(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 102724647 B
(45)授权公告日 2014.08.13

(21)申请号 201210184762.2
(22)申请日 2012.06.06
(73)专利权人 电子科技大学
地址 611731 四川省成都市高新区(西区)西源大道2006号
(72)发明人 刘梦娟 王聪 柯涛 赵洋 张朋
(74)专利代理机构 成都行之专利代理事务所(普通合伙) 51220
代理人 温利平
(51)Int.Cl.
*H04W 4/24*(2009.01)
*H04W 12/04*(2009.01)
*H04W 12/06*(2009.01)
(56)对比文件
CN 102196012 A,2011.09.21, 全文.
CN 102394887 A,2012.03.28, 全文.
CN 101789973 A,2010.07.28, 全文.
US 2003163733 A1,2003.08.28, 全文.
审查员 张倩

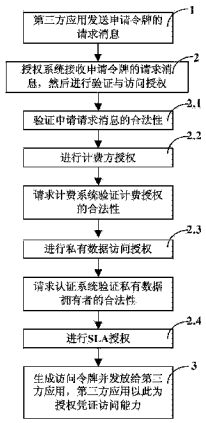
权利要求书3页 说明书10页 附图5页

(54)发明名称

一种能力访问授权方法及系统

(57)摘要

本发明公开了一种能力访问授权方法及系统,针对业务能力开放平台的授权进行管理:(1)第三方应用在访问业务能力时,需要获得业务计费方的显示授权;(2)第三方应用访问与终端用户私有数据相关的业务能力时,为保证终端用户数据的安全性、隐私性,需要获得私有数据拥有者的显示授权;(3)需要获得能力开放平台服务等级协定系统的授权;在获得多方授权以后,由授权系统生成相应的访问令牌,发放给第三方应用,第三方应用携带访问令牌,以访问令牌作为能力访问授权凭证即可直接访问对应的能力接口,从而确保业务能力开放平台的业务能力被合法的第三方应用进行合理的访问。




CN 102724647 B

1. 一种能力访问授权方法，其特征在于，包括以下步骤：

步骤 1、第三方应用向业务能力开放平台的授权系统发送申请某个能力接口访问令牌的请求消息，请求消息至少包括：申请访问的能力接口的名称，能力访问的计费方，第三方应用标识符，授权用户的终端地址，授权用户的终端 MSISDN 号，需用户授权私有数据的列表，以及含有第三方应用密钥的签名；

步骤 2、业务能力开放平台的授权系统接收申请访问令牌的请求消息，然后进行：

2.1)、验证访问令牌申请请求消息本身的合法性

验证请求消息本身的合法性包括第三方应用的合法性、申请访问的能力接口的合法性以及请求消息参数的合法性；

其中，第三方应用的合法性由请求消息中携带的第三方应用标识符和含有第三方应用密钥的签名为基础进行验证；

申请访问的能力接口的合法性由请求消息中携带的申请访问的能力接口的名称为基础进行验证；

请求消息参数的合法性验证包括请求消息中所有携带参数的格式和范围是否符合规范；

如果请求消息不合法，则授权系统返回“访问令牌申请不合法”的响应消息给第三方应用，终止授权过程，如果请求消息合法，则进行步骤 2.2；

2.2)、计费授权与验证

如果申请访问的能力接口是免费的，则直接执行步骤 2.3，否则根据请求消息中标识的计费方，计费方根据请求消息中携带的能力访问的计费方参数确定，向计费方发送计费授权的请求消息；

计费方接收计费授权的请求消息，对申请的能力访问的计费进行授权，并将授权信息返回给授权系统；

授权系统根据计费方返回的授权信息进行判断，如果计费方不同意授权，则返回“无计费方授权”的响应消息给第三方应用，终止授权过程；如果计费方同意授权，则要求能力开放平台的计费系统根据计费方式，验证计费方是否合法，如果计费方合法，则执行步骤 2.3，否则返回“计费方资费不够”或“信用度不够”的响应消息给第三方应用，终止授权过程；

2.3)、私有数据访问授权与验证

如果申请访问的能力接口不涉及私有数据，则直接执行步骤 2.4；否则发送私有数据访问授权的请求消息给私有数据的拥有者，如果该拥有者为在线状态，则其地址由请求消息中携带的授权用户的终端地址标识，如果该拥有者处于离线状态，则其地址由授权用户的终端 MSISDN 号标识；

私有数据的拥有者收到私有数据访问授权的请求消息，对申请的私有数据，即以访问令牌请求消息中携带的需用户授权私有数据的列表中数据的访问进行授权，并将授权信息返回给授权系统；

授权系统根据私有数据拥有者返回的授权信息进行判断，如果私有数据拥有者不同意授权，则授权系统返回“访问私有数据出错”的响应消息给第三方应用，终止授权过程；如果私有数据拥有者同意授权，则要求能力开放平台的认证系统验证私有数据拥有者，即授权用户是否合法，如果合法，则执行步骤 2.4，否则返回“授权用户不合法”的响应消息给第三

方应用，终止授权过程；

2.4)、SLA（Service Level Agreement）授权

授权系统要求能力开放平台的SLA（Service Level Agreement，服务等级协定）系统对第三方应用访问能力接口的合理性进行授权，如果第三方应用访问能力接口的频率符合预先签署的SLA合约，则SLA系统同意授权，否则SLA系统拒绝授权；

授权系统根据SLA系统的授权情况，如果SLA系统同意授权，则执行步骤3；否则返回“请求过于频繁”的响应消息给第三方应用，终止授权过程；

步骤3、访问令牌生成及发放

授权系统根据第三方应用的能力接口访问申请请求，生成一个唯一的涵盖计费、私有数据访问以及SLA授权的访问令牌发放给第三方应用；

步骤4、能力接口访问

第三方应用携带访问令牌，以访问令牌作为能力访问授权凭证直接访问业务能力开放平台相应的能力接口，能力服务器执行相应的能力访问，并将能力访问结果返回给第三方应用，完成能力访问。

2. 根据权利要求1所述的能力访问授权方法，其特征在于，所述的能力接口访问为：

4.1)、第三方应用接收授权系统返回的能力接口访问令牌，然后向业务能力开放平台的能力服务器发送能力接口访问的请求消息，所述请求消息包括访问的能力接口的名称、属性参数及对应接口的访问令牌；

4.2)、能力服务器接收访问请求，检验属性参数的合法性，如果参数不合法，则执行步骤4.3，否则执行步骤4.4；

4.3)、能力服务器返回“属性参数不合法”的响应消息给第三方应用，终止执行所述能力访问过程；

4.4)、能力服务器请求业务能力开放平台的授权系统对收到的访问令牌进行验证；

4.5)、授权系统验证访问令牌的有效性；

4.6)、授权系统返回访问令牌有效性验证结果给能力服务器；

4.7)、能力服务器接收验证结果，如果访问令牌有效，则执行步骤4.9；否则执行步骤4.8；

4.8)、能力服务器返回“访问令牌失效”的响应消息给第三方应用，终止执行所述能力访问过程；

4.9)、能力服务器相应的能力接口执行能力访问；

4.10)、能力服务器将能力访问结果返回给第三方应用，完成能力访问。

3. 一种能力访问授权系统，其特征在于，包括：

令牌申请合法性验证模块，用于验证访问令牌申请本身请求消息的合法性，包括第三方应用的合法性、申请访问的能力接口的合法性以及请求消息参数的合法性；

如果请求消息不合法，则授权系统返回“访问令牌申请不合法”的响应消息给第三方应用，终止授权过程，如果请求消息合法，则将令牌申请请求消息递交给计费授权模块继续处理；

计费授权模块，用于向计费方发起授权请求，以及接收计费方返回的授权响应：

如果申请访问的能力接口是免费的，则将令牌申请请求消息递交给私有数据访问授权

模块继续处理，否则根据请求消息中标识的计费方，计费授权模块向计费方发送计费授权的请求消息；

计费方收到计费授权的请求消息，对申请的能力访问的计费进行授权，并将授权信息返回给计费授权模块；

计费授权模块根据计费方返回的授权信息进行判断，如果计费方不同意授权，则返回“无计费方授权”的响应消息给第三方应用，终止授权过程；如果计费方同意授权，则要求能力开放平台的计费系统根据计费方式验证计费方是否合法，如果计费方合法，则令牌申请请求消息递交给私有数据访问授权模块继续处理，否则返回“计费方资费不够”或“信用度不够”的响应消息给第三方应用，终止授权过程；

私有数据访问授权模块，用于向私有数据拥有者发起授权请求，以及接收私有数据拥有者返回的授权响应：

如果申请访问的能力接口不涉及私有数据，则将令牌申请请求消息递交给 SLA 授权模块继续处理；否则发送私有数据访问授权的请求消息给私有数据的拥有者；

私有数据的拥有者收到私有数据访问授权的请求消息，对申请的私有数据访问进行授权，并将授权信息返回给私有数据访问授权模块；

私有数据访问授权模块根据私有数据拥有者返回的授权信息进行判断，如果私有数据拥有者不同意授权，否则返回“访问私有数据出错”的响应消息给第三方应用，终止授权过程；如果私有数据拥有者同意授权，则要求能力开放平台的认证系统验证私有数据拥有者是否合法，如果合法，则将令牌申请请求消息递交给 SLA 授权模块继续处理，否则返回“授权用户不合法”的响应消息给第三方应用，终止授权过程；

SLA 授权模块，用于请求能力开放平台的 SLA 系统对第三方应用访问能力接口的合理性进行授权，如果第三方应用访问能力接口的频率符合预先签署的 SLA 合约，则 SLA 系统同意授权，否则 SLA 系统拒绝授权；

SLA 授权模块根据 SLA 系统的授权情况，如果 SLA 系统同意授权，则将令牌申请请求消息递交给令牌发放模块继续处理；否则返回“请求过于频繁”的响应消息给第三方应用，终止授权过程；

令牌发放模块，用于根据第三方应用的能力接口访问申请请求，生成一个唯一的涵盖计费、私有数据访问以及 SLA 授权的访问令牌发放给第三方应用，第三方应用携带访问令牌，以访问令牌作为能力访问授权凭证即可直接访问业务能力开放平台相应的能力接口；

令牌验证模块，用于第三方应用携带访问令牌，以访问令牌作为能力访问授权凭证访问业务能力开放平台相应的能力接口时，接收能力服务器发送的访问令牌，并验证其合法性，如果验证合法，业务能力开放平台的能力服务器执行相应的能力访问。

# 一种能力访问授权方法及系统

## 技术领域

[0001] 本发明属于互联网技术领域，更为具体地讲，涉及一种面向业务能力开放平台的能力访问授权方法。

## 背景技术

[0002] 随着移动通信带宽的大幅提高和移动终端的智能化，传统的移动或互联网业务已经不能满足移动终端用户多样化、个性化的需求。为了进一步促进移动互联网业务的繁荣，国内外著名的互联网公司和电信运营商都推出了自己的业务能力开放平台，例如 Google App、中国电信的“天翼空间应用工厂”等。这类业务能力开放平台将自己的业务能力封装成统一格式的 API 接口，向第三方应用开发者(包括企业开发者和个人开发者)提供，从而使移动互联网业务的开发、部署、推广更加便捷。

[0003] 业务能力开放平台提供的业务能力通常包括短信、语音、定位、手机支付等电信能力，搜索、微博、云存储等互联网能力，以及终端用户的私有数据和信息的访问能力等。

[0004] 目前，业务能力开放平台的能力访问授权方法处于逐步完善中，还没有综合提供授权管理的方法。例如中国电信的业务能力开放平台只提供第三方应用开发者授权计费的能力访问方式，即开发者必须预先购买相应的能力，第三方应用才能访问所订购的能力接口，还不能提供由终端用户授权计费的能力访问以及由用户授权的私有数据访问等授权管理功能。针对用户私有数据的访问授权，互联网开放平台通常采用基于 OAuth 协议的授权方法。该方法无需用户向第三方应用暴露自身的身份认证凭证(例如用户名 / 密码等)，即可完成用户对第三方应用在自身范围内数据访问的授权。但是 OAuth 授权协议主要针对使用第三方应用的终端用户需要访问自身私有数据的情况，没有考虑其他私有数据拥有者提供第三方应用授权访问的功能。此外，OAuth 授权协议也没有考虑能力访问的计费授权和 SLA 系统授权等功能。

## 发明内容

[0005] 本发明的目的在于克服现有技术的不足，提供一种完善、综合的面向业务能力开放平台的能力访问授权方法，对第三方应用访问业务能力开放平台提供的业务能力进行授权管理，从而确保业务能力开放平台的业务能力被合法的第三方应用进行合理的访问。

[0006] 为实现上述发明目的，本发明能力访问授权方法，其特征在于，包括以下步骤：

[0007] 步骤 1、第三方应用向业务能力开放平台的授权系统发送申请某个能力接口访问令牌的请求消息，请求消息至少包括：申请访问的能力接口的名称，能力访问的计费方，第三方应用标识符，授权用户的终端地址，授权用户的终端 MSISDN 号，需用户授权私有数据的列表，以及含有第三方应用密钥的签名等；

[0008] 步骤 2、业务能力开放平台的授权系统接收申请访问令牌的请求消息，然后进行：

[0009] 2.1)、验证访问令牌申请请求消息本身的合法性

[0010] 验证请求消息本身的合法性包括第三方应用的合法性、申请访问的能力接口的合

法性以及请求消息参数的合法性；

[0011] 其中，第三方应用的合法性由请求消息中携带的第三方应用标识符和含有第三方应用密钥的签名为基础进行验证；

[0012] 申请访问的能力接口的合法性由请求消息中携带的申请访问的能力接口的名称为基础进行验证；

[0013] 请求消息参数的合法性验证例如请求消息中所有携带参数的格式和范围是否符合规范；

[0014] 如果请求消息不合法，则授权系统返回“访问令牌申请不合法”的响应消息给第三方应用，终止授权过程，如果请求消息合法，则进行步骤 2.2；

[0015] 2.2)、计费授权与验证

[0016] 如果申请访问的能力接口是免费的，则直接执行步骤 2.3，否则根据请求消息中标识的计费方，计费方根据请求消息中携带的能力访问的计费方参数确定，向计费方发送计费授权的请求消息；

[0017] 计费方接收计费授权的请求消息，对申请的能力访问的计费进行授权，并将授权信息返回给授权系统；

[0018] 授权系统根据计费方返回的授权信息进行判断，如果计费方不同意授权，则返回“无计费方授权”的响应消息给第三方应用，终止授权过程；如果计费方同意授权，则要求能力开放平台的计费系统根据计费方式，验证计费方是否合法，如果计费方合法，则执行步骤 2.3，否则返回“计费方资费不够”或“信用度不够”的响应消息给第三方应用，终止授权过程；

[0019] 2.3)、私有数据访问授权与验证

[0020] 如果申请访问的能力接口不涉及私有数据，则直接执行步骤 2.4；否则发送私有数据访问授权的请求消息给私有数据的拥有者，如果该拥有者为在线状态，则其地址由请求消息中携带的授权用户的终端地址标识，如果该拥有者处于离线状态，则其地址由授权用户的终端 MSISDN 号标识；

[0021] 私有数据的拥有者收到私有数据访问授权的请求消息，对申请的私有数据，即以访问令牌请求消息中携带的需用户授权私有数据的列表中数据的访问进行授权，并将授权信息返回给授权系统；

[0022] 授权系统根据私有数据拥有者返回的授权信息进行判断，如果私有数据拥有者不同意授权，则返回“访问私有数据出错”的响应消息给第三方应用，终止授权过程；如果私有数据拥有者同意授权，则要求能力开放平台的认证系统验证私有数据拥有者，即授权用户是否合法，如果合法，则执行步骤 2.4，否则返回“授权用户不合法”的响应消息给第三方应用，终止授权过程；

[0023] 2.4)、SLA（Service Level Agreement）授权

[0024] 授权系统要求能力开放平台的 SLA（Service Level Agreement，服务等级协定）系统对第三方应用访问能力接口的合理性进行授权，如果第三方应用访问能力接口的频率符合预先签署的 SLA 合约，则 SLA 系统同意授权，否则 SLA 系统拒绝授权；

[0025] 授权系统根据 SLA 系统的授权情况，如果 SLA 系统同意授权，则执行步骤 3；否则返回“请求过于频繁”的响应消息给第三方应用，终止授权过程；

[0026] 步骤 3、访问令牌生成及发放

[0027] 授权系统根据第三方应用的能力接口访问申请请求，生成一个唯一的涵盖计费、私有数据访问以及 SLA 授权的访问令牌发放给第三方应用；

[0028] 步骤 4、能力接口访问

[0029] 第三方应用携带访问令牌，以访问令牌作为能力访问授权凭证可直接访问业务能力开放平台相应的能力接口，能力服务器执行相应的能力访问，并将能力访问结果返回给第三方应用，完成能力访问。

[0030] 此外，本发明还提供了一种能力访问授权系统，包括：

[0031] 令牌申请合法性验证模块，用于验证访问令牌申请本身请求消息的合法性，包括第三方应用的合法性、申请访问的能力接口的合法性以及请求消息参数的合法性；

[0032] 如果请求消息不合法，则授权系统返回“访问令牌申请不合法”的响应消息给第三方应用，终止授权过程，如果请求消息合法，则将令牌申请请求消息递交给计费授权模块继续处理；

[0033] 计费授权模块，用于向计费方发起授权请求，以及接收计费方返回的授权响应：

[0034] 如果申请访问的能力接口是免费的，则将令牌申请请求消息递交给私有数据访问授权模块继续处理，否则根据请求消息中标识的计费方，计费授权模块向计费方发送计费授权的请求消息；

[0035] 计费方收到计费授权的请求消息，对申请的能力访问的计费进行授权，并将授权信息返回给计费授权模块；

[0036] 计费授权模块根据计费方返回的授权信息进行判断，如果计费方不同意授权，则返回“无计费方授权”的响应消息给第三方应用，终止授权过程；如果计费方同意授权，则要求能力开放平台的计费系统根据计费方式验证计费方是否合法，如果计费方合法，则令牌申请请求消息递交给私有数据访问授权模块继续处理，否则返回“计费方资费不够”或“信用度不够”的响应消息给第三方应用，终止授权过程；

[0037] 私有数据访问授权模块，用于向私有数据拥有者发起授权请求，以及接收资源拥有者返回的授权响应：

[0038] 如果申请访问的能力接口不涉及私有数据，则将令牌申请请求消息递交给 SLA 授权模块继续处理；否则发送私有数据访问授权的请求消息给私有数据的拥有者；

[0039] 私有数据的拥有者收到私有数据访问授权的请求消息，对申请的私有数据访问进行授权，并将授权信息返回给私有数据访问授权模块；

[0040] 私有数据访问授权模块根据私有数据拥有者返回的授权信息进行判断，如果私有数据拥有者不同意授权，否则返回“访问私有数据出错”的响应消息给第三方应用，终止授权过程；如果私有数据拥有者同意授权，则要求能力开放平台的认证系统验证私有数据拥有者是否合法，如果合法，则将令牌申请请求消息递交给 SLA 授权模块继续处理，否则返回“授权用户不合法”的响应消息给第三方应用，终止授权过程；

[0041] SLA 授权模块，用于请求能力开放平台的 SLA 系统对第三方应用访问能力接口的合理性进行授权，如果第三方应用访问能力接口的频率符合预先签署的 SLA 合约，则 SLA 系统同意授权，否则 SLA 系统拒绝授权；

[0042] SLA 授权模块根据 SLA 系统的授权情况，如果 SLA 系统同意授权，则将令牌申请请

求消息递交给令牌发放模块继续处理；否则返回“请求过于频繁”的响应消息给第三方应用，终止授权过程；

[0043] 令牌发放模块，用于根据第三方应用的能力接口访问申请请求，生成一个唯一的涵盖计费、私有数据访问以及 SLA 授权的访问令牌发放给第三方应用，第三方应用携带访问令牌，以访问令牌作为能力访问授权凭证即可直接访问业务能力开放平台相应的能力接口；

[0044] 令牌验证模块，用于第三方应用携带访问令牌，以访问令牌作为能力访问授权凭证访问业务能力开放平台相应的能力接口时，接收能力服务器发送的访问令牌，并验证其合法性，如果验证合法，业务能力开放平台的能力服务器执行相应的能力访问。

[0045] 本发明的目的是这样实现的：

[0046] 本发明能力访问授权方法是针对业务能力开放平台的授权进行管理，主要涉及以下内容：

[0047] (1) 第三方应用在访问业务能力时，需要获得业务计费方的显示授权，例如终端用户或者应用提供者是否允许以自己的账户作为本次能力访问的计费账户；

[0048] (2) 第三方应用访问与终端用户私有数据相关的业务能力(如获取用户信息、使用用户资源等)时，为保证终端用户数据的安全性、隐私性，需要获得该私有数据拥有者的显示授权，例如是否允许第三方应用获取终端用户的位置信息，是否允许第三方应用以终端用户的名义发送呼叫或者发送短信等；

[0049] (3) 出于能力接口的可控性考虑，保证能力接口的合理利用、数据访问权限的多粒度控制等，第三方应用在访问业务能力时，还需要获得能力开放平台服务等级协定(Service Level Agreement，SLA)系统的授权；

[0050] 在获得多方授权以后，由授权系统生成相应的访问令牌，发放给第三方应用，第三方应用携带访问令牌，以访问令牌作为能力访问授权凭证即可直接访问对应的能力接口，从而确保业务能力开放平台的业务能力被合法的第三方应用进行合理的访问。

## 附图说明

[0051] 图 1 是本发明能力访问授权方法的流程图；

[0052] 图 2 是本发明能力访问授权方法中各系统部署图；

[0053] 图 3 是本发明能力访问授权方法一具体实施方式的流程图；

[0054] 图 4 是本发明能力访问授权方法中访问令牌申请请求合法性判断方法一种具体实施方式流程图；

[0055] 图 5 是本发明能力访问授权方法中以访问令牌作为能力访问授权凭证的进行能力访问一种具体实施方式流程图；

[0056] 图 6 是本发明能力访问授权方法中授权系统的原理框图。

## 具体实施方式

[0057] 下面结合附图对本发明的具体实施方式进行描述，以便本领域的技术人员更好地理解本发明。需要特别提醒注意的是，在以下的描述中，当已知功能和设计的详细描述也许会淡化本发明的主要内容时，这些描述在这里将被忽略。

[0058] 图 1 是本发明能力访问授权方法的流程图。

[0059] 如图 1 所示，本发明能力访问授权方法包括：

[0060] 步骤 1：第三方应用发送申请访问令牌的请求消息；

[0061] 步骤 2：业务能力开放平台的授权系统接收申请访问令牌的请求消息，然后进行请求消息验证与能力访问的授权：

[0062] 步骤 2.1 验证申请请求消息的合法性；

[0063] 步骤 2.2 进行计费授权和验证；

[0064] 步骤 2.3：进行私有数据访问授权与验证；

[0065] 步骤 2.4：SLA 授权

[0066] 步骤 3：生成访问令牌并发放给第三方应用，第三方应用以此为授权凭证访问相应的能力接口。

[0067] 图 2 是本发明能力访问授权方法中各系统部署图。

[0068] 各系统在业务能力开放平台内部实现，其部署示意图如图 2 所示。

[0069] 首先，对本发明中所涉及的角色及其功能进行说明。本发明中涉及的角色包括：第三方应用、终端用户、计费方、私有数据拥有者、授权系统、认证系统、计费系统、SLA 系统、能力服务器。其中，第三方应用是基于开放平台提供的能力接口开发的程序与软件，第三方应用既可以是有后台服务器的应用，也可以是无后台服务器的桌面应用；终端用户是正在使用第三方应用的人；计费方为本次能力访问支付费用，既可以是使用第三方应用的终端用户，也可以是第三方应用的提供者，后者主要针对有后台服务器应用的情况；私有数据拥有者既可以是正在使用第三方应用的终端用户，也可以是其他开放平台用户；授权系统完成第三方应用访问能力接口的授权管理功能；认证系统完成对开放平台用户的认证功能；计费系统完成对开放平台用户的计费功能；SLA 系统判断第三方应用访问能力接口的频率是否符合预先签署的 SLA 合约；能力服务器通过能力接口，提供短信、语音、定位、微博、云存储等能力访问服务。

[0070] 图 3 是本发明能力访问授权方法一具体实施方式的流程图。

[0071] 在本实施例中，如图 3 所示，本发明能力访问授权方法具体步骤如下：

[0072] 步骤 101：第三方应用向能力开放平台的授权系统发送申请某个能力接口访问令牌的请求消息，所述请求消息包括：申请访问的能力接口的名称，能力访问的计费方，第三方应用标识符，授权用户的终端地址，授权用户的终端 MSISDN 号，用户授权列表，以及含有第三方应用密钥的签名。

[0073] 步骤 102：授权系统接收请求消息，验证访问令牌申请请求本身的合法性，包括第三方应用的合法性，申请访问能力接口的合法性，以及请求消息参数的合法性；如果请求消息合法，则执行步骤 104，否则执行步骤 103；

[0074] 步骤 103：授权系统返回“访问令牌申请不合法”的响应消息给第三方应用，终止授权过程；

[0075] 步骤 104：授权系统判断申请访问的能力接口是否免费，如果是免费的，则直接执行步骤 114，否则执行步骤 105；

[0076] 步骤 105：授权系统根据请求消息中标识的计费方，向计费方发送计费授权的请求消息，在实施例中，计费方可以是第三方应用的提供者、也可以是使用第三方应用的终端

用户；

[0077] 步骤 106：计费方收到计费授权的请求消息，计费方对本次能力访问的计费进行授权，并将授权信息返回给授权系统；

[0078] 步骤 107：授权系统判断计费方是否同意计费授权，如果同意，则执行步骤 109，否则执行步骤 108；

[0079] 步骤 108：授权系统返回“无计费方授权”的响应消息给第三方应用，终止授权过程；

[0080] 步骤 109：授权系统请求能力开放平台的计费系统验证计费授权是否合法；

[0081] 步骤 110：计费系统根据计费方采用的计费方式验证计费授权的合法性：在本实施例中，计费方式分为预付费方式和后付费方式两种，如果是预付费方式，判断计费方是否有余额支持本次访问；如果是后付费方式，判断计费方的信用度是否有问题；

[0082] 步骤 111：计费系统将本次计费授权的验证结果返回给授权系统；

[0083] 步骤 112：授权系统根据验证结果，如果本次计费授权合法，则执行步骤 114，否则执行步骤 113；

[0084] 步骤 113：授权系统返回“计费方资费不够”或“信用度不够”的响应消息给第三方应用，终止授权过程；

[0085] 步骤 114：授权系统判断申请访问的能力接口是否涉及终端用户的私有数据，如果涉及，则执行步骤 115，否则直接执行步骤 124；

[0086] 步骤 115：授权系统发送数据访问授权的请求消息给私有数据的拥有者，在本实施例中，即私有数据访问的终端用户，该请求消息携带有本次能力访问需用户授权私有数据的列表；

[0087] 步骤 116：私有数据拥有者对申请访问的私有数据进行授权，并将自己的认证凭证及授权信息返回给授权系统；

[0088] 步骤 117：授权系统判断私有数据拥有者是否同意授权，如果同意，则执行步骤 119，否则执行步骤 118；

[0089] 步骤 118：授权系统返回“访问私有数据出错”的响应消息给第三方应用，终止授权过程；

[0090] 步骤 119：授权系统请求能力开放平台的认证系统验证私有数据拥有者，即授权用户是否合法；

[0091] 步骤 120：认证系统根据授权用户提交的认证凭证对其合法性进行验证；

[0092] 步骤 121：认证系统将授权用户合法性的验证结果返回给授权系统；

[0093] 步骤 122：授权系统根据验证结果，如果授权用户合法，则执行步骤 124，否则执行步骤 123；

[0094] 步骤 123：授权系统返回“授权用户不合法”的响应消息给第三方应用，终止授权过程；

[0095] 步骤 124：授权系统请求能力开放平台的 SLA 系统对第三方应用访问能力接口的合理性进行授权；

[0096] 步骤 125：SLA 系统判断第三方应用访问能力接口的频率是否符合预先签署的 SLA 合约，如果符合则 SLA 系统同意授权，否则 SLA 系统拒绝授权；

[0097] 步骤 126 :SLA 系统将 SLA 授权结果返回给授权系统 ;

[0098] 步骤 127 :授权系统根据 SLA 系统的授权情况,如果 SLA 系统同意授权,则执行步骤 129,否则执行步骤 128 ;

[0099] 步骤 128 :授权系统返回“请求过于频繁”的响应消息给第三方应用,终止授权过程 ;

[0100] 步骤 129 :授权系统生成一个唯一的访问令牌,生成一个唯一的涵盖计费、私有数据访问以及 SLA 授权的访问令牌发放给第三方应用,第三方应用携带访问令牌,以访问令牌作为能力访问授权凭证即可直接访问业务能力开放平台相应的能力接口。

[0101] 图 4 是本发明能力访问授权方法中访问令牌申请请求合法性判断方法一种具体实施方式流程图。

[0102] 在本实施例中,如图 4 所示,访问令牌申请请求本身的合法性判断步骤如下 :

[0103] 步骤 201 :授权系统判断申请令牌的第三方应用是否合法,包括开发者的状态是否正常、第三方应用的状态是否正常、第三方应用是否与请求携带的第三方应用标识符一致 ;如果合法,则执行步骤 203 ;否则执行步骤 202 ;

[0104] 步骤 202 :返回“访问令牌申请不合法”的响应消息给第三方应用,终止授权过程 ;

[0105] 步骤 203 :授权系统判断申请访问的能力接口是否合法,即判断申请访问的能力接口是否在该第三方应用允许访问的接口范围内 ;如果合法,则执行步骤 204 ;否则执行步骤 202 ;

[0106] 步骤 204 :授权系统判断请求消息中携带的参数是否合法,如果合法,则完成访问令牌请求本身的合法性检查 ;否则执行步骤 202。

[0107] 图 5 是本发明能力访问授权方法中以访问令牌作为能力访问授权凭证的进行能力访问一种具体实施方式流程图。

[0108] 在本实施例中,如图 5 所示,以访问令牌作为能力访问授权凭证的进行能力访问方法,包括步骤如下 :

[0109] 步骤 301 :第三方应用接收授权系统返回的能力接口访问令牌,然后向业务能力开放平台的能力服务器发送能力接口访问的请求消息,所述请求消息包括访问的能力接口的名称、属性参数及对应接口的访问令牌 ;

[0110] 步骤 302 :能力服务器接收访问请求,检验属性参数的合法性,如果参数不合法,则执行步骤 303,否则执行步骤 304 ;

[0111] 步骤 303 :能力服务器返回“属性参数不合法”的响应消息给第三方应用,终止执行所述能力访问过程 ;

[0112] 步骤 304 :能力服务器请求业务能力开放平台的授权系统对收到的访问令牌进行验证 ;

[0113] 步骤 305 :授权系统验证访问令牌的有效性 ;

[0114] 步骤 306 :授权系统返回访问令牌有效性验证结果给能力服务器 ;

[0115] 步骤 307 :能力服务器接收验证结果,如果访问令牌有效,则执行步骤 309 ;否则执行步骤 308 ;

[0116] 步骤 308 :能力服务器返回“访问令牌失效”的响应消息给第三方应用,终止执行所述能力访问过程 ;

[0117] 步骤 309 :能力服务器相应的能力接口执行能力访问 ;

[0118] 步骤 310 :能力服务器将能力访问结果返回给第三方应用,完成能力访问。

[0119] 图 6 是本发明能力访问授权方法中授权系统的原理框图。

[0120] 在本实施例中,如图 6 所示,能力访问授权系统包括令牌申请合法性验证模块 401、计费授权模块 402、私有数据访问授权模块 403、SLA 授权模块 404、访问令牌发放模块 405、访问令牌验证模块 406。

[0121] 令牌申请合法性验证模块 401,用于验证请求消息本身的合法性,包括验证第三方应用的合法性,申请访问能力接口的合法性,以及请求消息参数的合法性。如果请求消息合法,则将令牌请求消息递交给计费授权模块继续处理 ;否则,请求消息不合法,令牌申请合法性验证模块直接返回“访问令牌申请不合法”的响应消息给第三方应用,终止授权过程。

[0122] 计费授权模块 402,用于完成能力访问的计费授权功能,主要包括 :首先分析申请访问的能力接口是否免费,如果是免费的,则直接执行后续的私有数据访问授权过程 ;否则根据令牌请求消息携带的参数分析本次能力访问的计费方,向计费方发起授权请求,并接收计费方返回的授权响应 :如果计费方不同意授权,则计费授权模块返回“无计费方授权”的响应消息给第三方应用,终止授权过程 ;如果计费方同意授权,则计费授权模块请求能力开放平台的计费系统验证本次计费授权是否合法,如果计费授权合法,则继续执行后续的私有数据访问授权过程 ;如果计费授权不合法,则返回“计费方资费不够”或“信用度不够”的响应消息给第三方应用,终止授权过程。

[0123] 私有数据访问授权模块 403,用于完成私有数据访问的授权功能,主要包括 :首先分析申请访问的能力接口是否涉及终端用户私有数据,如果不涉及,则直接执行后续的 SLA 授权过程 ;否则发送数据访问授权的请求消息给私有数据的拥有者,如果私有数据拥有者不同意授权,则返回“访问私有数据出错”的响应消息给第三方应用,终止授权过程 ;如果同意授权,则要求能力开放平台的认证系统验证授权用户是否合法,如果合法,则继续执行后续的 SLA 授权过程 ;否则返回“授权用户不合法”的响应消息给第三方应用,终止授权过程。

[0124] SLA 授权模块 404,用于请求能力开放平台的 SLA 系统对第三方应用访问能力接口的频率是否符合预先签署的 SLA 合约进行授权,以及接收 SLA 系统返回的授权响应。

[0125] 令牌发放模块 405,用于在申请合法且获得各方授权的情况下,产生一个新的全局唯一的访问令牌发送给第三方应用。

[0126] 访问令牌验证模块 406,用于第三方应用携带访问令牌,以访问令牌作为能力访问授权凭证访问业务能力开放平台相应的能力接口时,接收能力服务器发送访问令牌,并验证其合法性,如果验证合法,业务能力开放平台的能力服务器执行相应的能力访问。

[0127] 实例

[0128] 本发明提供一个具体的定位服务 (Location Based Service, LBS) 的能力访问实例。

[0129] 假设第三方应用需要访问能力开放平台提供的 LBS 能力,以获取终端用户当前的地理位置信息。假设该 LBS 能力由第三方应用购买并作为每次能力访问的计费方。此外,获取终端用户的地理位置信息属于该终端用户的私有数据,因此需要向终端用户进行私有数据访问授权。综上分析,能力开放平台的授权系统在向第三方应用发放 LBS 能力访问授权凭证前,首先要完成付费方授权、用户私有数据访问授权以及 SLA 授权三个过程,具体实

施步骤如下：

[0130] 步骤 501：第三方应用向能力开放平台的授权系统发送申请 LBS 能力接口访问令牌的请求消息，请求包含如下参数：申请访问的能力接口的名称 (api_name)，能力访问的计费方 (pay_account)，第三方应用标识符 (app_key)，终端用户的 IP 地址 (ip_client)，终端用户的 MSISDN 号 (msisdn)，地理位置信息的列表 (list)，以及含有第三方应用密钥的签名 (md5)。在本实施例中，具体参数如表 1 所示的访问令牌请求消息中携带的参数说明。

[0131]

| 参数名 | 设置值 | 说明 |
|---|---|---|
| api_name | LBS_BY_MSISDN | 请求访问的能力是 LBS 能力，该接口可反馈给访问者所提供手机号对应的用户终端的地理位置信息 |
| pay_ account | APP_KEY | 本次能力调用的付费方是第三方应用 |
| app_key | APP_KEY | 本应用在能力开放平台注册时获得的标示符为 APP_KEY，获得的密码为 APP_SECRET |

[0132]

| | | |
|---|---|---|
| ip_client | IP_CLIENT | 终端用户的 IP 地址，用于在线授权时，向用户发起授权请求，本实施例中假设为 202.38.75.11 |
| msisdn | MSISDN | 终端用户的 MSISDN 号，用于离线授权时，向用户发起授权请求，本实施例中假设为 13438865081 |
| list | AUTH_LBS | 请求用户对访问其 MSISDN 号对应的地理位置信息进行授权 |
| md5 | MD5_HASH | 应用把请求消息中携带的参数进行拼接，并在结尾处附加该应用在能力平台注册时获得的 APP_SECRET，形成字符串，然后将所生成的字符串使用 MD5 算法进行 hash，MD5_HASH 即为该字符串的 hash 值 |

[0133] 步骤 502：授权系统接收申请请求消息，验证访问令牌申请请求消息本身的合法性，具体包括第三方应用的合法性，申请访问能力接口的合法性，以及请求消息参数的合法性等；如果请求消息合法，则执行步骤 503，否则授权系统返回“访问令牌申请不合法”的响应消息给第三方应用，终止授权过程；

[0134] 步骤 503：授权系统判断申请访问的能力接口 LBS_BY_MSISDN 是由第三方应用作为计费方，因此向第三方应用发起计费授权请求；

[0135] 步骤 504：第三方应用对本次能力访问的计费进行授权(提供本应用的 APP_KEY 和 APP_SECRET，以及同意计费授权的信息)，并将授权信息返回给授权系统；

[0136] 步骤 505：授权系统判断第三方应用是否同意计费授权，如果同意，则请求能力开

放平台的计费系统验证计费授权是否合法；否则，授权系统返回“无计费方授权”的响应消息给第三方应用，终止授权过程；

[0137] 步骤 506：计费系统根据第三方应用订购能力时签订的计费方式验证计费授权的合法性，假设本实施例中的计费方式为预付费方式，则计费系统判断第三方应用是否有足够的余额支持本次访问，并将本次计费授权的验证结果返回给授权系统；

[0138] 步骤 507：授权系统根据验证结果，如果本次计费授权合法，则执行步骤 508；否则，返回“计费方资费不够”的响应消息给第三方应用，终止授权过程；

[0139] 步骤 508：授权系统判断申请访问的 LBS_BY_MSISDN 能力接口，需要终端用户对其私有数据访问进行授权，因此向用户终端发送私有数据访问的授权请求消息（可通过 IP_CLIENT 信息进行在线授权，也可通过 MSISDN 号进行短信方式授权），该请求消息携带有本次能力访问需用户授权的列表 list；

[0140] 步骤 509：终端用户对本次 LBS 能力访问授权（即允许第三方应用通过 MSISDN 号查找终端对应的地理位置信息），并将自己的认证凭证及授权信息返回给授权系统；

[0141] 步骤 510：授权系统判断终端用户是否同意授权，如果同意，则执行步骤 511，否则授权系统返回“访问私有数据出错”的响应消息给第三方应用，终止授权过程；

[0142] 步骤 511：授权系统请求能力开放平台的认证系统验证授权的终端用户是否合法；

[0143] 步骤 512：认证系统根据授权用户提交的凭证对其合法性进行验证；

[0144] 步骤 513：认证系统将授权用户合法性的验证结果返回给授权系统；

[0145] 步骤 514：授权系统根据验证结果，如果授权用户合法，则执行步骤 515，否则授权系统返回“授权用户不合法”的响应消息给第三方应用，终止授权过程；

[0146] 步骤 515：授权系统请求能力开放平台的 SLA 系统对第三方应用访问能力接口的合理性进行授权；

[0147] 步骤 516：SLA 系统判断第三方应用访问能力接口的频率是否符合预先签署的 SLA 合约，如果符合则 SLA 系统同意授权，否则 SLA 系统拒绝授权；

[0148] 步骤 517：SLA 系统将 SLA 授权结果返回给授权系统；

[0149] 步骤 518：授权系统根据 SLA 系统的授权情况，如果 SLA 系统同意授权，则执行步骤 519，否则授权系统返回“请求过于频繁”的响应消息给第三方应用，终止授权过程；

[0150] 步骤 519：授权系统生成一个唯一的访问令牌，发送给第三方应用，完成本次 LBS 能力访问的授权。

[0151] 尽管上面对本发明说明性的具体实施方式进行了描述，以便于本技术领的技术人员理解本发明，但应该清楚，本发明不限于具体实施方式的范围，对本技术领域的普通技术人员来讲，只要各种变化在所附的权利要求限定和确定的本发明的精神和范围内，这些变化是显而易见的，一切利用本发明构思的发明创造均在保护之列。

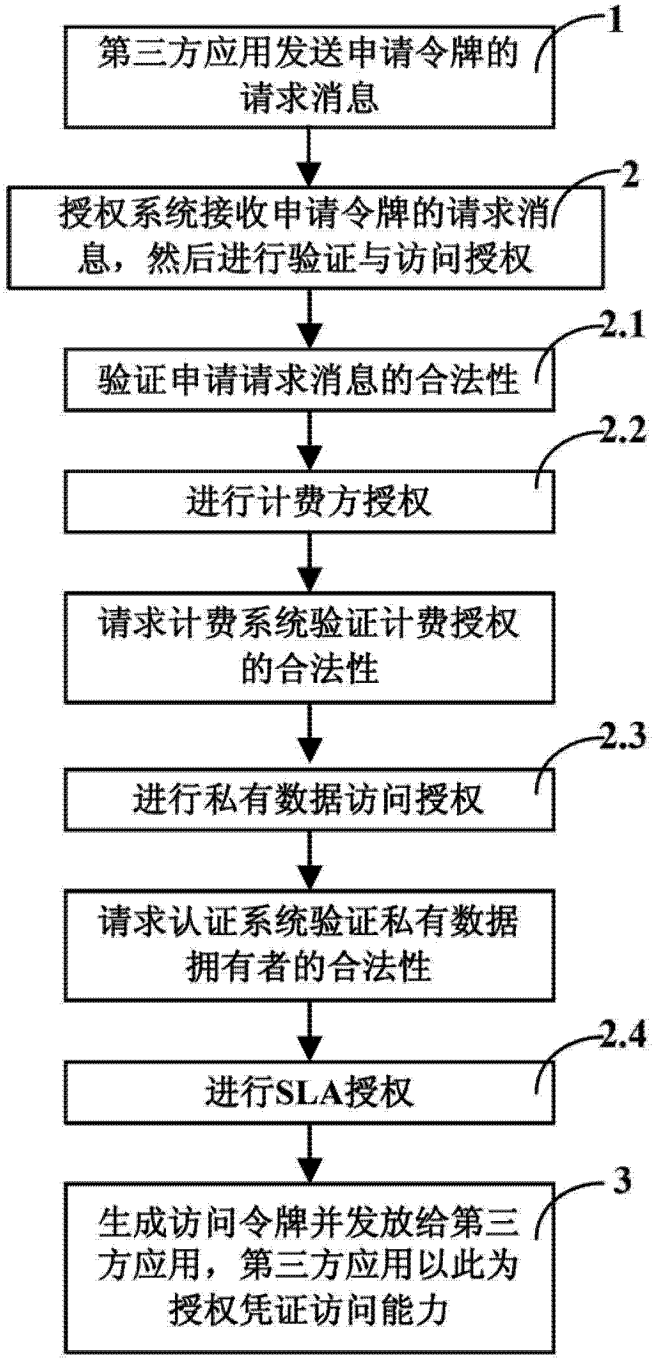

第三方应用发送申请令牌的请求消息
1
授权系统接收申请令牌的请求消息，然后进行验证与访问授权
2
验证申请请求消息的合法性
2.1
进行计费方授权
2.2
请求计费系统验证计费授权的合法性
进行私有数据访问授权
2.3
请求认证系统验证私有数据拥有者的合法性
进行SLA授权
2.4
生成访问令牌并发放给第三方应用，第三方应用以此为授权凭证访问能力
3

图 1

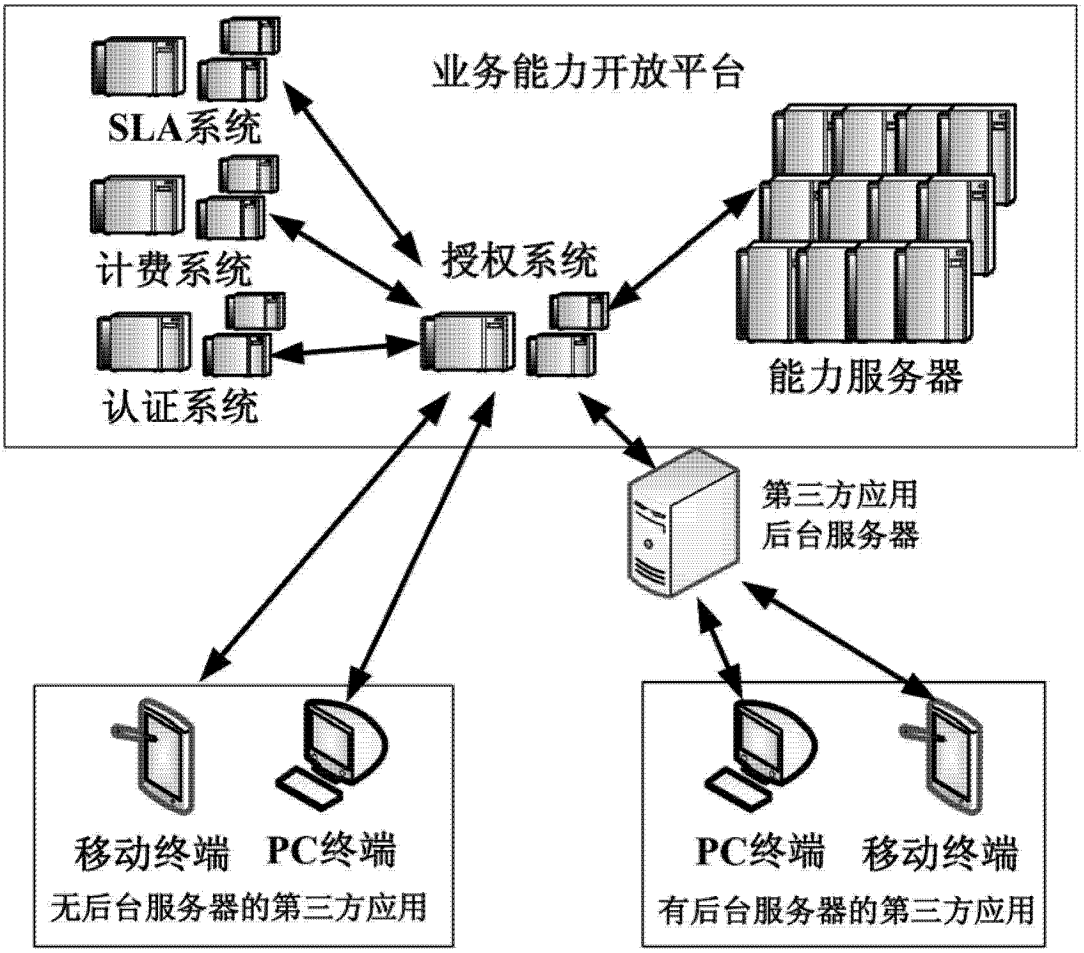

业务能力开放平台
SLA系统
计费系统
认证系统
授权系统
能力服务器
第三方应用
后台服务器
移动终端
PC终端
无后台服务器的第三方应用
PC终端
移动终端
有后台服务器的第三方应用

图 2

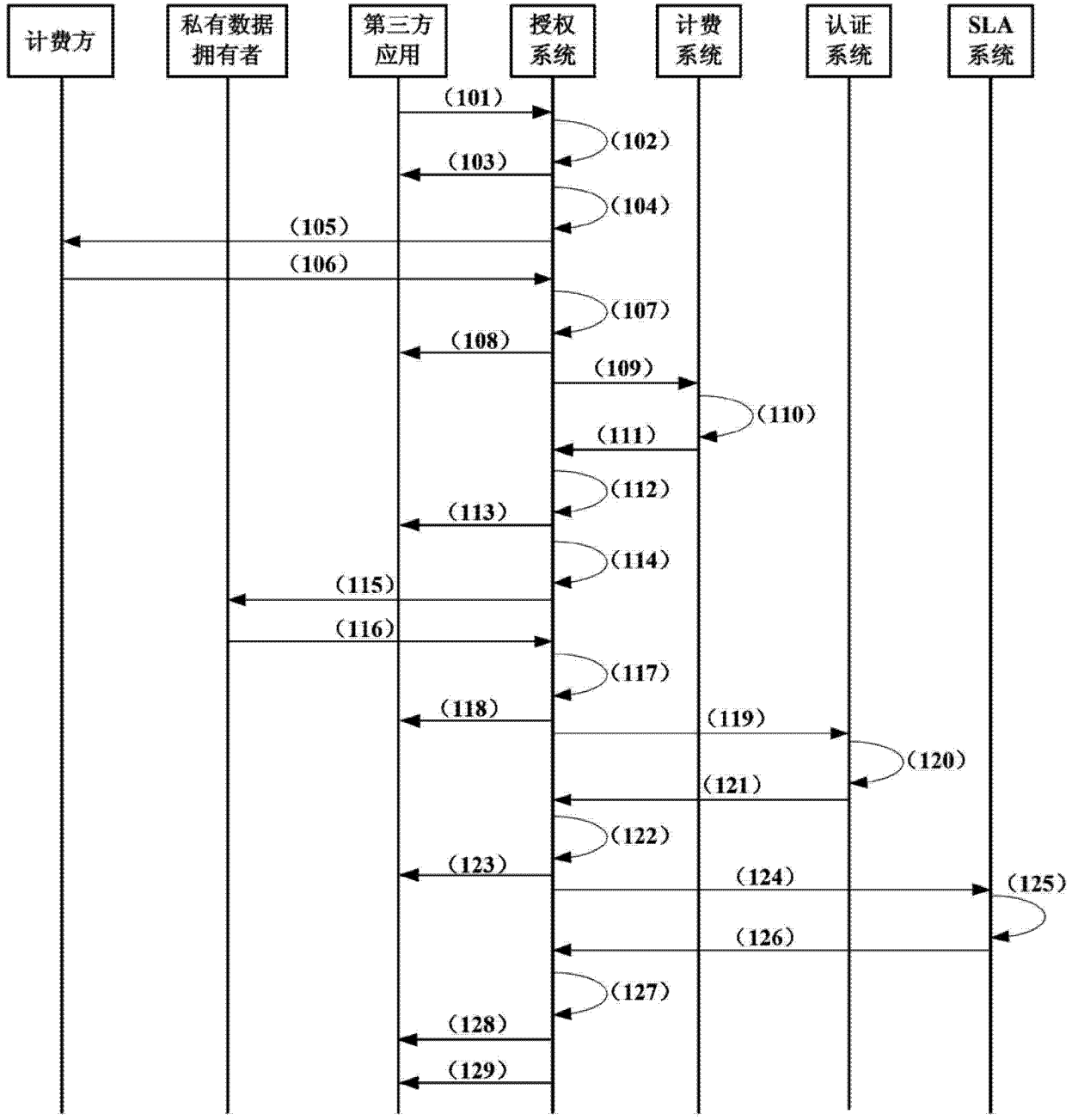

计费方
私有数据拥有者
第三方应用
授权系统
计费系统
认证系统
SLA系统
(101)
(102)
(103)
(104)
(105)
(106)
(107)
(108)
(109)
(110)
(111)
(112)
(113)
(114)
(115)
(116)
(117)
(118)
(119)
(120)
(121)
(122)
(123)
(124)
(125)
(126)
(127)
(128)
(129)

图 3

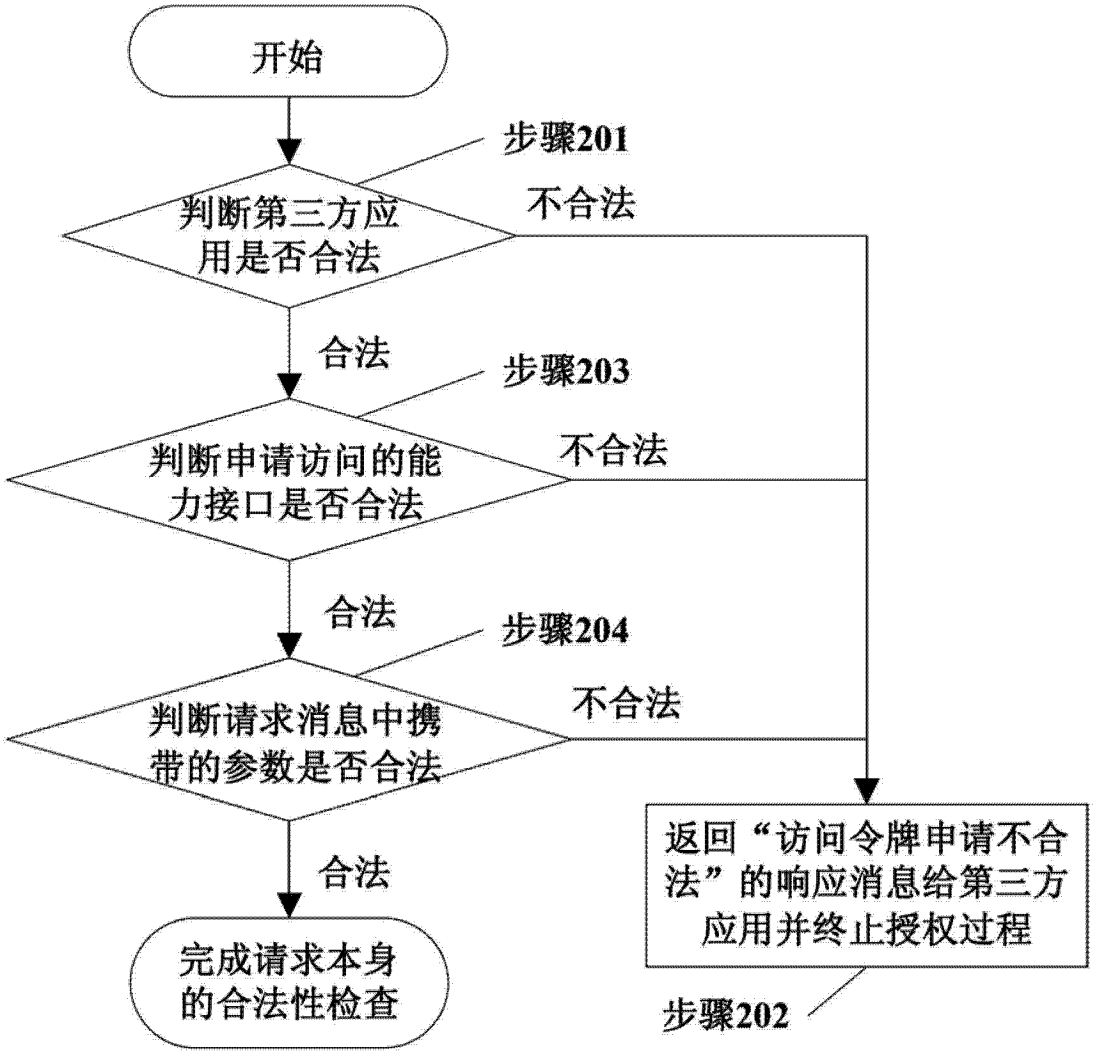

开始
步骤201
判断第三方应用是否合法
不合法
合法
步骤203
判断申请访问的能力接口是否合法
不合法
合法
步骤204
判断请求消息中携带的参数是否合法
不合法
合法
返回“访问令牌申请不合法”的响应消息给第三方应用并终止授权过程
步骤202
完成请求本身的合法性检查

图 4

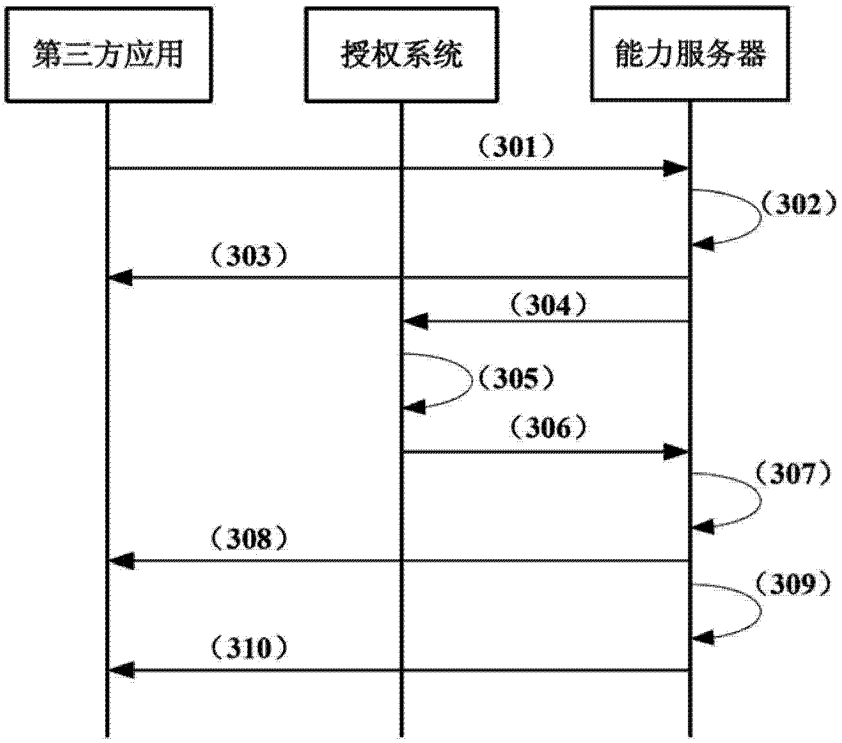

第三方应用
授权系统
能力服务器
(301)
(302)
(303)
(304)
(305)
(306)
(307)
(308)
(309)
(310)

图 5

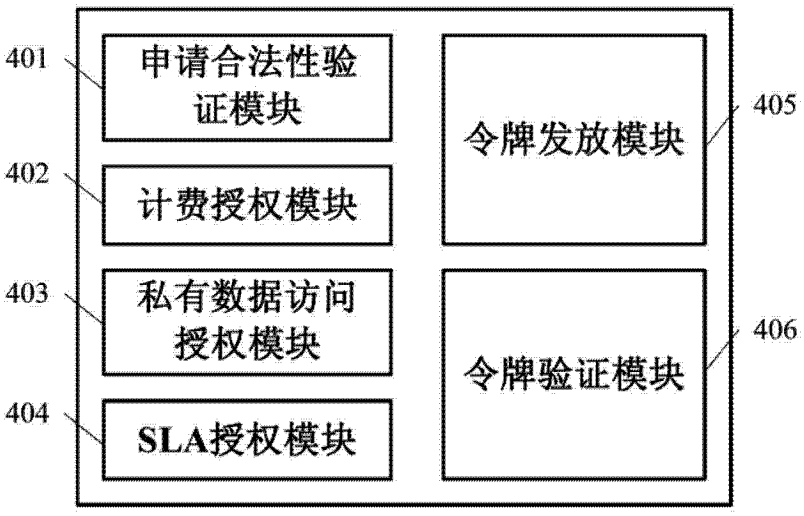

401
申请合法性验证模块
402
计费授权模块
403
私有数据访问授权模块
404
SLA授权模块
令牌发放模块
405
令牌验证模块
406

图 6