



(12)发明专利申请

(10)申请公布号 CN 111147572 A  
(43)申请公布日 2020.05.12

(21)申请号 201911346649.8

(22)申请日 2019.12.24

(71)申请人 中国建设银行股份有限公司  
地址 100033 北京市西城区金融大街25号  
申请人 建信金融科技有限责任公司

(72)发明人 邹斯韬 汪博 罗韬 邵小亮  
陈飞 汪平

(74)专利代理机构 北京三友知识产权代理有限公司 11127  
代理人 赵平 周永君

(51)Int.Cl.  
H04L 29/08(2006.01)  
H04L 29/06(2006.01)

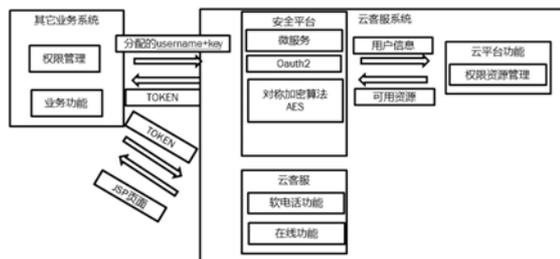
权利要求书2页 说明书12页 附图7页

(54)发明名称

云客服平台管理系统及方法

(57)摘要

一种云客服平台管理系统,包含:安全平台根据业务系统的身份信息生成访问令牌;将业务系统提供的权限信息与访问令牌绑定后存储至存储至编号资源对应表;根据业务系统提供的访问令牌查询对应的权限信息,根据权限信息验证业务系统提供的控制指令的权限;当验证通过后,通过资源管理模块获得控制指令对应的控制接口并反馈至业务系统;资源管理模块内预存多个不同业务功能组件,根据业务功能组件生成权限清单并提供至安全平台调用,根据控制指令获得对应的业务功能组件的控制接口;业务系统根据权限清单和用户勾选项生成权限信息;通过访问令牌和控制指令于云客服系统获得对应的业务功能组件的控制接口,通过控制接口操作对应的业务功能组件。



1. 一种云客服平台管理系统,其特征在于,所述系统包含:云客服系统和业务系统;  
所述云客服系统包含安全平台和资源管理模块;

所述安全平台用于根据所述业务系统的身份信息生成访问令牌,将所述访问令牌与权限清单提供给业务系统;将业务系统提供的权限信息与所述访问令牌绑定后存储至存储至编号资源对应表;以及,根据业务系统提供的访问令牌查询对应的权限信息,根据所述权限信息验证业务系统提供的控制指令的权限;当验证通过后,通过资源管理模块获得所述控制指令对应的控制接口并反馈至所述业务系统;

所述资源管理模块内预存多个不同业务功能组件,用于根据所述业务功能组件生成权限清单并提供至所述安全平台调用;以及,根据所述控制指令获得对应的所述业务功能组件的控制接口;

所述业务系统用于根据权限清单和用户勾选项生成权限信息并提供至云客服系统;以及,通过所述访问令牌和控制指令于所述云客服系统获得对应的业务功能组件的控制接口;通过控制接口操作对应的所述业务功能组件。

2. 根据权利要求1所述的云客服平台管理系统,其特征在于,所述安全平台还包含权限管理模块,所述权限管理模块用于接收用户请求信息和权限信息,根据所述用户请求信息生成用户编号;将所述用户编号与对应的权限信息关联后存储至编号资源对应表;以及,接收用户的访问请求,根据所述访问请求中的用户编号于所述编号资源对应表中获得对应的权限信息,根据所述权限信息和所述访问请求中的控制指令对所述资源管理模块内对应业务功能组件执行预定操作。

3. 根据权利要求1所述的云客服平台管理系统,其特征在于,所述业务系统还包含权限分配模块,所述权限分配模块用于获取所述业务系统使用者的用户信息,根据所述用户信息于所述权限信息内分配对应的用户权限;将所述用户权限和所述用户信息关联后通过所述访问令牌发送至所述安全平台;所述安全平台根据所述用户权限和所述用户信息生成用户角色对应表,将所述访问令牌和所述用户角色对应表关联后存储至对应的所述编号资源对应表。

4. 根据权利要求1所述的云客服平台管理系统,其特征在于,所述云客服系统还包含客服功能模块,所述客服功能模块的操作界面存储于所述资源管理模块中;所述资源管理模块根据所述控制指令调取所述操作界面,并将所述操作界面通过所述安全平台提供给所述业务系统;所述业务系统将所述操作界面展示。

5. 根据权利要求1至4中任一项所述的云客服平台管理系统,其特征在于,所述安全平台还包含权限验证模块,所述权限验证模块用以将所述控制指令所涉及的业务功能组件范围与所述权限信息中所涉及的业务功能组件范围相比较,当所述控制指令所涉及的业务功能组件范围处于所述权限信息中所涉及的业务功能组件范围时,将所述控制指令输出至所述资源管理模块。

6. 一种云客服平台管理方法,其特征在于,所述方法包含:

根据预存的多个不同业务功能组件生成权限清单;

根据所述业务系统的身份信息生成访问令牌,将所述访问令牌与权限清单提供给业务系统;

将业务系统提供的权限信息与所述访问令牌绑定后存储至存储至编号资源对应表;

根据业务系统提供的访问令牌查询对应的权限信息,根据所述权限信息验证业务系统提供的控制指令的权限;

当验证通过后,通过资源管理模块获得所述控制指令对应的控制接口并反馈至所述业务系统。

7.根据权利要求6所述的云客服平台管理方法,其特征在于,根据所述权限信息和所述控制报文中的控制指令获得对应的所述业务功能组件的控制接口包含:

将所述控制指令所涉及的业务功能组件范围与所述权限信息中所涉及的业务功能组件范围相比较;

当所述控制指令所涉及的业务功能组件范围处于所述权限信息中所涉及的业务功能组件范围时,获得所述控制指令对应的所述业务功能组件的控制接口。

8.一种云客服平台管理方法,其特征在于,所述方法包含:

根据业务系统的身份标识生成请求指令,通过请求指令获得云客服系统反馈的访问令牌和权限清单;

根据权限清单和用户勾选项生成权限信息并提供至云客服系统;

通过所述访问令牌和控制指令于所述云客服系统获得对应的业务功能组件的控制接口;

通过控制接口操作对应的所述业务功能组件。

9.一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求6至8任一所述方法。

10.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质存储有执行权利要求6至8任一所述方法的计算机程序。

## 云客服平台管理系统及方法

### 技术领域

[0001] 本发明涉及云端数据处理领域,尤指一种云客服平台管理系统及方法。

### 背景技术

[0002] 随着社会各个企业发展越来越迅速,客服服务渠道的建设对于各个企业来说已经迫在眉睫,但是各个企业的需求不一样,并且各个企业本身有自身的自建系统。如何能把自身的自建系统与电话在线客服系统融合在一起,为各个企业的自建系统提供电话和在线服务渠道成了目前需要解决的一个问题,该专利为解决这些问题提供一套解决方案。

[0003] 随着建行云客服项目的建设日趋成熟,来谈判的企业租户越来越多。但是各个企业都有自己的业务系统,有的企业不愿意放弃自身本身在用的业务系统,但是又想在现有的业务系统的基础上增加电话,在线的能力;目前市场上的企业级系统都是自成一套体系,系统与系统之间的对接缺乏模块化分拆机制。

### 发明内容

[0004] 本发明目的在于解决上述问题,提供一种云客服平台管理系统及方法,以安全组件为接入认证基础,以云平台的权限资源管理为业务系统用户控制依据,根据不同业务系统不同的需求以及不同的权限,赋予业务系统不同的能力。

[0005] 为达上述目的,本发明所提供的云客服平台管理系统具体包含云客服系统和业务系统;所述云客服系统包含安全平台和资源管理模块;所述安全平台用于根据所述业务系统的身份信息生成访问令牌,将所述访问令牌与权限清单提供给业务系统;将业务系统提供的权限信息与所述访问令牌绑定后存储至存储至编号资源对应表;以及,根据业务系统提供的访问令牌查询对应的权限信息,根据所述权限信息验证业务系统提供的控制指令的权限;当验证通过后,通过资源管理模块获得所述控制指令对应的控制接口并反馈至所述业务系统;所述资源管理模块内预存多个不同业务功能组件,用于根据所述业务功能组件生成权限清单并提供至所述安全平台调用;以及,根据所述控制指令获得对应的所述业务功能组件的控制接口;

[0006] 所述业务系统用于根据权限清单和用户勾选项生成权限信息并提供至云客服系统;以及,通过所述访问令牌和控制指令于所述云客服系统获得对应的业务功能组件的控制接口;通过控制接口操作对应的所述业务功能组件。

[0007] 在上述云客服平台管理系统中,优选的,所述安全平台还包含权限管理模块,所述权限管理模块用于接收用户请求信息和权限信息,根据所述用户请求信息生成用户编号;将所述用户编号与对应的权限信息关联后存储至编号资源对应表;以及,接收用户的访问请求,根据所述访问请求中的用户编号于所述编号资源对应表中获得对应的权限信息,根据所述权限信息和所述访问请求中的控制指令对所述资源管理模块内对应业务功能组件执行预定操作。

[0008] 在上述云客服平台管理系统中,优选的,所述业务系统还包含权限分配模块,所述

权限分配模块用于获取所述业务系统使用者的用户信息,根据所述用户信息于所述权限信息内分配对应的用户权限;将所述用户权限和所述用户信息关联后通过所述访问令牌发送至所述安全平台;所述安全平台根据所述用户权限和所述用户信息生成用户角色对应表,将所述访问令牌和所述用户角色对应表关联后存储至对应的所述编号资源对应表。

[0009] 在上述云客服平台管理系统中,优选的,所述云客服系统还包含客服功能模块,所述客服功能模块的操作界面存储于所述资源管理模块中;所述资源管理模块根据所述控制指令调取所述操作界面,并将所述操作界面通过所述安全平台提供给所述业务系统;所述业务系统将所述操作界面展示。

[0010] 在上述云客服平台管理系统中,优选的,所述安全平台还包含权限验证模块,所述权限验证模块用以将所述控制指令所涉及的业务功能组件范围与所述权限信息中所涉及的业务功能组件范围相比较,当所述控制指令所涉及的业务功能组件范围处于所述权限信息中所涉及的业务功能组件范围时,将所述控制指令输出至所述资源管理模块。

[0011] 本发明还提供一种云客服平台管理方法,所述方法包含:根据预存的多个不同业务功能组件生成权限清单;根据所述业务系统的身份信息生成访问令牌,将所述访问令牌与权限清单提供给业务系统;将业务系统提供的权限信息与所述访问令牌绑定后存储至存储至编号资源对应表;根据业务系统提供的访问令牌查询对应的权限信息,根据所述权限信息验证业务系统提供的控制指令的权限;当验证通过后,通过资源管理模块获得所述控制指令对应的控制接口并反馈至所述业务系统。

[0012] 在上述云客服平台管理方法中,优选的,根据所述权限信息和所述控制报文中的控制指令获得对应的所述业务功能组件的控制接口包含:将所述控制指令所涉及的业务功能组件范围与所述权限信息中所涉及的业务功能组件范围相比较;当所述控制指令所涉及的业务功能组件范围处于所述权限信息中所涉及的业务功能组件范围时,获得所述控制指令对应的所述业务功能组件的控制接口。

[0013] 本发明还提供一种云客服平台管理方法,所述方法包含:根据业务系统的身份标识生成请求指令,通过请求指令获得云客服系统反馈的访问令牌和权限清单;根据权限清单和用户勾选项生成权限信息并提供至云客服系统;通过所述访问令牌和控制指令于所述云客服系统获得对应的业务功能组件的控制接口;通过控制接口操作对应的所述业务功能组件。

[0014] 本发明还提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现上述方法。

[0015] 本发明还提供一种计算机可读存储介质,所述计算机可读存储介质存储有执行上述方法的计算机程序。

[0016] 本发明的有益技术效果在于:因此将统一的云平台进行拆分,将各个模块独立输出成为了一种趋势。既满足其他企业保留现有业务系统的需求,又赋予了现有业务系统电话、在线渠道接入的能力;以此使得不同企业和云客服系统对接仅需要按照云客服系统的规范标准为云客服系统提供对接的安全认证信息等参数,就能获取到云客服系统提供的电话、在线、工单、知识库等模块的服务。

## 附图说明

[0017] 此处所说明的附图用来提供对本发明的进一步理解,构成本申请的一部分,并不构成对本发明的限定。在附图中:

[0018] 图1为本发明一实施例所提供的云客服平台管理系统的结构示意图;

[0019] 图2A至图2C为本发明一实施例所提供的权限控制流程示意图;

[0020] 图3为本发明一实施例所提供的页面拆分结构示意图;

[0021] 图4为本发明一实施例所提供的云客服平台管理方法的流程示意图;

[0022] 图5为本发明一实施例所提供的云客服平台管理方法的流程示意图;

[0023] 图6为本发明一实施例所提供的安全认证的流程示意图;

[0024] 图7为本发明一实施例所提供的租户接入的流程示意图;

[0025] 图8为本发明一实施例所提供的租户接入的流程示意图;

[0026] 图9为本发明一实施例所提供的数字签名的生成流程示意图;

[0027] 图10为本发明一实施例所提供的计算机设备的结构示意图。

## 具体实施方式

[0028] 以下将结合附图及实施例来详细说明本发明的实施方式,借此对本发明如何应用技术手段来解决技术问题,并达成技术效果的实现过程能充分理解并据以实施。需要说明的是,只要不构成冲突,本发明中的各个实施例及各实施例中的各个特征可以相互结合,所形成的技术方案均在本发明的保护范围之内。

[0029] 另外,在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行,并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0030] 请参考图1所示,本发明所提供的云客服平台管理系统具体主要可包含云客服系统和业务系统;所述云客服系统包含安全平台和资源管理模块;

[0031] 其中,所述安全平台用于根据所述业务系统的身份信息生成访问令牌,将所述访问令牌与权限清单提供给业务系统;将业务系统提供的权限信息与所述访问令牌绑定后存储至存储至编号资源对应表;以及,根据业务系统提供的访问令牌查询对应的权限信息,根据所述权限信息验证业务系统提供的控制指令的权限;当验证通过后,通过资源管理模块获得所述控制指令对应的控制接口并反馈至所述业务系统;所述资源管理模块内预存多个不同业务功能组件,用于根据所述业务功能组件生成权限清单并提供至所述安全平台调用;以及,根据所述控制指令获得对应的所述业务功能组件的控制接口;所述业务系统用于根据权限清单和用户勾选项生成权限信息并提供至云客服系统;以及,通过所述访问令牌和控制指令于所述云客服系统获得对应的业务功能组件的控制接口;通过控制接口操作对应的所述业务功能组件。以此,在实际工作中,可将多种不同的业务功能模块都设置于云客服系统,其后当外部第三方的业务系统需要使用该些业务功能模块时,无需再重复开发,直接调用云客服系统中对应的业务功能模块即可;当然针对不同业务系统所需要的业务功能模块的差异,在该实施例中进一步采用权限的方式予以匹配业务系统所对应的业务功能模块,亦即,以安全组件为接入认证基础,以云平台的权限资源管理为业务系统用户控制依据,根据不同业务系统不同的需求以及不同的权限,赋予业务系统不同的能力。

[0032] 再请参考图1所示,所述云客服系统还可包含客服功能模块,所述客服功能模块的操作界面存储于所述资源管理模块中;所述资源管理模块根据所述控制指令调取所述操作界面,并将所述操作界面通过所述安全平台提供给所述业务系统;所述业务系统将所述操作界面展示。该客服功能模块主要实现的功能可包含软电话功能和在线功能等操作界面,使得业务系统可直接在该操作界面执行对应操作,而无需在本地进一步开发相应模块。

[0033] 在上述实施例中主要应用流程包含:云客服分配给其它业务系统用户名和固定的钥匙即访问令牌;其它业务系统通过分配的访问令牌访问云客服系统,其后云客服系统根据其他业务系统提供的访问令牌中含有的用户信息,访问自身的权限资源库;云客服系统根据自身权限资源库的内容,返回可用资源给其它业务系统;其它业务系统通过云客服赋予的资源权限,打开云客服对应的资源界面;根据对应的资源界面办理对应的业务。该方式提供给其它业务系统接入云客服系统的能力;通过安全控制机制,有效的防止非认证的资源访问云客服系统;通过权限控制机制,有效的控制对方系统访问的资源范围。

[0034] 在本发明一实施例中,所述安全平台还可包含权限管理模块,所述权限管理模块用于接收用户请求信息和权限信息,根据所述用户请求信息生成用户编号;将所述用户编号与对应的权限信息关联后存储至编号资源对应表;以及,接收用户的访问请求,根据所述访问请求中的用户编号于所述编号资源对应表中获得对应的权限信息,根据所述权限信息和所述访问请求中的控制指令对所述资源管理模块内对应业务功能组件执行预定操作。利用该权限管理模块可有效针对直接接入所述云客服系统的用户提供对应的业务服务功能,例如,依旧可采用权限管理的方式针对不同用户以权限的差异区别其所对应的业务功能,使得所述云客服系统除了为不同的业务系统提供业务功能模块之外还可处理不同用户直接接入该云客服系统时提出的相关业务处理要求。

[0035] 在本发明另一实施例中,所述业务系统还包含权限分配模块,所述权限分配模块用于获取所述业务系统使用者的用户信息,根据所述用户信息于所述权限信息内分配对应的用户权限;将所述用户权限和所述用户信息关联后通过所述访问令牌发送至所述安全平台;所述安全平台根据所述用户权限和所述用户信息生成用户角色对应表,将所述访问令牌和所述用户角色对应表关联后存储至对应的所述编号资源对应表。其中,为针对权限进行有效验证,所述安全平台还可包含权限验证模块,所述权限验证模块用以将所述控制指令所涉及的业务功能组件范围与所述权限信息中所涉及的业务功能组件范围相比较,当所述控制指令所涉及的业务功能组件范围处于所述权限信息中所涉及的业务功能组件范围时,将所述控制指令输出至所述资源管理模块。

[0036] 在实际工作中,以上实施例提供的权限管理模块和权限分配模块也可结合使用,具体权限控制流程主要可包含:使用云客服系统的用户,请参考图2A至图2B所示,如图2A所示,租户创建后,在机构员工分配五位字符串的租户标识,在产品服务创建虚拟中心。在云客服系统新增法人,选择法人需要使用的功能,菜单资源,首页模块,坐席类型,维护坐席数量,是否使用工单。选择后,法人所能使用的功能都是独立于其他法人的。接着,请参考图2B所示,创建法人后,租户管理员可以创建法人自身的权限,角色,用户。租户管理员可以控制租户用户能够使用哪些业务功能。至于使用权限分配模块的外部业务系统的用户,请参考图2C所示,使用租户标识创建clientId(用户编号),租户clientId(用户编号)创建后绑定可以使用的权限。权限能够访问哪些系统第三方调用Api接口同样可以通过界面进行分配。

绑定后租户就可以访问分配的云客服第三方Api接口。

[0037] 整体上,权限管理模块和权限分配模块在权限维护上主要具有以下功能:租户管理:租户接入系统后,首先分配租户Id,在系统维护租户相关的参数。同时选择租户能使用的菜单资源,没有选择的功能菜单,法人下的用户没有访问权限。法人对应菜单存放在法人资源对应关系表中。资源管理:资源分为菜单资源,首页模块,图片资源,受保护接口资源。导入或者在界面创建资源,资源维护了资源Id,资源路径,资源类型这些信息。权限管理:创建法人后,创建属于法人的权限,权限维护了权限Id,权限名称,所属法人标识这些信息。权限创建后进行分配资源的操作,从权限所属法人中查询出法人能够访问哪些不同的资源,然后勾选权限能访问的资源,勾选后这个权限就能访问相应的资源。一个权限可以对应访问多个资源,权限资源对应关系存放在权限资源关系表中。角色管理:创建法人后,创建属于法人的角色,角色维护了角色Id,角色名称,角色类型,所属法人标识这些信息。角色创建后进行分配权限的操作。根据角色所属法人标识查询法人下创建了哪些权限,勾选角色能够使用的权限。勾选后角色权限绑定,角色权限对应关系存放在角色权限对应表中。用户管理:创建法人后,可以创建法人下的用户。用户表维护了用户Id,用户名称,所属法人等用户信息。创建用户后,可以对用户进行分配角色的操作。根据用户所属法人标识查询法人下创建了哪些角色。勾选用户能有那些角色,勾选后用户角色进行绑定,用户角色对应关系存放在用户角色对应表中。绑定后,用户即可以使用相应权限分配的资源,对于法人能使用,但是用户所有权限未分配的资源,该用户无法访问。第三方客户管理:第三方客户是针对使用云客服接口的法人,创建第三方客户,维护客户Id,客户密钥。接入客户分配权限,客户才能使用对于权限的第三方保护资源。

[0038] 在本发明一实施例中,为保证后端各业务功能组件能够稳定提供服务,本发明中云客服系统可采用前后端分离予以组建,后端采用的技术栈是SpringCloud+mysql,功能模块包括多媒体服务、用户管理、权限管理、工单服务、知识服务、外呼服务等模块,每个模块都是一个独立的微服务,其接口可以通过安全网关上独立输出;前端采用的技术栈是VUE+NodeJS+Webpack,云客服功能页面按照SPA(single page web application,单页面应用)的方式进行构建,支持按角色加载不同的模块和菜单。各租户中有按模块接入的需求,比如租户需在其自建应用中嵌入软电话模块而不需要工单功能,两个模块彼此相互独立,如果这时还使用单页面应用会打包一堆与目标模块无关的代码,增加了页面响应时间,而且还会增加功能超范围使用的风险;因此,需对云客服的单页面应用按功能模块来进行拆分;单页面打包之后只生成一个html文件,这个文件就是项目的入口文件,多页面就是每个页面都对应一个html文件,页面和页面之间是相互独立的;每个模块都有权限分配机制来控制用户的访问规则。实际应用中,各业务功能组件的拆分原则主要包含以下四点:能力单一性,一个子页面只输出一种能力;能力独立性,功能拆分要高内聚低耦合,各子页面的功能尽量做到相互独立,避免环形依赖与双向依赖;能力完备性,子页面具有某种完备的能力,能够形成一个功能闭环。如工单模块,除了创建工单界面,应该还有查询、处理的操作界面;角色独立性,保证单一能力内的角色差异,如语音电话功能,普通坐席角色应该只有软电话操作界面、来电信息界面、技能组查询界面等,而电话参数配置、技能组分配等功能就应该赋给管理员角色。当然,本领域相关技术人员可根据实际需要,适当增加或修改上述各步骤,本发明对此并不做进一步限定。

[0039] 请参考图3所示,上述业务功能组件的拆分步骤主要是角色独立性,保证单一能力内的角色差异,如语音电话功能,普通坐席角色应该只有软电话操作界面、来电信息界面、技能组查询界面等,而电话参数配置、技能组分配等功能就应该赋给管理员角色。

[0040] 基于上述结构,实际工作中权限校验流程如下:

[0041] 云客服系统管理员创建法人,配置法人分配能访问拆分后的不同模块,创建权限,配置权限能访问的拆分模块资源,创建角色角色,配置角色能使用的权限,创建用户,给用户分配不同的角色。云客服系统用户访问云客服登陆界面,输入用户名密码登陆系统。获取到用户在系统的usrId。请求接口queryResOfUser传入对应的userId。

[0042] 请求报文如下:

```

    MsgData: {
      msgHead: {
        "sys_req_sec_id" : "", // 发起方安全节点编号
        "sys_snd_sec_id" : "", // 发送方安全节点编号
        "sys_evt_trace_id" : generalGlobalSerialNo(config.url), // 全局事件跟踪号
        "sys_snd_serial_no" : "", // 子交易号
        // "sys_req_time" : date.format('yyyyMMddhhmmss') // 发起方交易时间
      },
      msgEntity: {
        "usrId " : "xxx", // 员工 usrId
        .....
      }
    }
  
```

[0044] 请求接口后获得云客服的响应报文,返回用户能访问的拆分后的子界面,根据返回报文,渲染拆分后的子界面。返回报文如下:

[0045] MsgData: {

```

msgHead: {
  "sys_req_sec_id" : "", // 发起方安全节点编号
  "sys_snd_sec_id" : "", // 发送方安全节点编号
  "sys_evt_trace_id" : generalGlobalSerialNo(config.url), // 全局事件跟踪号
  "sys_snd_serial_no" : "", // 子交易号
  "sys_req_time" : date.format('yyyyMMddhhmmss') // 发起方交易时间
},

```

```

[0046] msgEntity: {
  "usrId": "xxx", // 员工编号
  "usrNm": "xxx", // 员工姓名
  "rscId": "xxx", // 资源 Id
  "rscNm": "xxx", // 资源名称
  "rscRte": "worksheet/index.html", // 资源路径, 以工单拆分模块为例
  .....
}
}

```

[0047] 基于这样的拆分机制,云客服各模块更加独立,接入租户使用不同的模块可配置化,便于后期的维护。如果租户扩展业务需要使用更多的模块,系统不需要根据租户重新发布,只需在后台进行权限配置即可。

[0048] 请参考图4所示,本发明还提供一种云客服平台管理方法,所述方法包含:S401根据预存的多个不同业务功能组件生成权限清单;S402根据所述业务系统的身份信息生成访问令牌,将所述访问令牌与权限清单提供给业务系统;S403将业务系统提供的权限信息与所述访问令牌绑定后存储至存储至编号资源对应表;S404根据业务系统提供的访问令牌查询对应的权限信息,根据所述权限信息验证业务系统提供的控制指令的权限;S405当验证通过后,通过资源管理模块获得所述控制指令对应的控制接口并反馈至所述业务系统。其中,根据所述权限信息和所述控制报文中的控制指令获得对应的所述业务功能组件的控制接口包含:将所述控制指令所涉及的业务功能组件范围与所述权限信息中所涉及的业务功能组件范围相比较;当所述控制指令所涉及的业务功能组件范围处于所述权限信息中所涉及的业务功能组件范围时,获得所述控制指令对应的所述业务功能组件的控制接口。

[0049] 请参考图5所示,本发明还提供一种云客服平台管理方法,所述方法包含:S501根据业务系统的身份标识生成请求指令,通过请求指令获得云客服系统反馈的访问令牌和权限清单;S502根据权限清单和用户勾选项生成权限信息并提供至云客服系统;S503通过所述访问令牌和控制指令于所述云客服系统获得对应的业务功能组件的控制接口;S504通过控制接口操作对应的所述业务功能组件。

[0050] 基于安全考虑,在不同业务系统访问本发明所提供的云客服系统时还需进一步进行相关安全认证,为此,本发明所提供的安全认证主要可分为两种不同的机制:对于云客服系统内部用户,采用spring-security认证。对于其他业务系统接入的用户。采用spring-oauth2认证。两种认证方式互不影响,各自控制系统受保护资源的访问。

[0051] 请参考图6所示,云客服系统内部提供了工单,知识库,智能外呼等各模块的微服务,以及web界面。统一由网关对外暴露,网关接入了安全组件和0auth2(一种安全组件插件)插件。安全组件主要用于对云客服内部用户的认证和权限校验。0auth2插件主要用来对接入第三方系统的用户认证和权限校验。

[0052] 在证书校验原理上:用户访问web界面实际上是访问安全网关映射的地址。安全网关映射到互联网是https的请求,需要证书的校验。

[0053] 用户认证和权限校验过程如下:

[0054] a) 云客服系统用户认证。

[0055] 对于云客服系统内部的用户来说。使用云客服系统,首先通过安全组件进行用户认证。对于所有的客服云资源的访问都需要是认证用户,如果用户未认证访问提示“无权访问系统”。校验session是否用户登陆,如果未登录则跳转至登陆界面。如果用户已经登陆,校验session获取用户权限,在云客服系统内部用户调用登录服务时,系统会给用户创建一个默认的权限,该权限为随机字符串通过md5(一种加密算法)加密算法生成,访问系统所有的资源需要匹配这个加密随机码权限,如果不匹配则提示“访问被拒绝”。从而实现只有通过云客服系统登录认证的用户,才能访问云客服系统的资源。

[0056] b) 第三方接入系统用户认证。

[0057] 对于接入云客服的第三方系统,使用云客服系统的接口,必须带有云客服系统生成的令牌。如果调用方未传入令牌,则访问返回“访问被拒绝”。第三方系统接入后,云客服系统分配用户名(也称为AppId),和接入密钥(key),第三方调用相关接口传入用户名和密钥获得到令牌。调用云客服受保护资源时,传入到Http Headers中,云客服系统解析令牌,判断令牌是正确的则访问通过,如果令牌和系统生成的令牌不匹配则返回“无效令牌”。令牌是具有时效性,超过有效期的令牌系统返回“无效令牌”。

[0058] c) 云客服系统权限校验。

[0059] 本发明包含一套灵活可配置的权限校验。对于云客服系统内部的用户,可以配置的资源有菜单资源,首页模块资源,坐席类型资源,受保护接口资源,图片资源。第一,用户通过session进行用户认证后,获取到用户的用户名。通过用户名查询权限微服务,返回用户可以访问的菜单,首页模块,坐席类型,图片资源,在云客服系统进行渲染。第二,在系统内部,对一些敏感接口进行保护,比如更改用户信息接口,删除日志接口,更新报表数据接口。对于敏感接口,系统提供了一套受保护接口配置功能,保证必须分配有某些角色的用户才能访问这些接口,如果用户没有分配这些角色。即便是系统管理员,调用这些接口也会返回“访问被拒绝”的错误提示信息。

[0060] d) 第三方接入系统权限校验。

[0061] 对第三方接入系统,0auth2(一种安全组件插件)插件同样提供系统受保护资源的权限校验。云客服校验令牌通过后,第三方接入系统就可以访问系统的普通接口,但想要访问受保护的接口,必须要云客服系统管理员给用户名(也称为AppId)分配对应的权限,否则

调用返回“访问被拒绝”。

[0062] 在签名和验签的原理上:为确认用户端请求数据是否合法以及请求数据是否被篡改,本发明增加了签名和验签的机制。签名:发送方用一个哈希函数从报文文本中生成报文摘要,然后用自己的私人密钥对这个摘要进行加密,得到的就是这个报文对应的数字签名。通常来说,发送方会把数字签名和报文原文一并发送给接受者。验签:接收方得到原始报文和数字签名后,用同一个哈希函数从报文中生成摘要A,另外,用发送方提供的公钥对数字签名进行解密,得到摘要B,对比A和B是否相同,就可以得知报文有没有被篡改过。

[0063] 生成签名与验签流程如下。

[0064] 生成签名方:首先把参数放入一个字符串数组中,把参数和值放入一个对象或HashMap(Java中的一种数据结构)中,使用JSONObject(Java中的一种工具类)把这个对象转化成json(一种数据结构)对象。然后生成签名数据,在生成签名数据时,我们调用Java的排序方法把参数按照字典顺序排序。然后使用RSA(一种非对称加密算法)的私钥对签名数据进行签名。

[0065] 验签方:和生产签名方一样先生成签名数据,然后使用RSA的公钥、生成签名方传入的签名及签名数据对生成签名方传入的签名进行验证,验证结果为正确时说明验证成功,否则为未通过。

[0066] 在防御重放攻击原理上:重放攻击(Replay Attacks)又称重播攻击、回放攻击或新鲜性攻击(Freshness Attacks),是指攻击者发送一个目的主机已接收过的包,来达到欺骗系统的目的,主要用于身份认证过程,破坏认证的正确性。为防止重放攻击,本发明增加防御重放攻击的机制。安全网关中获取的参数中,带有时间戳和随机数。在有效期时间内,如果攻击者拦截并发送一个目的主机已接收过的数据包,那么这个数据包中包含的随机数和已经接收过的请求数据包中随机数相同,认定为重放攻击。

[0067] 结合上述实施例,以下请参考图7至图8所示,对用户接入所述云客服系统调用业务功能组件的流程做整体说明,本领域相关技术人员当可知,该实施例仅为便于理解本发明所提供的上述各实施例,并不对其做进一步限定。

[0068] 用户直接使用云客服系统时,具体流程如下:

[0069] 1. 租户先申请租户编号、租户管理员、权限、资源、接入时间、license等;

[0070] 2. 云客服根据申请为租户开户,创建租户,赋予资源,并提供租户管理员的登录ID和密码;

[0071] 3. 租户管理员登录到云客服系统,自己创建角色、分配资源;

[0072] 4. 该方案中租户登录系统采用session的方式,后端根据session进行安全、权限、流量的校验,并记录交易日志。

[0073] 用户调用云客服系统API接口的具体流程如下:

[0074] 租户申请租户编号、权限、资源、接入时间、license等;

[0075] 云客服根据申请为租户开户,提供APPID、APPSecret、签名的生成机制、接口调用规范、可调用接口清单等;

[0076] 租户在调用接口时,其流程如图7所示:

[0077] 1. 租户用户发在前端发起请求;

[0078] 2. 租户的应用中根据APPID、APPSecret组装请求,向云客服发起token请求;

- [0079] 3. 云客服验证APPID、APPSecret的有效性,并返回accessToken;
- [0080] 4. 租户应用将accessToken缓存起来,并设置到接口http请求的header中,组装请求报文,生成签名,访问云客服的API接口;
- [0081] 5. 云客服校验签名的有效,校验accessToken的有效性,再校验accessToken的权限,最后执行接口请求,返回接口执行结果;
- [0082] 6. 租户应用将返回结果展示给用户。
- [0083] 该方案中租户访问云客服的接口采用Token和签名的方式,后端根据签名进行请求合法性的校验,根据Token进行安全、权限、流量的校验,并全程记录交易日志。
- [0084] 用户嵌入云客服系统子页面的流程如下:
- [0085] 租户申请租户编号、权限、资源、接入时间、license等;
- [0086] 云客服根据申请为租户开户,提供APPID、APPSecret、子页面调用规范、子页面调用地址等;
- [0087] 租户在调用子页面时,其流程如图8所示:
- [0088] 1. 租户用户发在前端发起请求;
- [0089] 2. 租户的应用中根据APPID、APPSecret组装请求,向云客服发起token请求;
- [0090] 3. 云客服验证APPID、APPSecret的有效性,并返回accessToken;
- [0091] 4. 租户应用将accessToken缓存起来,在访问页面时,其url后要携带accessToken;
- [0092] 5. 云客服校验accessToken的有效性,再校验accessToken的权限,最后返回路由到页面资源的地址;
- [0093] 6. 租户应用返回云客服子页面。
- [0094] 该方案中租户访问云客服的子页面采用Token的方式,后端根据Token进行安全、权限、流量的校验,并全程记录交易日志。
- [0095] 在上述实施例中,生成数字签名的流程可参考图9所示,数字签名是对请求报文的参数进行计算,生成一个特殊的校验字符串;由于请求报文采用的json格式,每一个请求的参数顺序可能不一致,会影响签名的生成。因此在计算签名前,先要对参数进行排序;请求参数列表中的key按照ASCII码从小到大排序,然后将排好序的参数转成字符串,最后对字符串用MD5生成数字签名。
- [0096] 本发明还提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,所述处理器执行所述计算机程序时实现上述方法。
- [0097] 本发明还提供一种计算机可读存储介质,所述计算机可读存储介质存储有执行上述方法的计算机程序。
- [0098] 本发明的有益技术效果在于:因此将统一的云平台进行拆分,将各个模块独立输出成为了一种趋势。既满足其他企业保留现有业务系统的需求,又赋予了现有业务系统电话、在线渠道接入的能力;以此使得不同企业和云客服系统对接仅需要按照云客服系统的规范标准为云客服系统提供对接的安全认证信息等参数,就能获取到云客服系统提供的电话、在线、工单、知识库等模块的服务。
- [0099] 如图10所示,该计算机设备600还可以包括:通信模块110、输入单元120、音频处理单元130、显示器160、电源170。值得注意的是,计算机设备600也并不是必须要包括图10中所示的所有部件;此外,计算机设备600还可以包括图10中没有示出的部件,可以参考现有

技术。

[0100] 如图10所示,中央处理器100有时也称为控制器或操作控件,可以包括微处理器或其他处理器装置和/或逻辑装置,该中央处理器100接收输入并控制计算机设备600的各个部件的操作。

[0101] 其中,存储器140,例如可以是缓存器、闪存、硬驱、可移动介质、易失性存储器、非易失性存储器或其它合适装置中的一种或更多种。可储存上述与失败有关的信息,此外还可存储执行有关信息的程序。并且中央处理器100可执行该存储器140存储的该程序,以实现信息存储或处理等。

[0102] 输入单元120向中央处理器100提供输入。该输入单元120例如为按键或触摸输入装置。电源170用于向计算机设备600提供电力。显示器160用于进行图像和文字等显示对象的显示。该显示器例如可为LCD显示器,但并不限于此。

[0103] 该存储器140可以是固态存储器,例如,只读存储器(ROM)、随机存取存储器(RAM)、SIM卡等。还可以是这样的存储器,其即使在断电时也保存信息,可被选择性地擦除且设有更多数据,该存储器的示例有时被称为EPROM等。存储器140还可以是某种其它类型的装置。存储器140包括缓冲存储器141(有时被称为缓冲器)。存储器140可以包括应用/功能存储部142,该应用/功能存储部142用于存储应用程序和功能程序或用于通过中央处理器100执行计算机设备600的操作的流程。

[0104] 存储器140还可以包括数据存储部143,该数据存储部143用于存储数据,例如联系人、数字数据、图片、声音和/或任何其他由计算机设备使用的的数据。存储器140的驱动程序存储部144可以包括计算机设备的用于通信功能和/或用于执行计算机设备的其他功能(如消息传送应用、通讯录应用等)的各种驱动程序。

[0105] 通信模块110即为经由天线111发送和接收信号的发送机/接收机110。通信模块(发送机/接收机)110耦合到中央处理器100,以提供输入信号和接收输出信号,这可以和常规移动通信终端的情况相同。

[0106] 基于不同的通信技术,在同一计算机设备中,可以设置有多个通信模块110,如蜂窝网络模块、蓝牙模块和/或无线局域网模块等。通信模块(发送机/接收机)110还经由音频处理器130耦合到扬声器131和麦克风132,以经由扬声器131提供音频输出,并接收来自麦克风132的音频输入,从而实现通常的电信功能。音频处理器130可以包括任何合适的缓冲器、解码器、放大器等。另外,音频处理器130还耦合到中央处理器100,从而使得可以通过麦克风132能够在本机上录音,且使得可以通过扬声器131来播放本机上存储的声音。

[0107] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0108] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产

生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0109] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0110] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0111] 以上所述的具体实施例,对本发明的目的、技术方案和有益效果进行了进一步详细说明,所应理解的是,以上所述仅为本发明的具体实施例而已,并不用于限定本发明的保护范围,凡在本发明的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

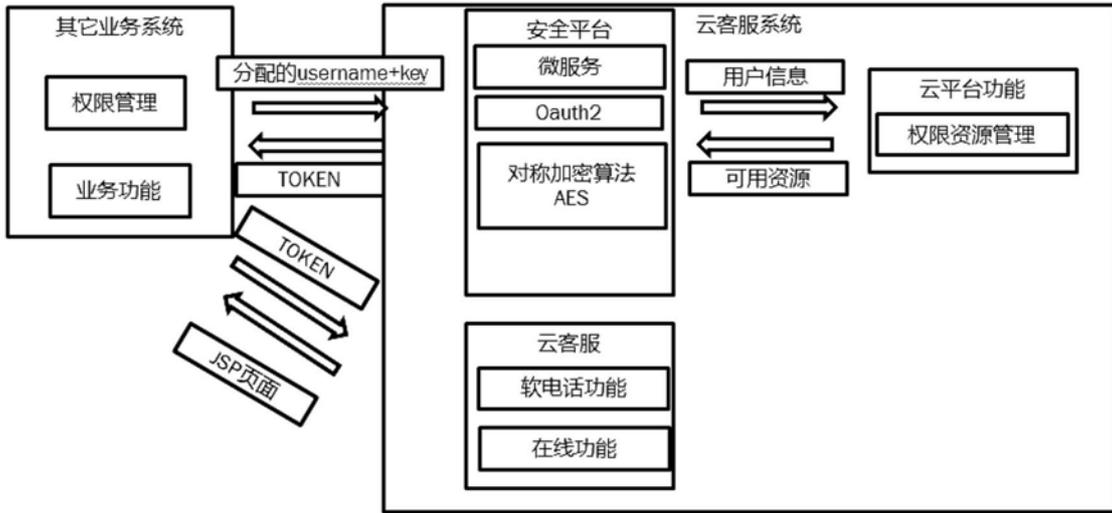


图1

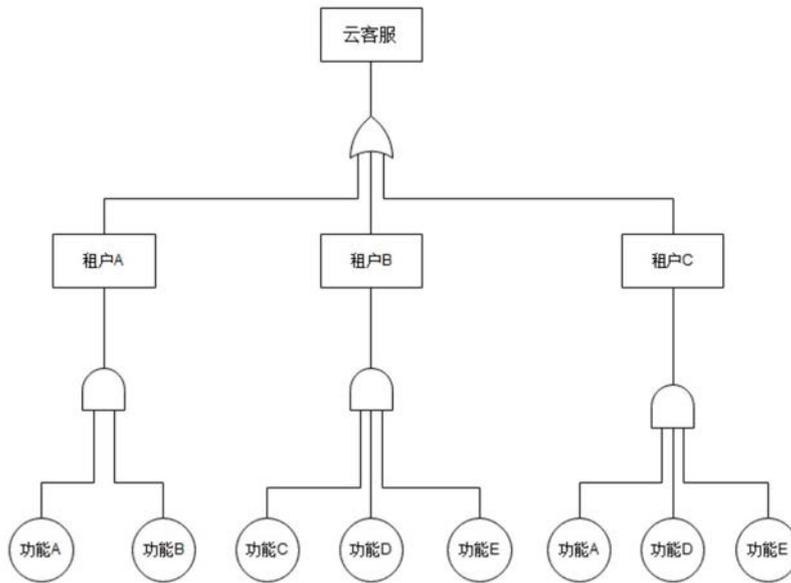


图2A

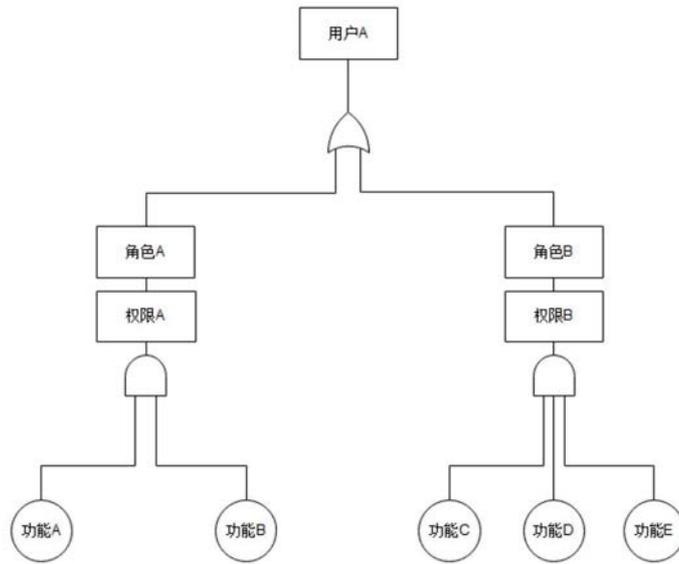


图2B

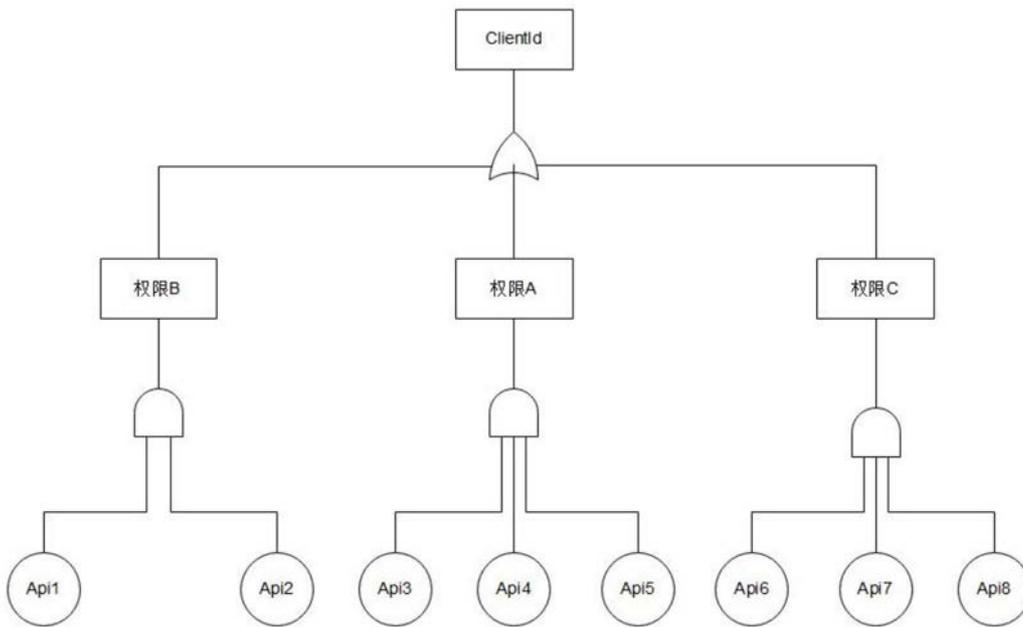


图2C

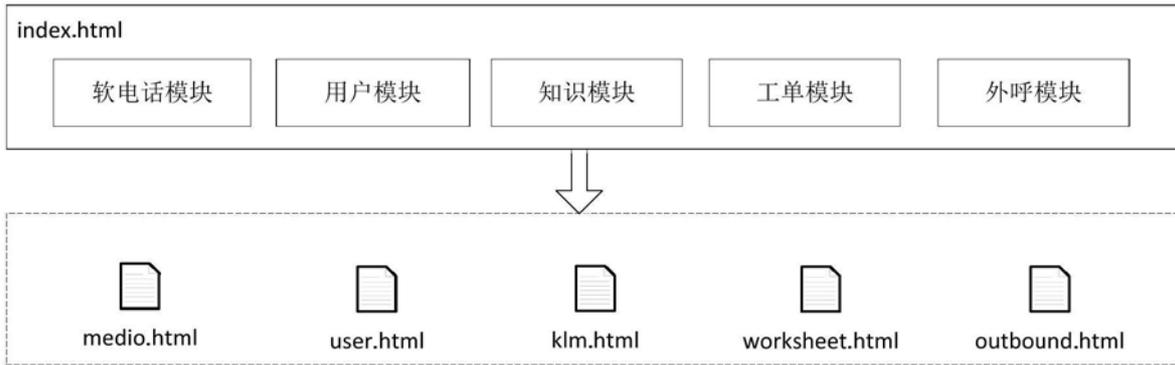


图3

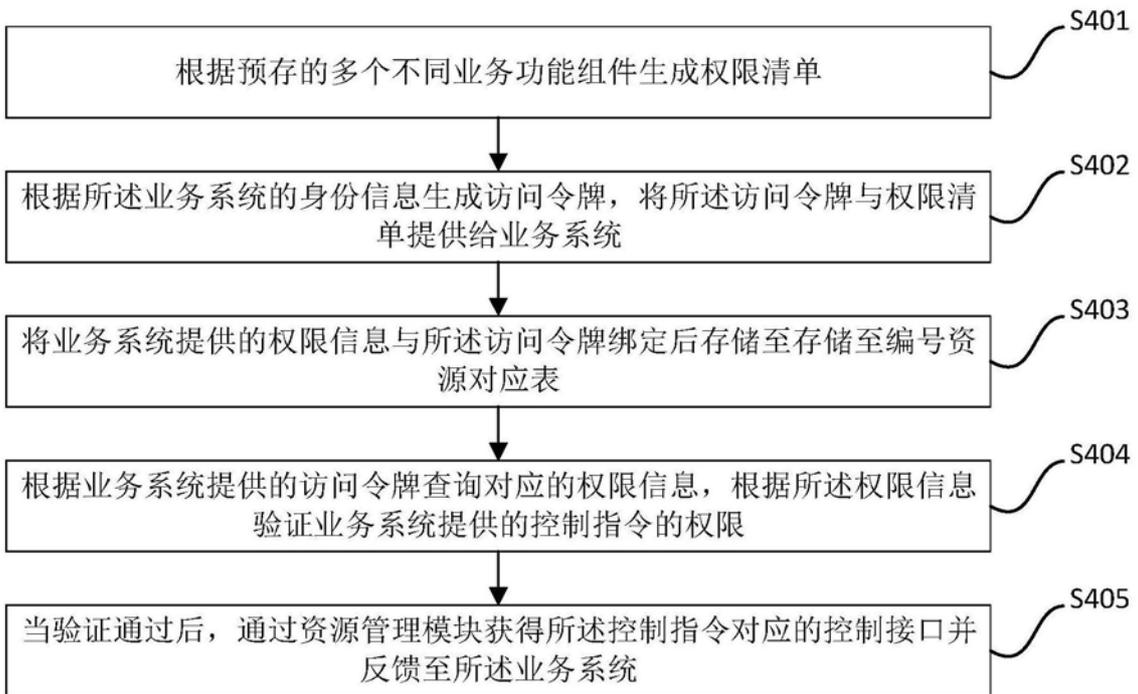


图4

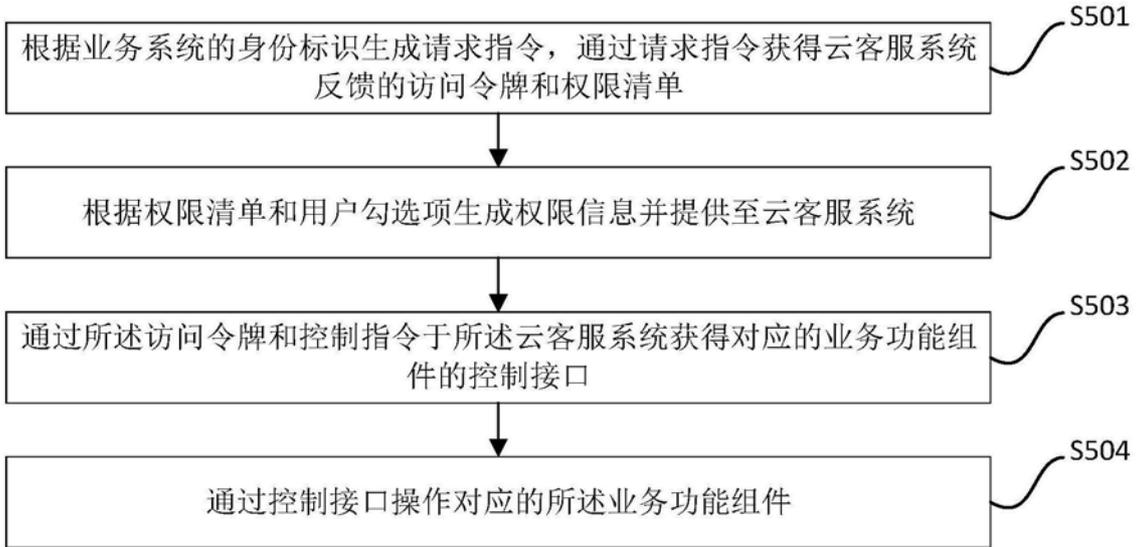


图5

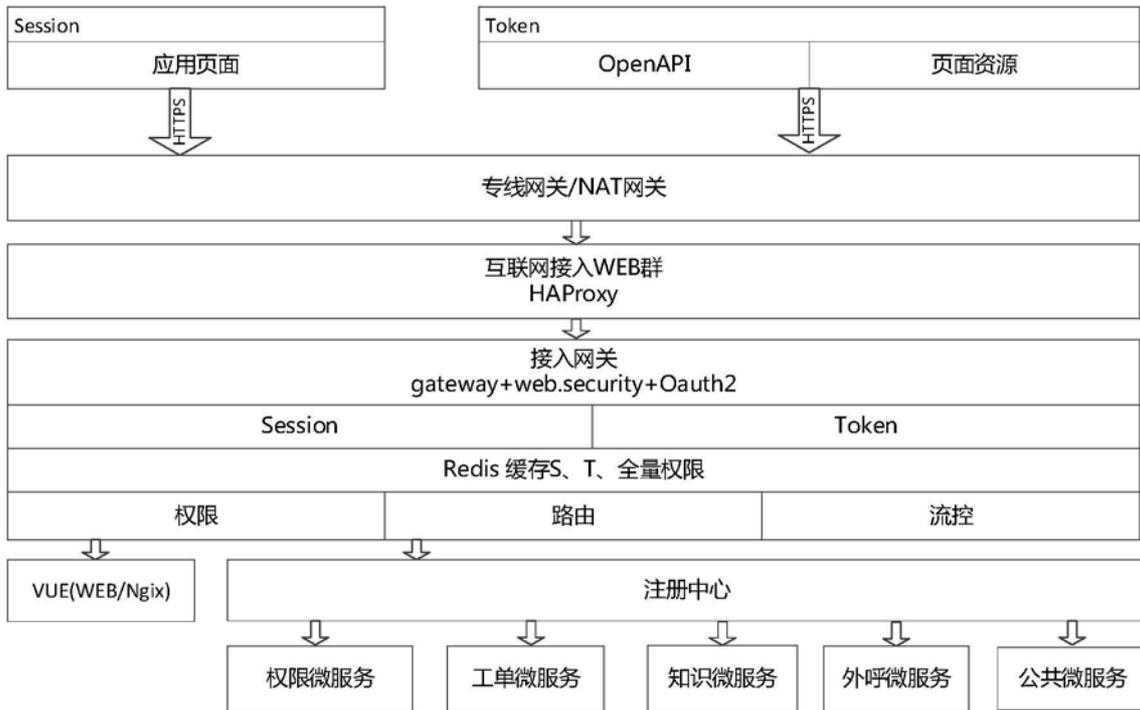


图6

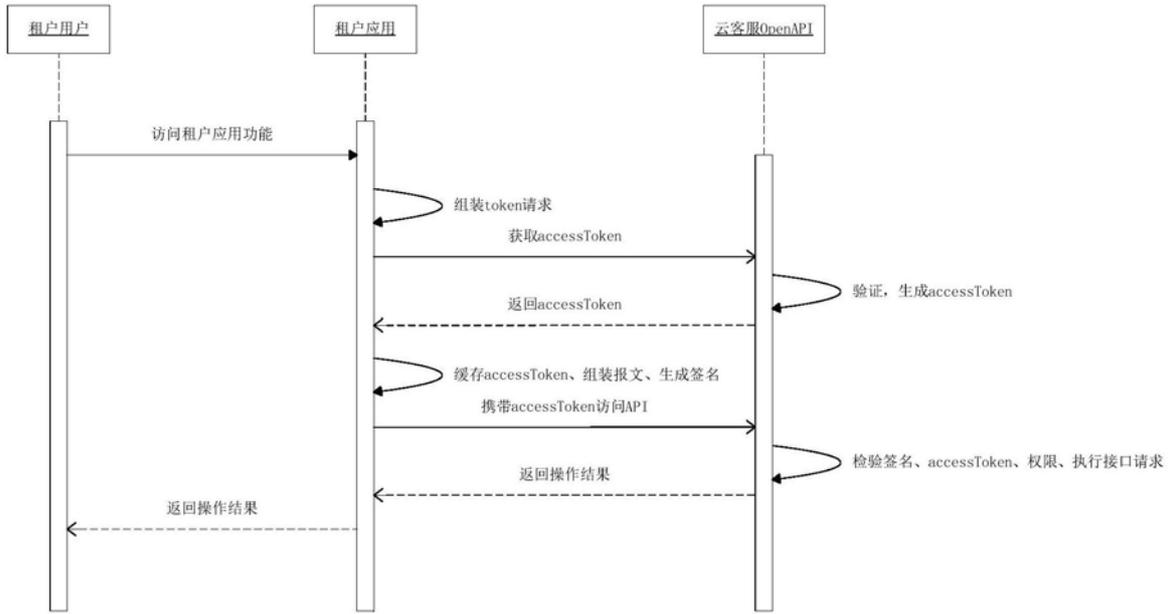


图7

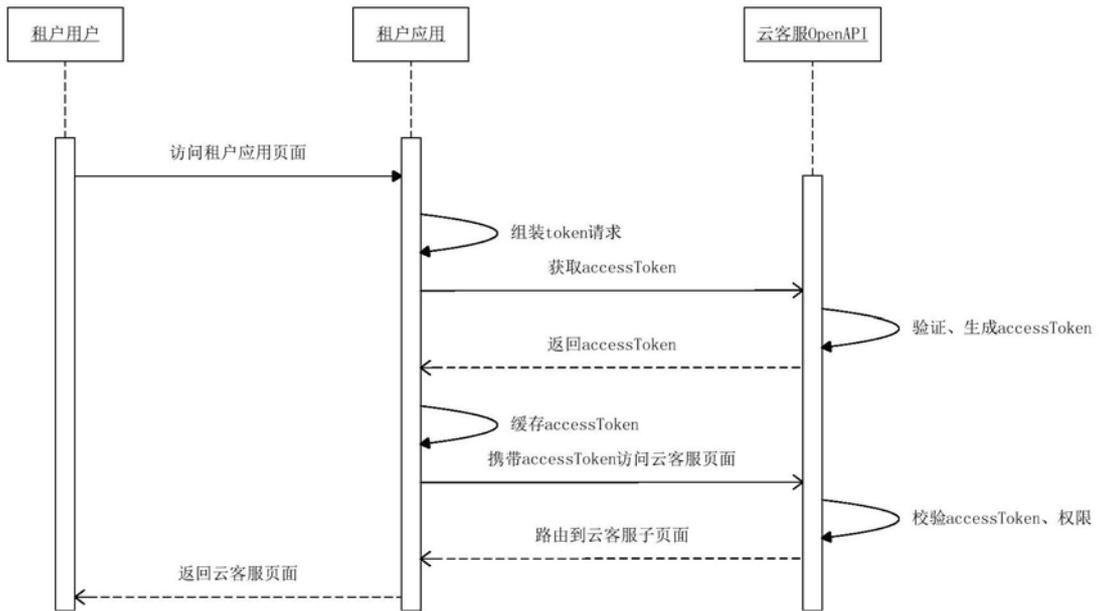


图8

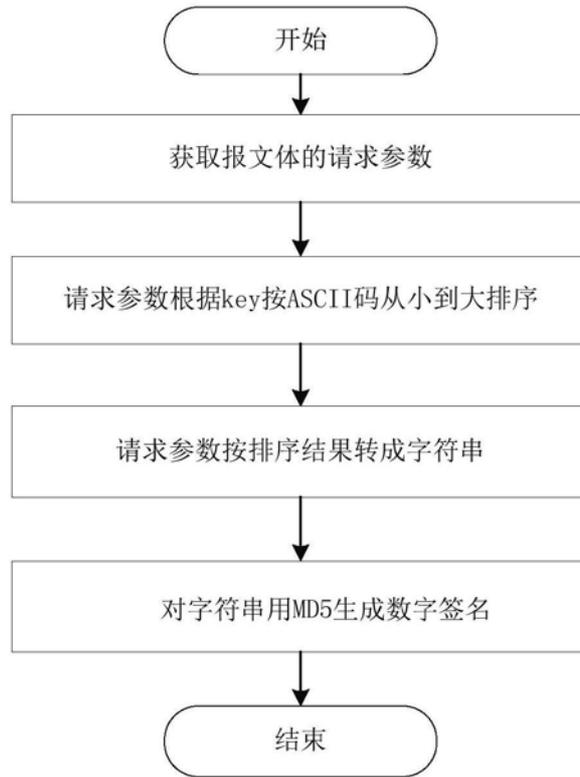


图9

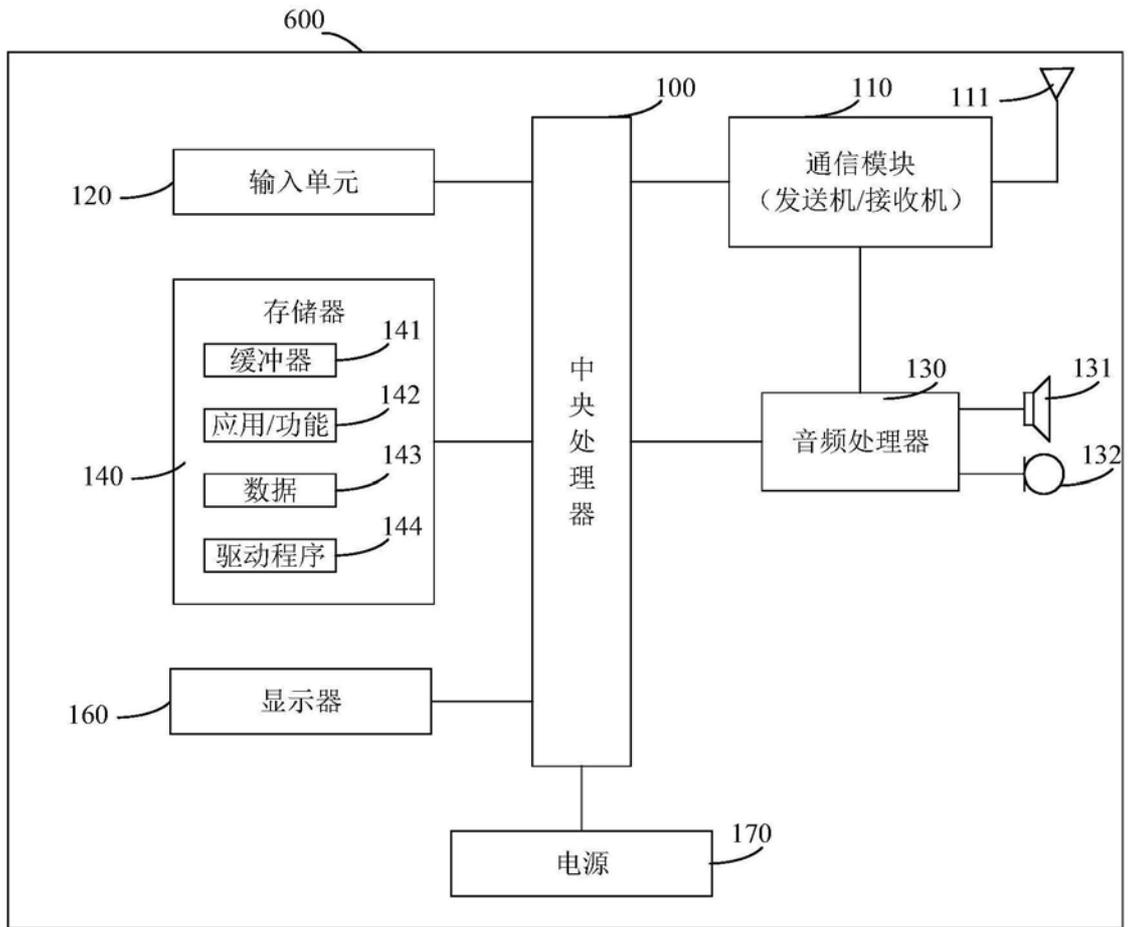


图10