(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103124252 B
(45)授权公告日 2016.08.03

(21)申请号 201110367609.9

(22)申请日 2011.11.18

(73)专利权人 华为软件技术有限公司
地址 210012 江苏省南京市宁南大道11号花神国际大酒店

(72)发明人 陈耿华

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 刘芳

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 1466308 A,2004.01.07,
WO 2010081256 A,2010.07.22,
CN 101083528 A,2007.12.05,
CN 102202300 A,2011.09.28,
CN 101282505 A,2008.10.08,
CN 102004987 A,2011.04.06,

审查员 周萍

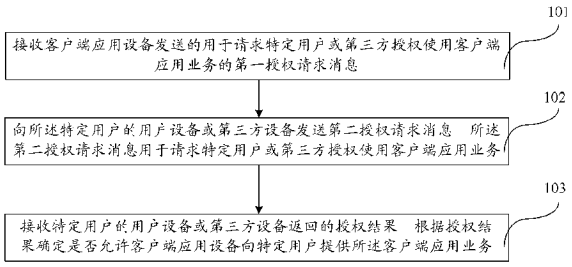
权利要求书3页 说明书8页 附图3页

(54)发明名称

客户端应用访问鉴权处理方法和装置

(57)摘要

本发明实施例提供一种客户端应用访问鉴权处理方法和装置，以及客户端应用业务处理装置和客户端应用设备，其中方法包括：接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息；向所述特定用户的用户设备或第三方设备发送第二授权请求消息，所述第二授权请求消息用于请求所述特定用户或第三方授权使用所述客户端应用业务；接收所述特定用户的用户设备或第三方设备返回的授权结果，根据所述授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务。本发明的技术方案，能够提高SP利用运营商的电信网络能力为目标用户提供服务的安全性。



CN 103124252 B

1.一种客户端应用访问鉴权处理方法,其特征在于,包括:

客户端应用访问鉴权处理装置接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息;

所述客户端应用访问鉴权处理装置向所述特定用户的用户设备或第三方设备发送第二授权请求消息,所述第二授权请求消息用于请求所述特定用户或第三方授权使用所述客户端应用业务;

所述客户端应用访问鉴权处理装置接收所述特定用户的用户设备或第三方设备返回的授权结果,根据所述授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务;

其中,所述客户端应用访问鉴权处理装置接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息之前还包括:

所述客户端应用访问鉴权处理装置接收客户端应用设备发送的第一口令申请消息,向所述客户端应用设备返回为其分配的第一访问口令;

所述客户端应用访问鉴权处理装置根据授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务包括:

在所述授权结果为所述特定用户接受所述客户端应用业务时,客户端应用访问鉴权处理装置授权所述客户端应用设备利用所述第一访问口令访问电信网络能力,向所述特定用户提供所述客户端应用业务;或者,在所述授权结果为所述特定用户接受所述客户端应用业务时,生成与所述第一访问口令对应的验证码,并将所述验证码发送给所述客户端应用设备,并在接收到客户端应用设备发送的携带所述第一访问口令和所述验证码的第二口令申请消息后,向客户端应用设备返回第二访问口令,以授权所述客户端应用设备利用所述第二访问口令访问电信网络能力,向所述特定用户提供所述客户端应用业务。

2.根据权利要求1所述的客户端应用访问鉴权处理方法,其特征在于,在所述客户端应用访问鉴权处理装置接收到所述特定用户的用户设备或第三方设备返回的授权结果后,且所述授权结果为所述特定用户接受所述客户端应用业务时,所述方法还包括:

所述客户端应用访问鉴权处理装置对所述特定用户进行身份认证,并在认证通过后向客户端应用设备返回授权结果。

3.根据权利要求1所述的客户端应用访问鉴权处理方法,其特征在于,若所述客户端应用访问鉴权处理装置根据授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务包括:在所述授权结果为所述特定用户接受所述客户端应用业务时,客户端应用访问鉴权处理装置授权所述客户端应用设备利用所述第一访问口令访问电信网络能力,向所述特定用户提供所述客户端应用业务,所述方法还包括:

所述客户端应用访问鉴权处理装置接收客户端应用设备发送的携带第一访问口令的调用请求消息,并在确认所述第一访问口令可用时,允许客户端应用设备调用电信网络能力,向所述特定用户提供所述客户端应用业务。

4.根据权利要求1所述的客户端应用访问鉴权处理方法,其特征在于,若所述客户端应用访问鉴权处理装置根据授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务包括:在所述授权结果为所述特定用户接受所述客户端应用业务时,生成与所述第一访问口令对应的验证码,并将所述验证码发送给所述客户端应用设备,

并在接收到客户端应用设备发送的携带所述第一访问口令和所述验证码的第二口令申请消息后，向客户端应用设备返回第二访问口令，以授权所述客户端应用设备利用所述第二访问口令访问电信网络能力，向所述特定用户提供所述客户端应用业务，所述方法还包括：

所述客户端应用访问鉴权处理装置接收客户端应用设备发送的携带第二访问口令的业务请求消息，并在确认所述第二访问口令可用时，允许客户端应用设备访问电信网络能力，向所述特定用户提供所述客户端应用业务。

5.根据权利要求1所述的客户端应用访问鉴权处理方法，其特征在于，所述客户端应用访问鉴权处理装置向特定用户的用户设备或第三方设备发送第二授权请求消息包括：

所述客户端应用访问鉴权处理装置按照Web方式、无线应用协议方式、非结构化补充数据业务方式、互动式语音应答或短消息方式向与所述特定用户的用户设备或第三方设备发送第二授权请求消息。

6.根据权利要求1所述的客户端应用访问鉴权处理方法，其特征在于，所述第二授权请求消息包括所述客户端应用业务对应的电信网络能力信息、使用所述网络能力的资费信息和授权使用所述客户端应用业务的期限类型。

7.根据权利要求6所述的客户端应用访问鉴权处理方法，其特征在于，所述授权使用所述客户端应用业务的期限类型包括：

授权单次使用所述客户端应用业务、授权多次使用所述客户端应用业务、授权在一设定期限前使用所述客户端应用业务或授权在一设定时间范围内使用所述客户端应用业务。

8.一种客户端应用访问鉴权处理装置，其特征在于，包括：

第一接收模块，用于接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息；

第一发送模块，用于向所述特定用户的用户设备或第三方设备发送第二授权请求消息，所述第二授权请求消息用于请求所述特定用户或第三方授权使用所述客户端应用业务；

业务授权模块，用于接收所述特定用户的用户设备或第三方设备返回的授权结果，根据所述授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务；

第一口令分配模块，用于在接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息之前，接收客户端应用设备发送的第一口令申请消息，并向所述客户端应用设备返回为其分配的第一访问口令；

所述业务授权模块具体用于在所述授权结果为所述特定用户接受所述客户端应用业务时，授权所述客户端应用设备利用所述第一访问口令访问电信网络能力，向所述特定用户提供所述客户端应用业务；或者，在所述授权结果为所述特定用户接受所述客户端应用业务时，生成与所述第一访问口令对应的验证码，并将所述验证码发送给所述客户端应用设备，并在接收到客户端应用设备发送的携带所述第一访问口令和所述验证码的第二口令申请消息后，向客户端应用设备返回第二访问口令，以授权所述客户端应用设备利用所述第二访问口令访问电信网络能力，向所述特定用户提供所述客户端应用业务。

9.根据权利要求8所述的客户端应用访问鉴权处理装置，其特征在于，还包括：

用户身份认证模块，用于在接收到所述特定用户的用户设备或第三方设备返回的授权

结果后，且所述授权结果为所述特定用户接受所述客户端应用业务时，对所述特定用户进行身份认证，并在认证通过后向客户端应用设备返回授权结果，若生成了与所述第一访问口令对应的验证码，并将所述验证码携带在所述授权结果中发送给所述客户端应用设备。

10.一种客户端应用业务处理装置，其特征在于，包括权利要求8或9所述的客户端应用访问鉴权处理装置和电信网络开放网关模块，所述电信网络开放网关模块用于在接收到客户端应用设备发送的携带访问口令的调用请求消息后，向客户端应用访问鉴权处理装置发送请求对所述访问口令进行认证的鉴权认证请求消息，并在认证通过后为客户端应用设备调用电信网络能力。

11.一种客户端应用设备，其特征在于，包括电信网络接入认证处理模块和电信网络服务调用模块，所述电信网络接入认证处理模块用于向电信运营商的网络系统发送用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息，在特定用户接受所述客户端应用业务时，获取允许调用电信网络能力，向所述特定用户提供客户端应用业务的访问口令；所述电信网络服务调用模块用于向电信运营商的网络系统发送携带所述访问口令的调用请求消息，所述调用请求消息用于请求调用电信网络能力为所述特定用户提供客户端应用业务。

客户端应用访问鉴权处理方法和装置

技术领域

[0001] 本发明实施例涉及通信技术领域，尤其涉及一种客户端应用访问鉴权处理方法和装置。

背景技术

[0002] 随着移动互联网时代的到来，互联网和电信网络越来越紧密的融合到一起。在互联网和用户终端上，涌现了越来越多丰富多彩的互联网应用和终端应用，如Web应用、终端Widget应用、原生终端应用等。这些应用通常需要访问运营商的电信网路能力，以实现特定的业务功能特性，例如，某个交通信息查询的Widget应用，需要能够发送承载交通线路图的彩信消息给某个终端手机用户。因此，运营商需要一种安全、开放、可控的手段，允许客户端应用访问运营商的电信网络能力。

[0003] 现有技术中，运营商电信网络能力的开放，主要是面向可信任的服务提供商(Service Provider，以下简称：SP)的业务应用服务器，SP的各种互联网应用和终端应用为用户提供服务，其访问运营商网络能力主要包括如下的流程：SP的业务应用服务器向运营商的网络运营平台发送访问请求，请求调用运营商的电信网络能力，例如可以是SP的web应用服务器请求调用电信网络能力发送彩信形式的手机报。SP的业务应用服务器发送的访问请求中会携带SP的身份标识、密码以及目标用户的手机号码，运营商的网络运营平台在对SP进行鉴权确认后，便会根据SP业务应用服务器的要求，利用电信网络能力向目标用户提供SP要求的服务，并进一步的对向目标用户提供的服务进行计费。

[0004] 现有技术中，SP利用运营商的电信网络能力为目标用户提供服务的方案安全性差，容易被SP利用提供一些非法业务。

发明内容

[0005] 本发明实施例提供一种客户端应用访问鉴权处理方法和装置，以及客户端应用业务处理装置和客户端应用设备，用以提高SP利用运营商的电信网络能力为目标用户提供服务的方案安全性。

[0006] 本发明实施例提供了一种客户端应用访问鉴权处理方法，包括：

[0007] 接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息；

[0008] 向所述特定用户的用户设备或第三方设备发送第二授权请求消息，所述第二授权请求消息用于请求所述特定用户或第三方授权使用所述客户端应用业务；

[0009] 接收所述特定用户的用户设备或第三方设备返回的授权结果，根据所述授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务。

[0010] 本发明实施例还提供了一种客户端应用访问鉴权处理装置，包括：

[0011] 第一接收模块，用于接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息；

[0012] 第一发送模块，用于向所述特定用户的用户设备或第三方设备发送第二授权请求消息，所述第二授权请求消息用于请求所述特定用户或第三方授权使用所述客户端应用业务；

[0013] 业务授权模块，用于接收所述特定用户的用户设备或第三方设备返回的授权结果，根据所述授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务。

[0014] 本发明实施例还提供了一种客户端应用业务处理装置，包括上述的客户端应用访问鉴权处理装置和电信网络开放网关模块，所述电信网络开放网关模块用于在接收到客户端应用设备发送的携带访问口令的调用请求消息后，向客户端应用访问鉴权处理装置发送请求对所述访问口令进行认证的鉴权认证请求消息，并在认证通过后为客户端应用设备调用电信网络能力。

[0015] 本发明实施例还提供了一种客户端应用设备，包括电信网络接入认证处理模块和电信网络服务调用模块，所述电信网络接入认证处理模块用于向电信运营商的网络系统发送用于请求特定用户授权或第三方使用客户端应用业务的第一授权请求消息，在特定用户接受所述客户端应用业务时，获取允许调用电信网络能力，向所述特定用户提供客户端应用业务的访问口令；所述电信网络服务调用模块用于向电信运营商的网络系统发送携带所述访问口令的调用请求消息，所述调用请求消息用于请求调用电信网络能力为所述特定用户提供客户端应用业务。

[0016] 本发明上述技术方案，其中，SP的客户端应用设备如果要向用户提供客户端应用业务，首先发送第一授权请求消息，然后由设置在电信运营商的网络系统中的客户端应用访问鉴权处理装置处理，其通过向特定用户的用户设备或第三方设备发送第二授权请求消息，询问该特定用户或第三方是否授权使用该客户端应用业务，然后根据特定用户的用户设备或第三方设备返回的授权结果确定是否允许客户端应用设备向所述特定用户提供所述客户端应用业务，进而使得客户端应用设备为特定用户提供的客户端应用业务都是经该特定用户或第三方授权的，提高SP为用户提供客户端应用业务的安全性。

附图说明

[0017] 为了更清楚地说明本发明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一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，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。

[0018] 图1为本发明客户端应用访问鉴权处理方法实施例一的流程示意图；

[0019] 图2为本发明客户端应用访问鉴权处理方法实施例二的流程示意图；

[0020] 图3为本发明客户端应用访问鉴权处理方法实施例三的流程示意图；

[0021] 图4为本发明客户端应用访问鉴权处理装置实施例一的结构示意图；

[0022] 图5为本发明客户端应用访问鉴权处理装置实施例二的结构示意图；

[0023] 图6为本发明客户端应用业务处理装置实施例的结构示意图；

[0024] 图7为本发明客户端应用设备实施例的结构示意图。

具体实施方式

[0025] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0026] 针对现有技术中SP利用运营商的电信网络能力为用户提供服务时安全性差的问题，本发明实施例提供了一种解决方案，其是通过在电信运营商的网络系统中增加客户端应用访问鉴权处理装置实现的，图1为本发明客户端应用访问鉴权处理方法实施例一的流程示意图，如图1所示，包括如下的步骤：

[0027] 步骤101、接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息；

[0028] 步骤102、向所述特定用户的用户设备或第三方设备发送第二授权请求消息，所述第二授权请求消息用于请求所述特定用户或第三方授权使用所述客户端应用业务；

[0029] 步骤103、接收所述特定用户的用户设备或第三方设备返回的授权结果，根据所述授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务。

[0030] 本发明上述实施例中，SP的客户端应用设备如果要向该客户端用户提供客户端应用业务，首先发送第一授权请求消息，然后由设置在电信运营商的网络系统中的客户端应用访问鉴权处理装置处理，其通过向特定用户的用户设备或第三方设备发送第二授权请求消息，询问该特定用户或第三方是否授权使用该客户端应用业务，然后根据特定用户的用户设备或第三方设备返回的授权结果确定是否允许客户端应用设备向所述特定用户提供所述客户端应用业务，进而使得客户端应用设备为特定用户提供的客户端应用业务都是经该特定用户或第三方授权的，提高SP为用户提供客户端应用业务的安全性。

[0031] 本发明上述实施例中的第二授权请求消息可以是特定用户所持有的用户设备，以由特定用户自身确认是否接受客户端应用业务，也可以是由第三方确认，例如上述的第三方设备可以是特定用户的管理者所持有的设备，由该特定用户的管理者确认特定用户是否接受客户端应用业务，或者是由运营商的服务器作为第三方设备，由运营商确定特定用户是否接受客户端应用业务。

[0032] 本发明上述实施例中运营商能够根据特定用户或第三方的意愿确定是否为其提供客户端应用业务，也就是确定是否允许客户端应用设备访问电信网络能力，在客户端应用设备中可以设置相应的电信网络接入认证处理装置执行相应的处理，在具体的实施过程中，可以通过向客户端应用设备分配访问口令的方式，控制客户端应用设备对电信网络的访问，具体的可以包括两种实施方式。

[0033] 一种是在客户端应用设备发送的用于请求特定用户授权使用客户端应用业务的第一授权请求消息之前，首先向电信运营商的网络系统中的客户端应用访问鉴权处理装置发送第一口令申请消息，客户端应用访问鉴权处理装置接收到客户端应用设备发送的第一口令申请消息后，向所述客户端应用设备返回为其分配的所述第一访问口令。上述的第一访问口令可以看作是一个临时口令，并未生效，客户端应用设备无法根据该临时口令访问运营商的电信网络能力。只有在特定用户的用户设备或第三方设备返回授权结果，并且所

述授权结果为所述特定用户接受所述客户端应用业务时，才可以在本地系统内将上述的第一访问口令的性质改变为正式口令，以授权所述客户端应用设备利用所述第一访问口令访问电信网络能力，向所述特定用户提供所述客户端应用业务。进而客户端应用设备可以利用该第一访问口令执行客户端应用业务，具体的是客户端应用设备向电信运营商的网络系统中的第一业务处理模块发送携带第一访问口令的业务请求消息，上述第一业务处理模块在接收到业务请求消息，并在确认上述第一访问口令可用时，允许客户端应用设备访问电信网络能力，向所述特定用户提供客户端应用业务，具体的可以向电信运营商的网络系统中的客户端应用访问鉴权处理装置确认所述第一访问口令是否可用。

[0034] 另外还有一种实施方式，与上述实施例不同之处在于，运营商的客户端应用访问鉴权处理装置在上述授权结果为所述特定用户接受所述客户端应用业务时，不是改变第一访问口令的性质，而是生成与所述第一访问口令对应的验证码，并将所述验证码发送给所述客户端应用设备，在接收到客户端应用设备发送的携带所述第一访问口令和所述验证码的第二口令申请消息后，向客户端应用设备返回第二访问口令，该第二访问口令为正式口令，以授权所述客户端应用设备利用所述第二访问口令访问电信网络能力，向所述特定用户提供所述客户端应用业务。

[0035] 具体的，在使用第二访问口令时，客户端应用设备向电信运营商的网络系统中的第二业务处理模块发送携带第二访问口令的业务请求消息，上述第二业务处理接收业务请求消息，并在确认所述第二访问口令可用时，允许客户端应用设备访问电信网络能力，向所述特定用户提供所述客户端应用业务，具体的可以向电信运营商的网络系统中的客户端应用访问鉴权处理装置确认所述第二访问口令是否可用。

[0036] 本发明上述实施例中，在接收到所述特定用户的用户设备或第三方设备返回的授权结果，并确认所述授权结果为所述特定用户接受所述客户端应用业务后，还可以进一步对所述特定用户进行身份认证，并在认证通过后向客户端应用设备返回授权结果，具体的，针对上述使用第二访问口令的实施例，可以是先生成与第一访问口令对应的验证码，再将所述验证码携带在授权结果中发送给所述客户端应用设备。

[0037] 图2为本发明客户端应用访问鉴权处理方法实施例二的流程示意图，如图2所示，包括如下的步骤：

[0038] 步骤201、客户端应用设备的电信网络接入认证处理装置在访问运营商电信网络能力之前，先到电信运营商的网络系统中的客户端应用访问鉴权处理装置申请临时口令，即发送第一口令申请消息，本发明实施例中的客户端应用设备，按照终端类型划分，可以分为移动终端客户端，例如手机、PDA，或者是计算机客户端等；按照客户端应用开发语言，可以分为Widge应用客户端、JAVA应用客户端、Brew应用客户端、Web客户端等。其中的电信网络接入认证处理装置为客户端应用设备内部设置的，专用于向电信网络进行认证的功能模块；

[0039] 步骤202、运营商网络系统的客户端应用访问鉴权处理装置在对客户端应用设备进行认证通过后，向电信网络接入认证处理装置返回为其分配的第一访问口令，该第一访问口令为一临时口令，并未生效，也就是客户端应用设备不能够直接使用该第一访问口令访问电信网络；

[0040] 步骤203、电信网络接入认证处理装置向客户端应用访问鉴权处理装置发送第一

授权请求消息，请求特定用户或第三方授权使用客户端应用业务；

[0041] 步骤204、客户端应用访问鉴权处理装置向特定用户的用户设备或第三方设备发送第二授权请求消息，该第二授权请求消息用于请求所述特定用户授权使用所述客户端应用业务；具体的，该请求方式可以按照Web方式、无线应用协议(Wireless Application Protocol，以下简称：WAP)方式、非结构化补充数据业务(Unstructured Supplementary Service Data，以下简称：USSD)方式、互动式语音应答(Interactive Voice Response，以下简称：IVR)或短消息方式向与所述特定用户的用户设备发送第二授权请求消息。可选的，该第二授权请求消息可以包括客户端应用业务对应的电信网络能力信息、使用所述电信网络能力的资费信息和授权使用所述客户端应用业务的期限类型，例如授权单次使用上述客户端应用业务、授权多次使用上述客户端应用业务、授权在一设定期限前使用上述客户端应用业务或授权在一设定时间范围内使用上述客户端应用业务；

[0042] 步骤205、特定用户或第三方进行授权操作，向客户端应用访问鉴权处理装置返回授权结果，对于不同的请求方式，用户可以用不同方式提交身份认证信息并进行授权，例如对于Web或WAP页面，用户可以在Web或WAP页面上提交个人用户名和密码，并在页面上确认同意使用客户端应用业务；对于短消息的请求方式，用户可以通过确认回复短消息的方式，向电信运营商的网络系统中的客户端应用访问鉴权处理装置返回授权结果；

[0043] 步骤206、客户端应用访问鉴权处理装置识别特定用户的用户设备或第三方设备返回的授权结果，并在特定用户接受上述客户端应用业务时，对特定用户进行身份认证；

[0044] 步骤207、在对特定用户的身份认证通过后，客户端应用访问鉴权处理装置向电信网络接入认证处理装置返回授权结果，同时将步骤202中返回的第一访问口令的性质修改为正式口令，以使得客户端应用设备可以访问电信网络为特定用户提供服务；

[0045] 步骤208、客户端应用设备利用第一访问口令发起调用请求消息，具体的，可以是客户端应用设备的电信网络服务调用模块向电信运营商的网络系统中的电信网络开放网关模块发送调用请求消息，调用电信网络能力，访问运营商的电信网络；

[0046] 步骤209、电信网络开放网关模块在接收到上述的调用请求消息后，获取调用请求消息中携带的第一访问口令，并向客户端应用访问鉴权处理装置发送鉴权认证请求消息，进一步的，对于第一访问口令，是在接收到特定用户的授权结果后，将其性质转变为正式口令的，每一个该第一访问口令都是与特定用户对应的，因此，该第一访问口令仅允许向特定用户提供服务，在步骤208中的调用请求消息中，还可以进一步的携带用户标识，例如用户使用手机的SIM卡号，本步骤中会进一步对该用户标识进行认证，以确定其是否与第一访问口令对应，以防止客户端应用设备利用第一访问口令为其他用户提供服务；

[0047] 步骤210、客户端应用访问鉴权处理装置对用户标识和第一访问口令的合法性、有效期进行认证；

[0048] 步骤211、客户端应用访问鉴权处理装置向电信网络开放网关模块返回鉴权认证结果；

[0049] 步骤212、电信网络开放网关模块在认证通过后，调用电信网络能力，并将调用结果返回给客户端应用设备，为特定用户提供服务。

[0050] 本发明上述实施例中，其中步骤206中在特定用户接受客户端应用业务后，对特定用户的用户身份进行了身份认证，在实际应用中，该步骤为可选步骤，可以不执行上述的身

份认证过程，或者也可以是在上述步骤204中向特定用户的用户设备或第三方设备发送第二授权请求消息之前进行身份认证，并在身份认证通过后，再执行向特定用户的用户设备或第三方设备发送第二授权请求消息的步骤。本发明上述实施例中，其中的客户端应用访问鉴权处理装置可以设置在在运营商网络系统的各网关设备中，其具体的设置位置不影响本发明技术方案的实施。本实施例中在调用电信网络能力，为特定用户提供客户端应用业务之前，首先向特定用户或第三方去请求授权，在得到授权后再提供客户端应用业务，能够提高SP为用户提供业务的安全性。

[0051] 上述图2所示的实施例是对应只分配第一访问口令的实施方案，图3为本发明客户端应用访问鉴权处理方法实施例三的流程示意图，该实施例中客户端应用访问鉴权处理装置会进一步分配第二访问口令作为正式口令，如图3所示，包括如下的步骤：

[0052] 步骤301～步骤306与上述实施例中的步骤201～步骤206完成基本相同的功能。

[0053] 步骤307、在对特定用户的身份认证通过后，生成与所述第一访问口令对应的验证码；

[0054] 步骤308、向电信网络接入认证处理装置返回授权结果，该授权结果中携带上述验证码；

[0055] 步骤309、电信网络接入认证处理装置向运营商的客户端应用访问鉴权处理装置发送携带所述第一访问口令和所述验证码的第二口令申请消息；

[0056] 步骤310、客户端应用访问鉴权处理装置分配第二访问口令，该第二访问口令为正式口令，用于授权所述客户端应用设备利用该第二访问口令访问电信网络能力，并向上述特定用户提供所述客户端应用业务；

[0057] 步骤311、客户端应用访问鉴权处理装置向电信网络接入认证处理装置返回第二访问口令；

[0058] 步骤312～步骤316同上述实施例的步骤208～步骤212完成基本相同的功能，区别仅在于电信网络接入认证处理装置利用第二访问口令发起调用请求消息。

[0059] 本实施例中，通过分别为客户端应用设备分配第一访问口令和第二访问口令，最后由客户端应用设备依据第二访问口令调用电能网络能力，为特定用户提供客户端应用业务，能够提高SP为用户提供客户单应用业务的安全性。

[0060] 本发明实施例还提供了一种客户端应用访问鉴权处理装置，图4为本发明客户端应用访问鉴权处理装置实施例一的结构示意图，如图4所示，该客户端应用访问鉴权处理装置40包括第一接收模块11、第一发送模块12和业务授权模块13，其中第一接收模块11用于接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息；第一发送模块12用于向所述特定用户的用户设备或第三方设备发送第二授权请求消息，所述第二授权请求消息用于请求所述特定用户或第三方授权使用所述客户端应用业务；业务授权模块13用于接收所述特定用户的用户设备或第三方设备返回的授权结果，根据所述授权结果确定是否允许所述客户端应用设备向所述特定用户提供所述客户端应用业务。

[0061] 本发明实施例中，由设置在电信运营商的网络系统中的客户端应用访问鉴权处理装置接收第一授权请求消息后，向特定用户的用户设备或第三方设备发送第二授权请求消息，询问该特定用户或第三方是否授权使用该客户端应用业务，然后根据特定用户的用户

设备或第三方设备返回的授权结果确定是否允许客户端应用设备向所述特定用户提供所述客户端应用业务，进而使得客户端应用设备为特定用户提供的客户单应用业务都是经该特定用户授权的，提高SP为用户提供业务的安全性。

[0062] 在上述的方法实施例中已经介绍了，可以通过口令的方式控制客户端应用设备访问电信网络为特定用户提供服务，具体的可以包括仅分配一次访问口令和分配两次访问口令的情形，分别对应图2和图3所示的方法实施例。

[0063] 针对上述图2所示的实施例，对于只需分配第一访问口令的情形，可以如图5所示，客户端应用访问鉴权处理装置50进一步包括第一口令分配模块14，该第一口令分配模块14用于在接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息之前，接收客户端应用设备发送的第一口令申请消息，并向所述客户端应用设备返回为其分配的所述第一访问口令；而上述的业务授权模块13具体用于在所述授权结果为所述特定用户接受所述客户端应用业务时，授权所述客户端应用设备利用所述第一访问口令访问电信网络能力，向所述特定用户提供所述客户端应用业务。

[0064] 针对上述图3所示的实施例，需要分配第一访问口令和第二访问口令的情形，也包括上述的第一口令分配模块14，为客户端应用设备分配第一访问口令，而其中的业务授权模块13具体用于在授权结果为所述特定用户接受所述客户端应用业务时，生成与所述第一访问口令对应的验证码，并将所述验证码发送给所述客户端应用设备，并在接收到客户端应用设备发送的携带所述第一访问口令和所述验证码的第二口令申请消息后，向客户端应用设备返回第二访问口令，以授权所述客户端应用设备利用所述第二访问口令访问电信网络能力，向所述特定用户提供所述客户端应用业务。

[0065] 另外，本发明实施例中还可以进一步的对特定用户的身份进行认证，即在客户端应用访问鉴权处理装置中设置用户身份认证模块15，该用户身份认证模块15用于在接收到所述特定用户的用户设备或第三方设备返回的授权结果后，且所述授权结果为所述特定用户接受所述客户端应用业务时，对所述特定用户进行身份认证，并在认证通过后向客户端应用设备返回授权结果，若生成了与所述第一访问口令对应的验证码，并将所述验证码携带在所述授权结果中发送给所述客户端应用设备。

[0066] 进一步的，本发明实施例还提供了一种客户端应用业务处理装置，图6为本发明客户端应用业务处理装置实施例的结构示意图，如图6所示，客户端应用业务处理装置60包括客户端应用访问鉴权处理装置21和电信网络开放网关模块22，其中客户端应用访问鉴权处理装置21可以采用上述任一实施例提供的客户端应用访问鉴权处理装置，而电信网络开放网关模块22用于在接收到客户端应用设备发送的携带访问口令的调用请求消息后，向客户端应用访问鉴权处理装置发送请求对所述访问口令进行认证的鉴权认证请求消息，并在认证通过后为客户端应用设备调用电信网络能力。

[0067] 本发明实施例还提供了一种客户端应用设备，图7为本发明客户端应用设备实施例的结构示意图，如图7所示，客户端应用设备70包括电信网络接入认证处理模块31和电信网络服务调用模块32，所述电信网络接入认证处理模块31用于向电信运营商的网络系统发送用于请求特定用户授权使用客户端应用业务的第一授权请求消息，在特定用户接受所述客户端应用业务时，获取允许调用电信网络能力，向所述特定用户提供客户端应用业务的访问口令；电信网络服务调用模块32用于向电信运营商的网络系统发送携带所述访问口令

的调用请求消息，所述调用请求消息用于请求调用电信网络能力为所述特定用户提供客户端应用业务。

[0068] 本发明上述实施例提供的客户端应用访问鉴权处理方法、装置，以及客户端应用业务处理装置、客户端应用设备，其中在调用电信网络能力为用户提供客户端应用业务前，首先向特定用户使用的用户设备或第三方设备发送授权请求消息，以请求授权该特定用户使用上述的客户端应用业务，在用户接受上述客户端应用业务后，再授权所述客户端应用设备访问电信网络能力，向所述特定用户提供所述客户端应用业务，通过上述技术方案，能够提高SP为用户提供客户端应用业务的安全性。另外，运营商也可以是在获得用户同意的情况下为其提供服务，并根据服务进行计费，能够有效防止第三方应用运营商的电信网络能力进行计费欺诈。

[0069] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0070] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

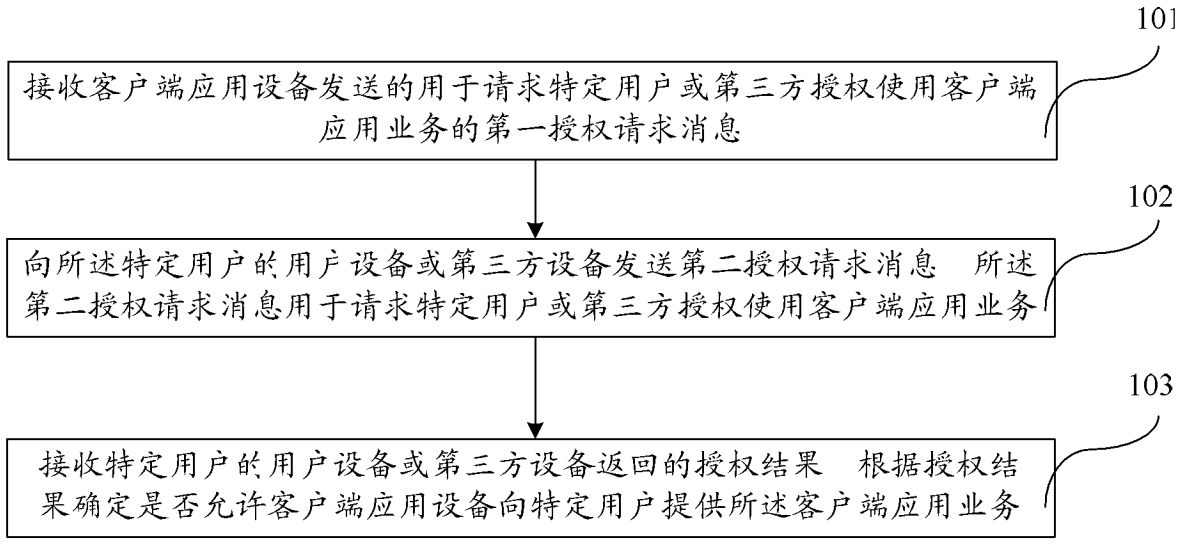

101
接收客户端应用设备发送的用于请求特定用户或第三方授权使用客户端应用业务的第一授权请求消息
102
向所述特定用户的用户设备或第三方设备发送第二授权请求消息，所述第二授权请求消息用于请求特定用户或第三方授权使用客户端应用业务
103
接收特定用户的用户设备或第三方设备返回的授权结果，根据授权结果确定是否允许客户端应用设备向特定用户提供所述客户端应用业务

图1

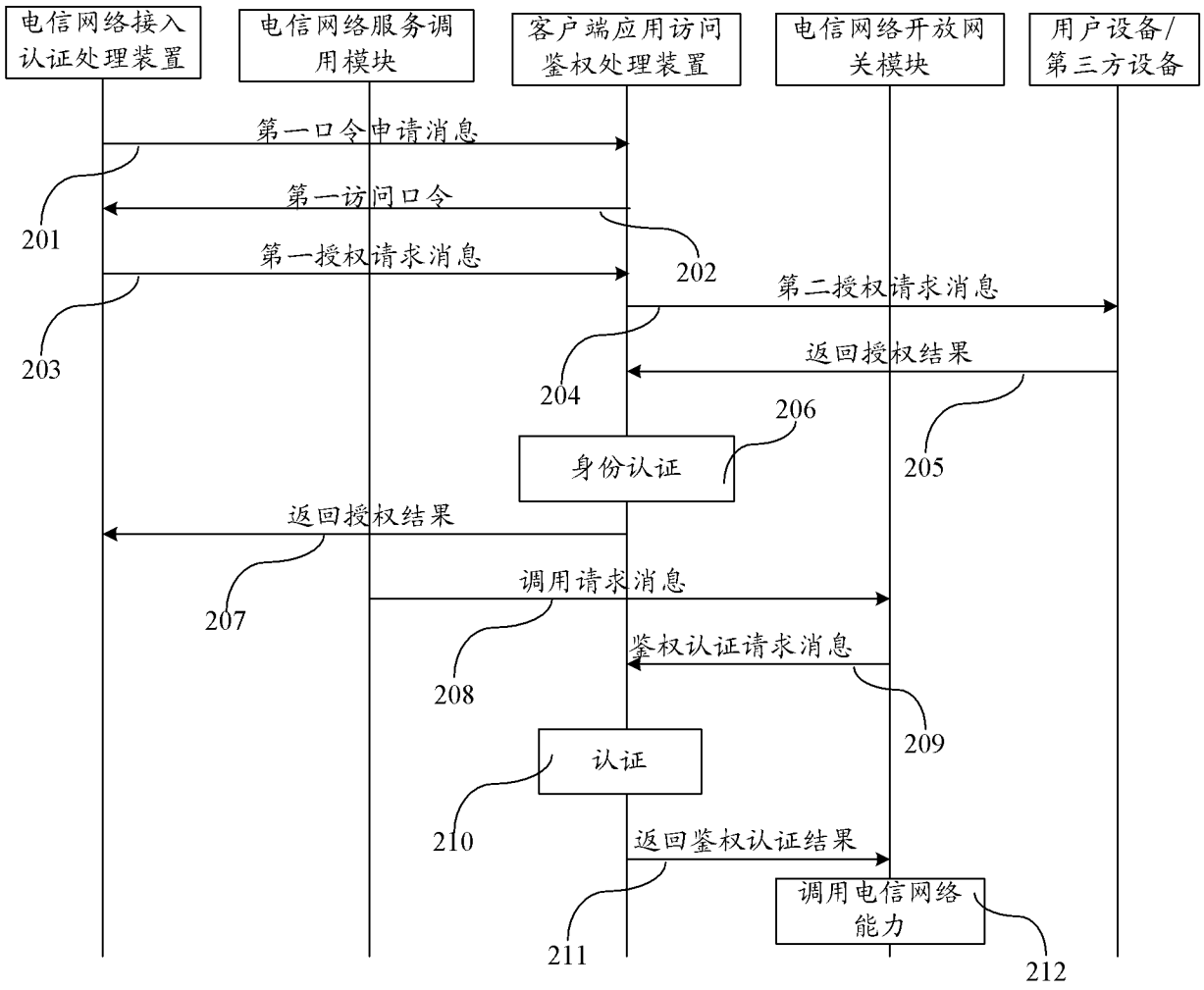

电信网络接入认证处理装置
电信网络服务调用模块
客户端应用访问鉴权处理装置
电信网络开放网关模块
用户设备/第三方设备
第一口令申请消息
201
第一访问口令
202
第一授权请求消息
203
第二授权请求消息
204
返回授权结果
205
206
身份认证
返回授权结果
207
调用请求消息
208
鉴权认证请求消息
209
认证
210
返回鉴权认证结果
211
调用电信网络能力
212

图2

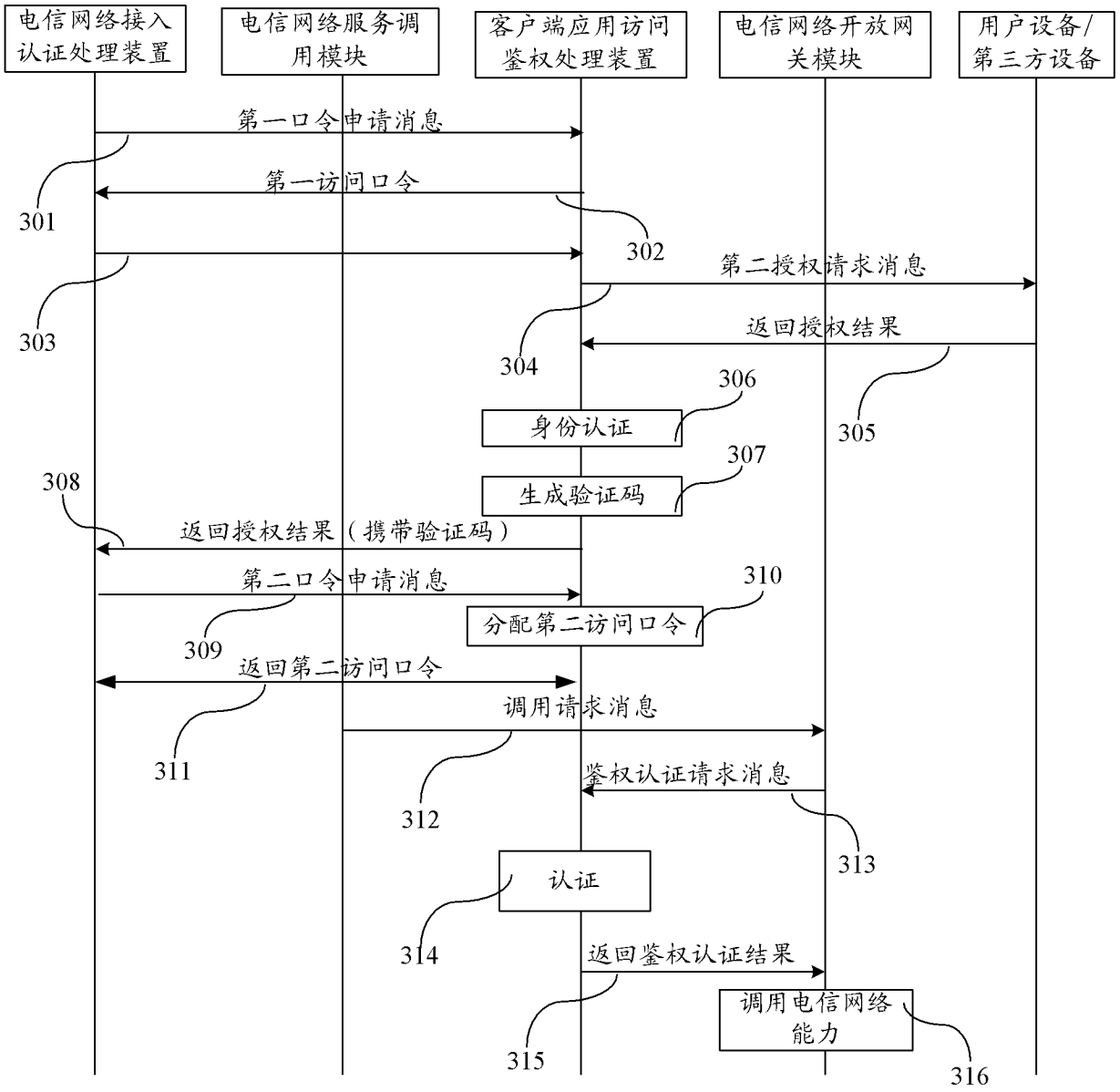

电信网络接入认证处理装置
电信网络服务调用模块
客户端应用访问鉴权处理装置
电信网络开放网关模块
用户设备/第三方设备
第一口令申请消息
301
第一访问口令
302
303
第二授权请求消息
304
返回授权结果
305
306
身份认证
307
生成验证码
308
返回授权结果（携带验证码）
第二口令申请消息
309
310
分配第二访问口令
返回第二访问口令
311
调用请求消息
312
鉴权认证请求消息
313
认证
314
返回鉴权认证结果
315
调用电信网络能力
316

图3

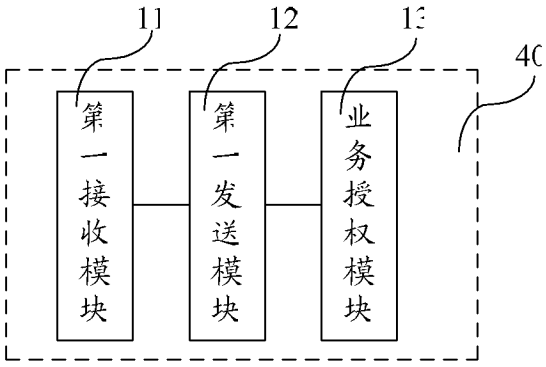

11
12
13
40
第一接收模块
第一发送模块
业务授权模块

图4

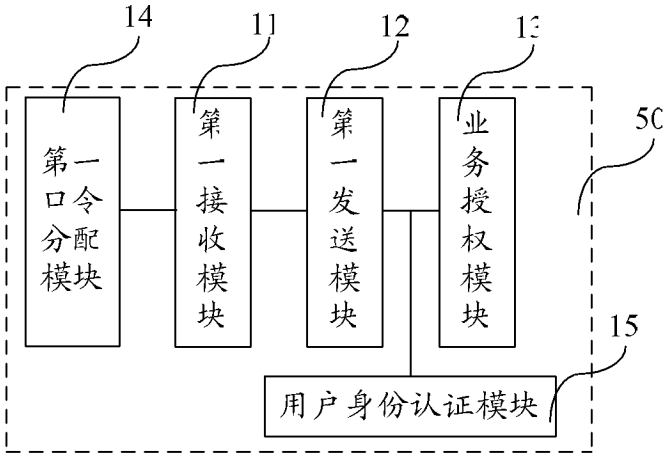

14
11
12
13
50
第一令牌分配模块
第一接收模块
第一发送模块
业务授权模块
15
用户身份认证模块

图5

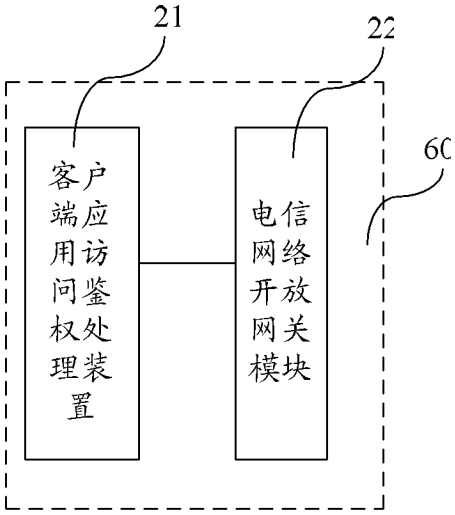

21
22
60
客户端应用访问鉴权处理装置
电信网络开放关网模块

图6

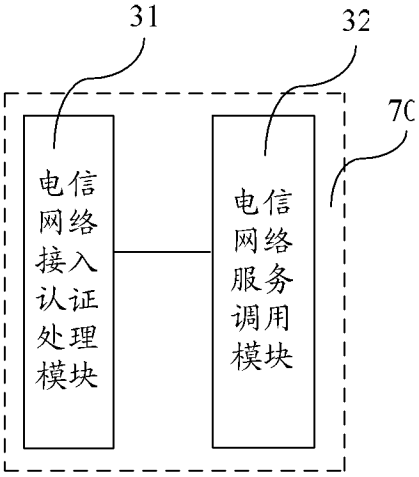

31
32
70
电信网络接入认证处理模块
电信网络服务调用模块

图7