方法，其特征在于，所述与用户预先约定密码是指安全应用程序与用户之间约定的密码。

15、如权利要求 1 所述的方法，其特征在于，在所述网络设备利用所述密钥对验证信息进行加密之前，还包括:

所述网络设备通过预先获得的有关所述终端验证信息的协商参数，获知所述终端支持密文验证信息。

16、如权利要求 1 所述的方法，其特征在于，

所述密钥是指对称密钥，所述网络设备与所述终端使用同一个密钥对验证信息进行加密和解密；或者，

所述密钥是指非对称密钥，所述网络设备使用公钥对验证信息进行加密，所述终端使用私钥对加密的验证信息进行解密。

17、如权利要求 1 所述的方法，其特征在于，所述终端通过短信、邮件或者即时通信工具的通信方式从所述网络设备获取所述加密的验证信息。

18、如权利要求 17 所述的方法，其特征在于，在所述终端从所述网络设备获取加密的验证信息之后，还包括:

所述目标应用程序或者安全应用程序利用自身具有的访问所述通信方式的权限，直接访问所述通信方式获取所述加密的验证信息。

19、如权利要求 1-18 所述的方法，其特征在于，所述目标应用程序包括即时通信软件、支付软件或电商软件。

20、如权利要求 1-18 任一项所述的方法，其特征在于，所述网络设备是指发送所述验证信息的服务器、网关或代理服务器。

21、一种验证信息的获取装置，其特征在于，包括:

密钥协商单元，用于在终端与网络设备之间协商用于对验证信息进行加解密的密钥，其中，所述验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息;

加密验证信息获取单元，用于接收所述网络设备利用所述密钥对验证信息进行加密的验证信息;

解密单元，用于利用协商的密钥对加密的验证信息进行解密，获得验证信息;

服务执行单元，用于在所述目标应用程序执行特定服务过程中，利用所述验证信息验证终端或用户的身份或权限。

22、如权利要求 21 所述的装置，其特征在于，由所述目标应用程序执行所述与网络设备协商用于验证信息的密钥以及所述利用协商的密钥对加密的验证信息进行解密。

23、如权利要求 21 所述的装置，其特征在于，由所述终端上的安全应用程序执行与网络设备协商用于验证信息的密钥以及所述利用协商的密钥对加密的

验证信息进行解密;

所述密钥协商单元具体用于：利用所述安全应用程序与网络设备协商用于验证信息的密钥;

所述装置还包括:

验证信息提供单元，用于利用所述安全应用程序将所述验证信息提供给所述目标应用程序。

24、如权利要求 23 所述的装置，其特征在于，所述目标应用程序调用所述安全应用程序提供的接口，从所述安全应用程序获取所述验证信息。

25、如权利要求 23 所述的装置，其特征在于，所述装置还包括:

目标合法性验证单元，用于利用所述安全应用程序验证所述目标应用程序的合法性;

所述验证信息提供单元只有所述目标应用程序合法时，才将所述验证信息提供给所述目标应用程序。

26、如权利要求 25 所述的装置，其特征在于，所述目标合法性验证单元具体用于：通过所述目标应用程序的签名判断所述目标应用程序是否合法，和/或，判断所述目标应用程序是否具有读取所述验证信息的权限。

27、如权利要求 26 所述的装置，其特征在于，所述目标合法性验证单元具体用于：根据所述目标应用程序的签名判断所述目标应用程序是否属于安全应用程序，或者，根据所述目标应用程序的签名判断所述目标应用程序是否属于恶意应用程序，如果所述目标应用程序属于安全应用程序或者不属于恶意安全程序，则确定所述目标应用程序合法。

28、如权利要求 26 所述的装置，其特征在于，所述目标合法性验证单元具体用于：判断所述目标应用程序是否是与提供所述验证信息的网络设备对应的应用程序，如果是，则确定所述目标应用程序具有读取所述验证信息的权限。

29、如权利要求 28 所述的装置，其特征在于，所述目标合法性验证单元具体用于：判断所述验证信息携带的标识是否与提供所述验证信息的网络设备对应。

30、如权利要求 23 所述的装置，其特征在于，还包括:

密码验证单元，用于获取用户输入的密码，根据与用户预先约定密码确定用户输入的密码是否正确;

所述验证信息提供单元在用户输入的密码正确时，才将所述验证信息提供给所述目标应用程序。

31、如权利要求 30 所述的装置，其特征在于，所述与用户预先约定密码是指安全应用程序与用户之间约定的密码。

32、如权利要求 21 所述的装置，其特征在于，由所述终端上的安全应用程序执行与网络设备协商用于验证信息的密钥以及所述利用协商的密钥对加密的验证信息进行解密；

所述密钥协商单元具体用于：利用所述安全应用程序与网络设备协商用于验证信息的密钥；

所述装置还包括：验证信息展示单元，用于利用所述安全应用程序将解密后的验证信息展示给用户。

33、如权利要求 32 所述的装置，其特征在于，所述装置还包括：

密码验证单元，用于获取用户输入的密码，根据与用户预先约定密码确定用户输入的密码是否正确；

所述验证信息展示单元，在用户输入的密码正确时，才将所述验证信息展示给所述用户。

34、如权利要求 33 所述的装置，其特征在于，所述与用户预先约定密码是指安全应用程序与用户之间约定的密码。

35、如权利要求 21 所述的装置，其特征在于，所述网络设备通过预先获得的有关所述终端验证信息的协商参数，获知所述终端支持密文验证信息。

36、如权利要求 21 所述的装置，其特征在于，

所述密钥是指对称密钥，所述网络设备与所述应用程序使用同一个密钥对验证信息进行加密和解密；或者，

所述密钥是指非对称密钥，所述网络设备使用公钥对验证信息进行加密，所述应用程序使用私钥对加密的验证信息进行解密。

37、如权利要求 21 所述的装置，其特征在于，所述终端通过短信、邮件或者即时通信工具的通信方式从所述网络设备获取所述加密的验证信息。

38、如权利要求 37 所述的装置，其特征在于，所述装置还包括：权限访问单元，用于支持所述应用程序利用自身具有的访问所述通信方式的权限，直接访问所述通信方式获取所述加密的验证信息。

39、如权利要求 21-38 所述的装置，其特征在于，所述目标应用程序包括即时通信软件、支付软件或电商软件。

40、如权利要求 21-38 任一项所述的装置，其特征在于，所述网络设备是指发送所述验证信息的服务器、网关或代理服务器。

41、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在终端上运行时，导致所述终端执行根据权利要求 1 至 20 中的任一所述的方法。

42、一种计算机可读介质，其中存储了如权利要求 41 所述的计算机程序。

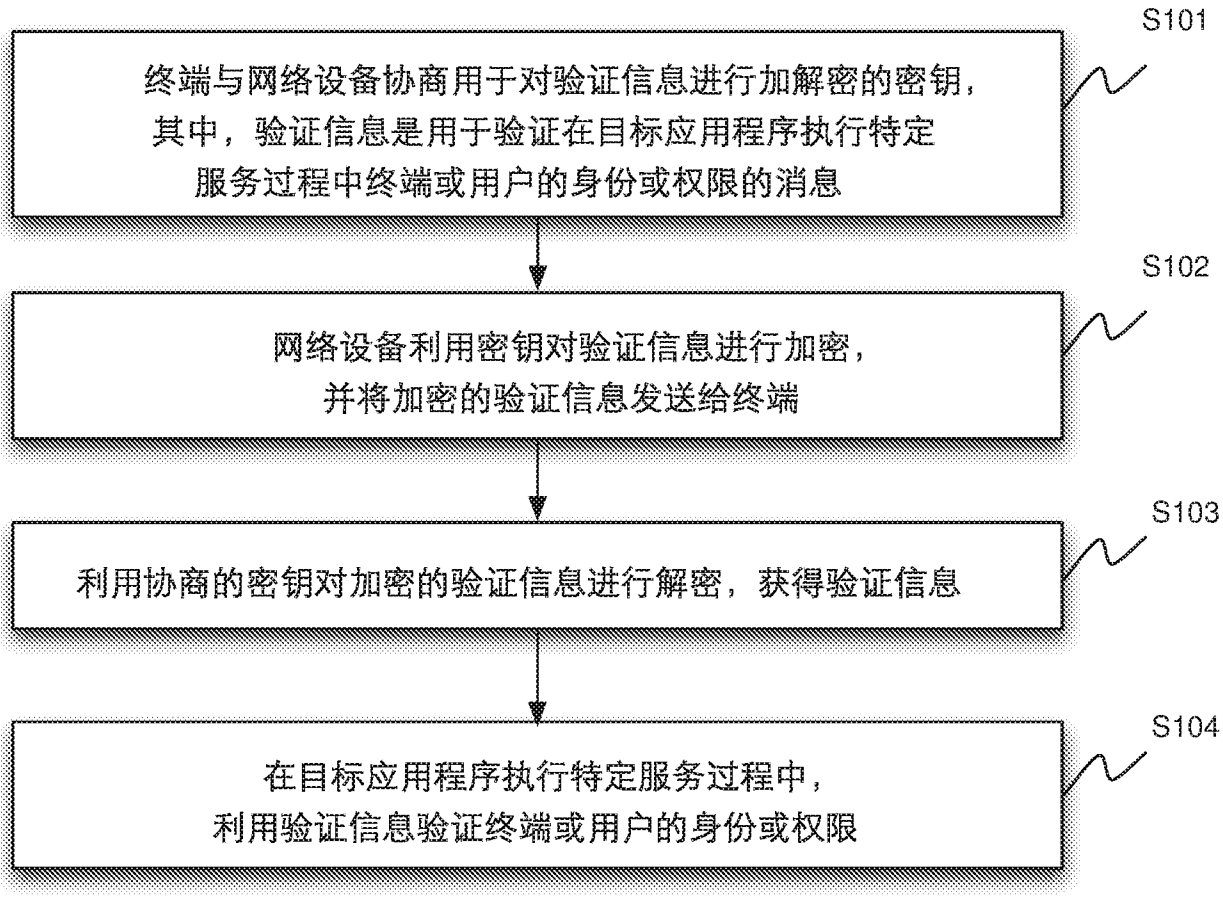
S101
终端与网络设备协商用于对验证信息进行加解密的密钥，其中，验证信息是用于验证在目标应用程序执行特定服务过程中终端或用户的身份或权限的消息
S102
网络设备利用密钥对验证信息进行加密，并将加密的验证信息发送给终端
S103
利用协商的密钥对加密的验证信息进行解密，获得验证信息
S104
在目标应用程序执行特定服务过程中，利用验证信息验证终端或用户的身份或权限

图 1

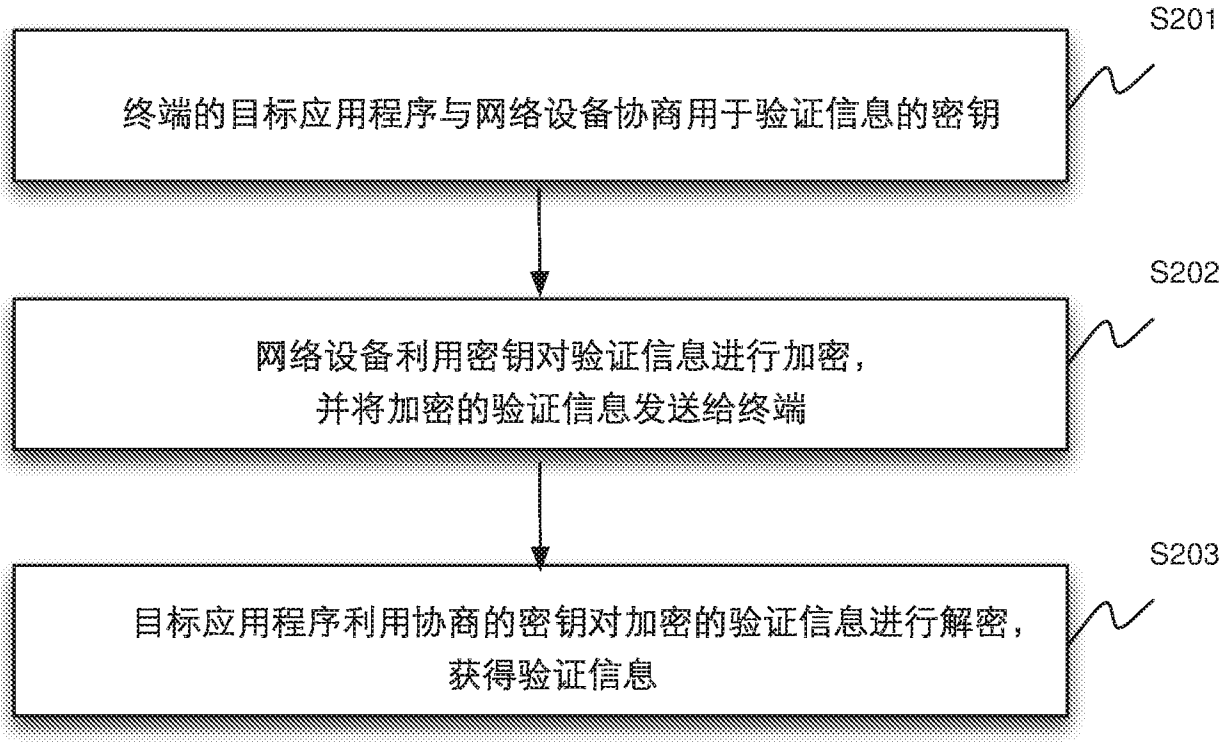
S201
终端的目标应用程序与网络设备协商用于验证信息的密钥
S202
网络设备利用密钥对验证信息进行加密，并将加密的验证信息发送给终端
S203
目标应用程序利用协商的密钥对加密的验证信息进行解密，获得验证信息

图 2

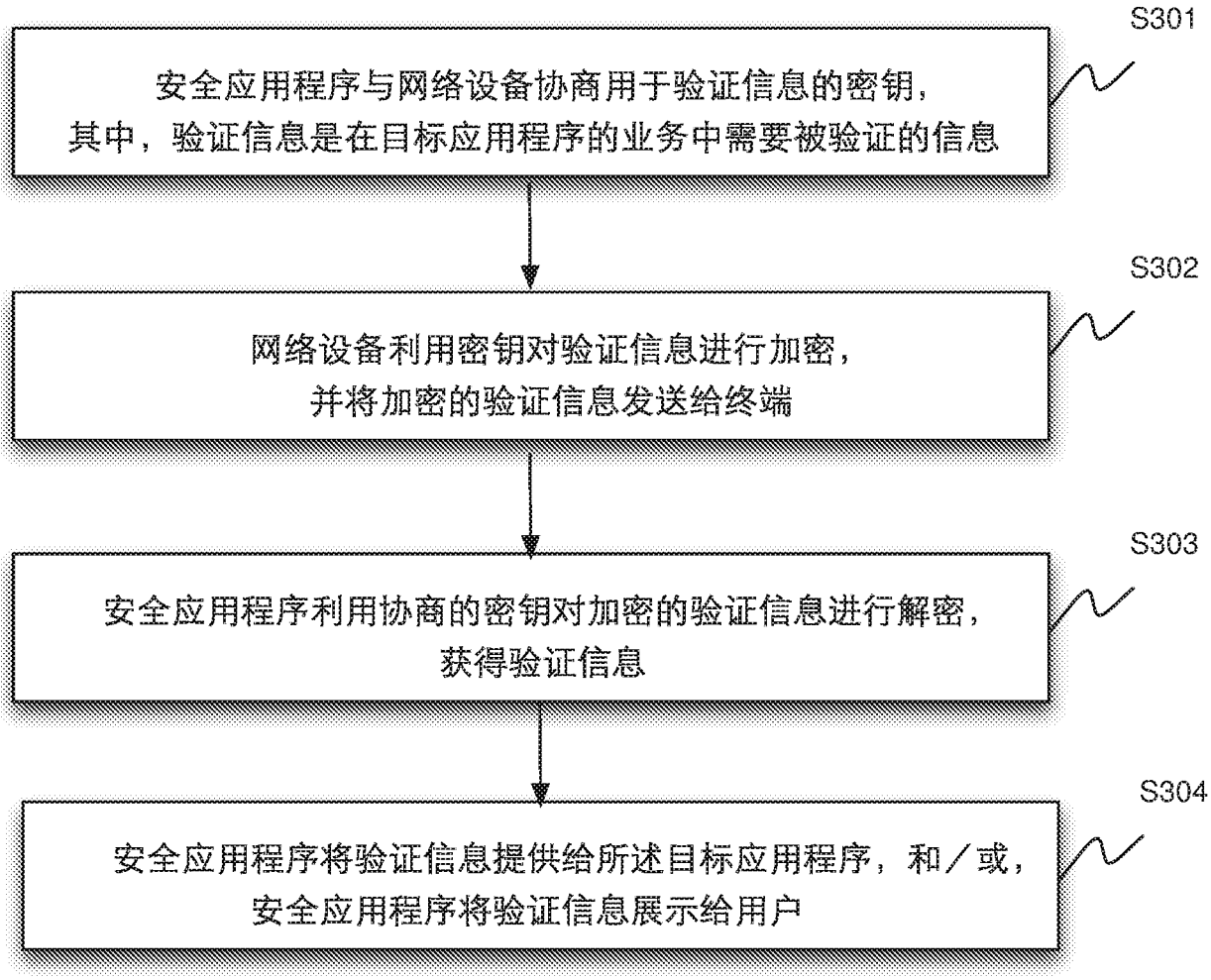
S301
安全应用程序与网络设备协商用于验证信息的密钥，
其中，验证信息是在目标应用程序的业务中需要被验证的信息
S302
网络设备利用密钥对验证信息进行加密，
并将加密的验证信息发送给终端
S303
安全应用程序利用协商的密钥对加密的验证信息进行解密，
获得验证信息
S304
安全应用程序将验证信息提供给所述目标应用程序，和／或，
安全应用程序将验证信息展示给用户

图 3

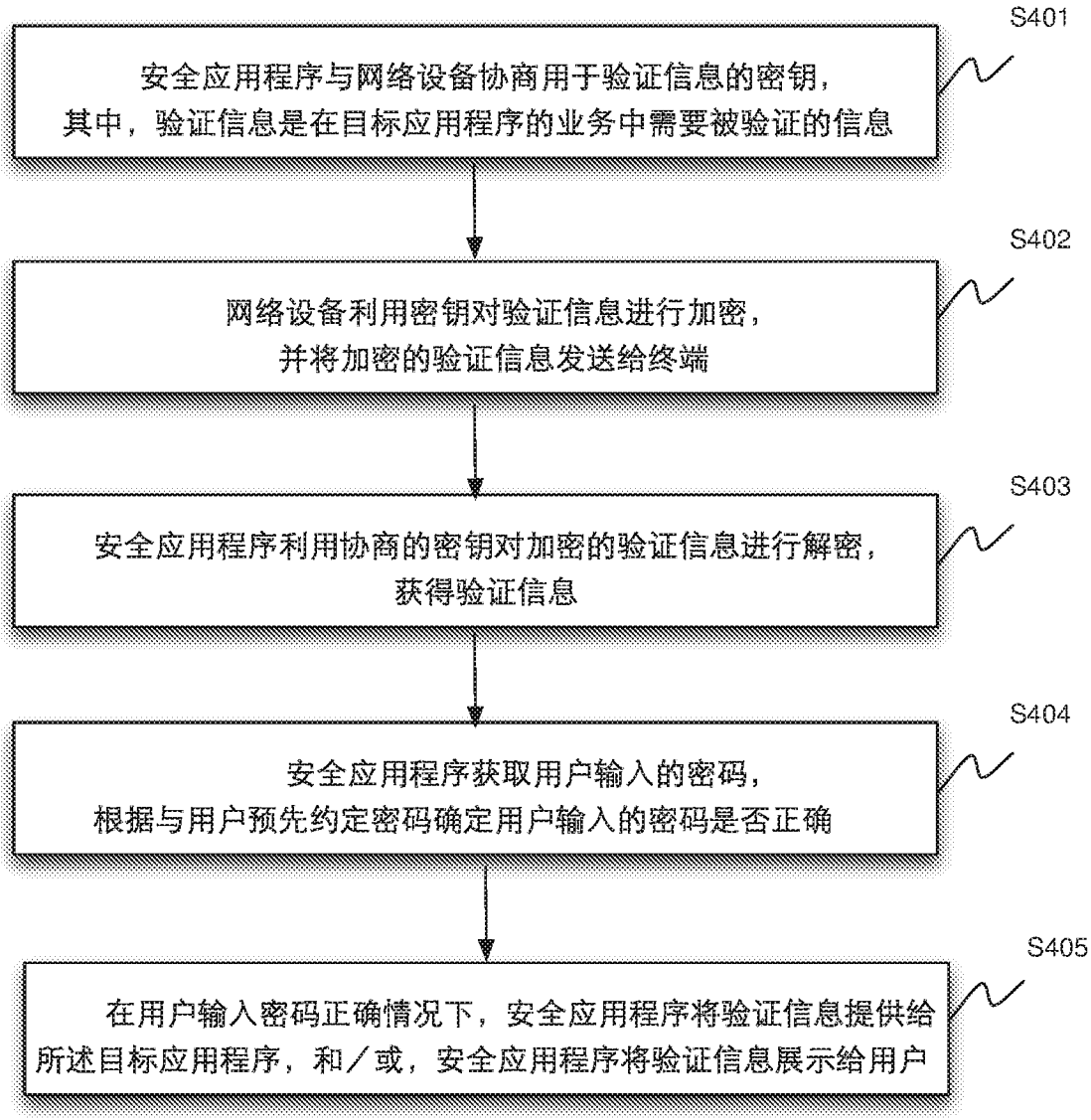
S401
安全应用程序与网络设备协商用于验证信息的密钥，
其中，验证信息是在目标应用程序的业务中需要被验证的信息
S402
网络设备利用密钥对验证信息进行加密，
并将加密的验证信息发送给终端
S403
安全应用程序利用协商的密钥对加密的验证信息进行解密，
获得验证信息
S404
安全应用程序获取用户输入的密码，
根据与用户预先约定密码确定用户输入的密码是否正确
S405
在用户输入密码正确情况下，安全应用程序将验证信息提供给
所述目标应用程序，和／或，安全应用程序将验证信息展示给用户

图 4

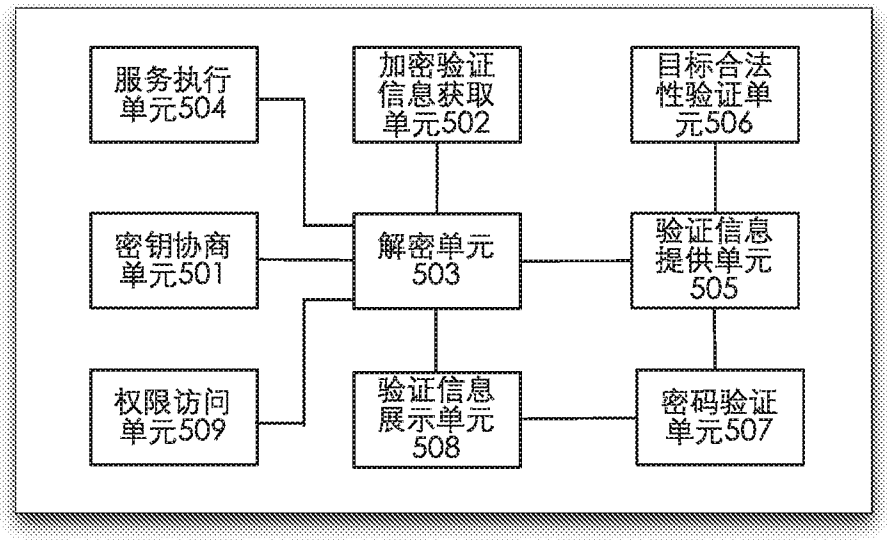
服务执行
单元504
加密验证
信息获取
单元502
目标合法
性验证单
元506
密钥协商
单元501
解密单元
503
验证信息
提供单元
505
权限访问
单元509
验证信息
展示单元
508
密码验证
单元507

图 5

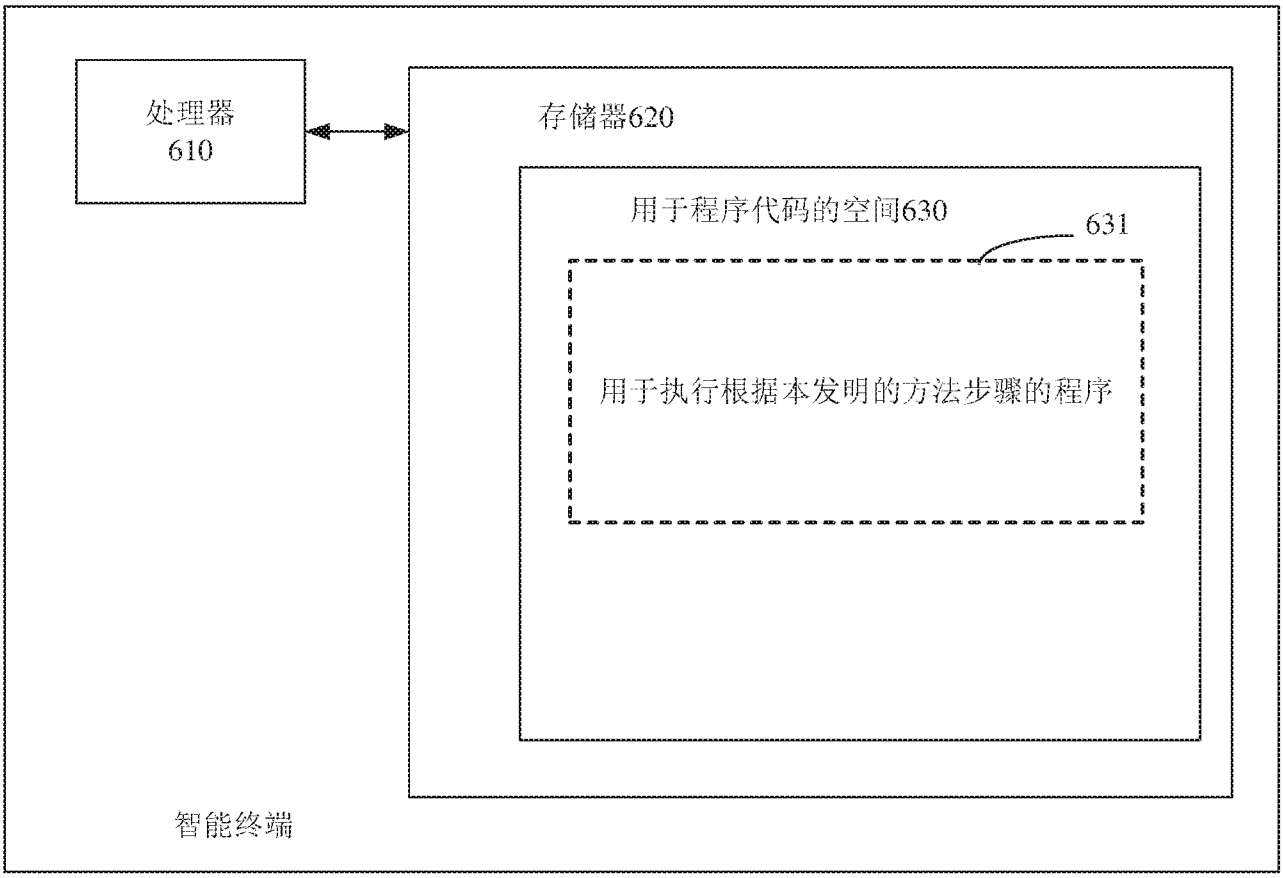
处理器
610
存储器620
用于程序代码的空间630
631
用于执行根据本发明的方法步骤的程序
智能终端

图 6

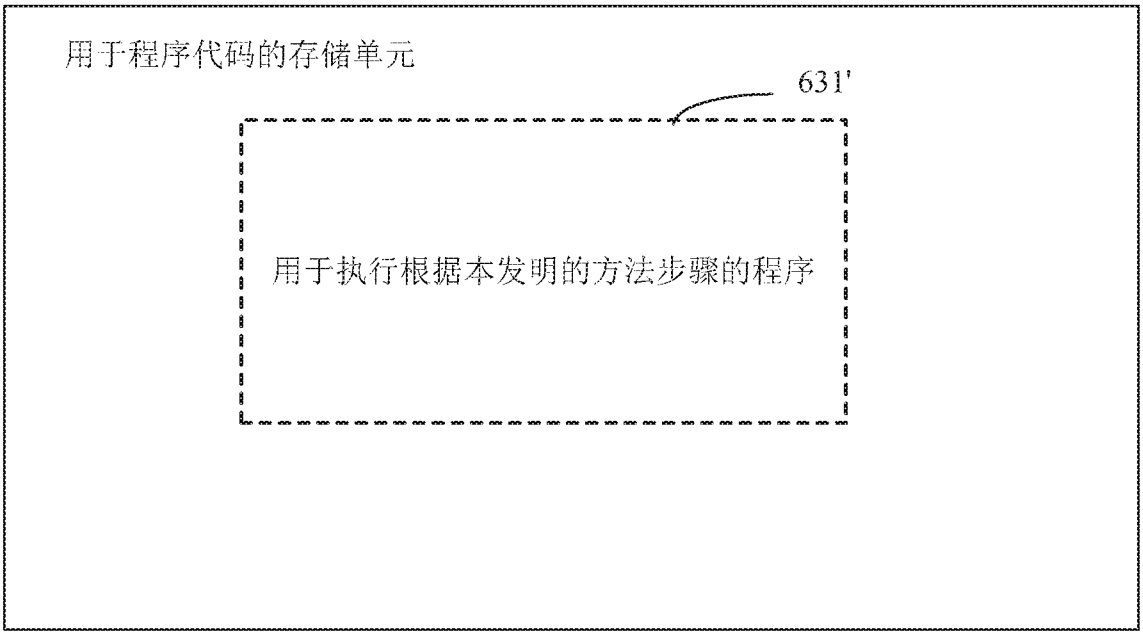
用于程序代码的存储单元
631'
用于执行根据本发明的方法步骤的程序

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/080315

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) 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)

H04L; H04W; H04Q

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)

CNTXT; CPRSABS; SIPOABS; CNKI; DWPI; VEN: network payment, validate, online, pay, server, encrypt, negotiate, terminal, key, authenticat+, cellphone

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103414707 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 27 November 2013 (27.11.2013), description, paragraphs [0024]-[0027]	1-42
A	CN 102780674 A (TONGFANG CO., LTD.), 14 November 2012 (14.11.2012), the whole document	1-42
A	CN 101145908 A (HUAWEI TECHNOLOGIES CO., LTD.), 19 March 2008 (19.03.2008), the whole document	1-42

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 August 2015 (03.08.2015)	**26 August 2015 (26.08.2015)**
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, Yongzhe** Telephone No.: (86-10) **62412024**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/080315

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103414707 A	27 November 2013	None	
CN 102780674 A	14 November 2012	None	
CN 101145908 A	19 March 2008	None	

国际检索报告

国际申请号
PCT/CN2015/080315

A. 主题的分类

H04W 12/06(2009.01)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)

H04L; H04W; H04Q

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）)

CNTXT;CPRSABS;SIPOABS;CNKI;DWPI;VEN:验证，网络支付，服务器，加密，协商，终端，密钥，认证，手机，validate，online，pay，server，encrypt，negotiate，terminal，key，authenticat+，cellphone

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
X	CN 103414707 A (中国联合网络通信集团有限公司) 2013年 11月 27日 (2013-11-27) 说明书第[0024]-[0027]段	1-42
A	CN 102780674 A (同方股份有限公司) 2012年 11月 14日 (2012-11-14) 全文	1-42
A	CN 101145908 A (华为技术有限公司) 2008年 3月 19日 (2008-03-19) 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	国际检索报告邮寄日期
2015年 8月 3日	2015年 8月 26日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	刘永喆 电话号码 (86-10)62412024

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/080315

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	103414707	A	2013年 11月 27日	无	
CN	102780674	A	2012年 11月 14日	无	
CN	101145908	A	2008年 3月 19日	无	