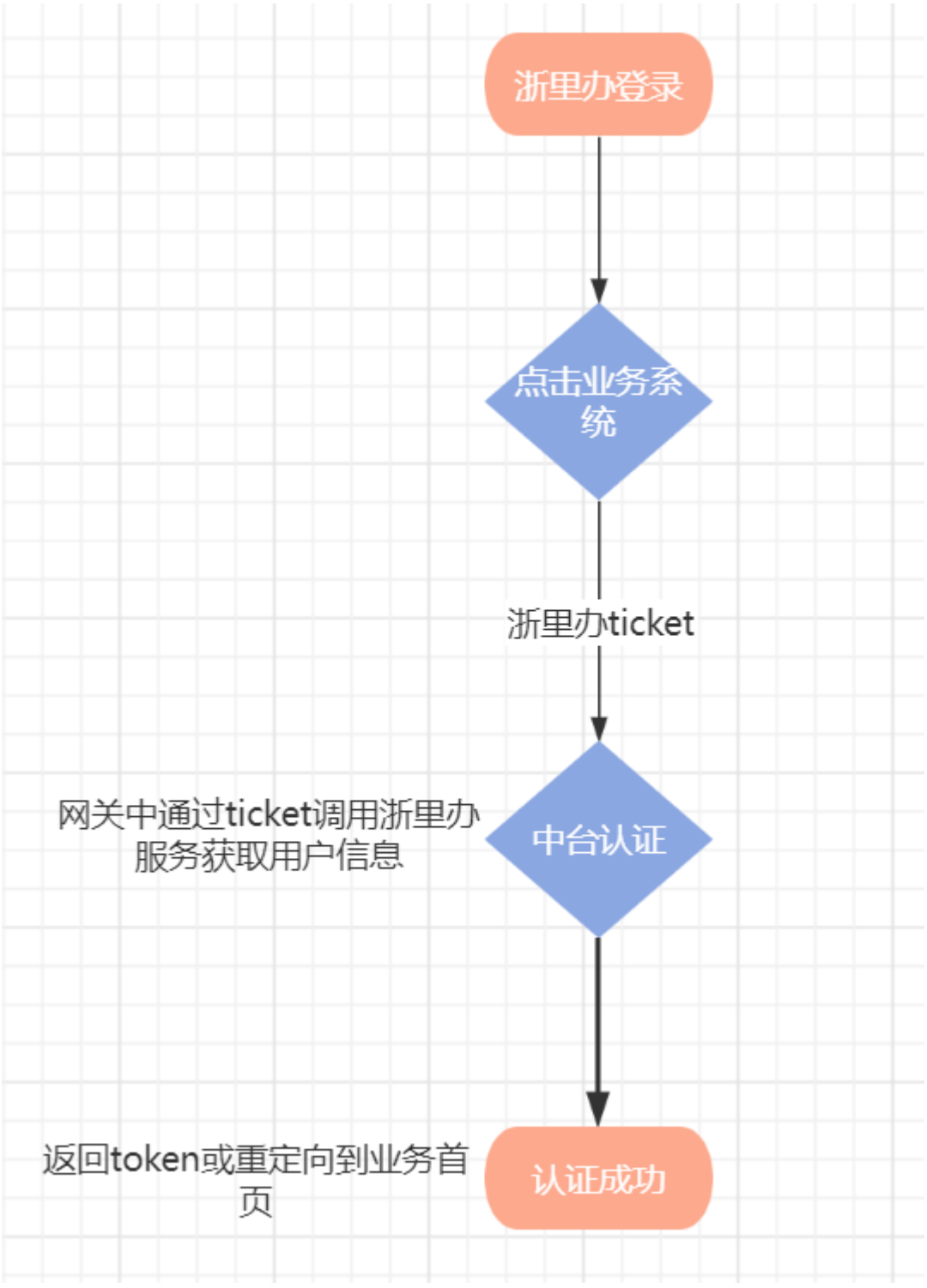
1 浙里办认证

1.1 认证流程



1.2 认证配置

Apollo 中需添加如下配置

浙里办个人：

```
//servicecode（上架后提供）
commnetsoft.servicecode = tzzxptmhscmkcshj
//servicepwd（上架后提供）
commnetsoft.servicepwd = tzzxptmhscmkcshjpwd
//serviceurl （上架后提供一般此处不用修改）
commnetsoft.serviceurl = http://puser.zjzwfw.gov.cn/sso/
//默认的重定向地址(如配置了 type=token 或 sp={redirecturl}此项可不配置）
sso.redirecturl = http://192.168.11.73:9081
//新加用户的机构 id（查询 bt_department 表获取，默认为公众用户，有多个用逗号隔开）
commnetsoft.deptIds = 9aa9e30e-5b5a-11e9-bf20-54a05055f480
//新加用户的角色 id（查询 bt_role 表，多个用逗号隔开，默认配置可能现场没有当前角色 id，此项必须修改）
commnetsoft.userRoles = 02fdb956-8bc5-11e7-90b6-74d02b7c2db7
//是否与浙政钉使用同一账号（通过手机号关联，默认为 false）
commnetsoft.relatezzding = false
```

浙里办法人：

```
//上架后提供
ssolegal.projectId = 1111564305
//上架后提供
ssolegal.projectSecret = 55ea54dac3f497c43344a9904f4aa1ae
//上架后提供
ssolegal.QUERY_URL =
http://essotest.zjzwfw.gov.cn:8080/rest/user/query
//同个人
ssolegal.deptIds = 05a19c05-1ed7-11e9-9d7f-b0359f24ae97
//同个人
ssolegal.userRoles = b5afacec-8ff1-4b68-ad48-a2cd0adba8c8
//同个人
sso.redirecturl = http://192.168.11.73:9081
```

1.3 接口说明

浙里办个人：

GET：http://ip:19088/auth/auth/auu/ticket

认证成功后如需直接返回中台认证后的 token，需要在接口后添加参数?type=token，不加则默认重定向到指定页面。

认证成功后如需重定向到指定页面，需在接口后添加参数?sp={redirect_url}，如不加且没有加 type=token 会重定向到默认配置 sso.redirecturl（默认重定向地址是 http://192.168.11.73:9081，可通过 apollo 中 oauth2-server 的此配置项修改）

浙里办法人：

POST：http://ip:19088/auth/auth/auu/ssoLegal

需注意，认证成功后如需重定向到指定页面，需在接口后添加参数?goto={redirect_url}，其他和浙里办个人一致。

1.4 用户同步

浙里办个人：

用户首次通过浙里办登录时（在框架数据库中没有此用户），会默认创建一条用户记录，包含 id、用户名、手机号、中文名（均为调用浙里办接口返回的用户信息）

浙里办法人：

除以上信息还将法人的详细信息存在了 bt_user 表中的 user_extend 字段中，可通过调用获取用户信息接口查看

http://ip:19088/identity/users/getByIdUser/{userid}
信息如下：

1.5 常见问题

在同一系统使用了浙政钉、浙里办两种登录方式的情况下，如遇到同一个用户分别使用浙政钉和浙里办登录导致系统中出现两条用户记录的情况，需修改配置项 commnetsoft.relatezzding = true，此配置项会统一先通过用户手机号进行判断。

2. 浙政钉认证

2.1 认证流程

浙政钉认证分为扫码登录和 app 内登录

扫码登录：

在扫码后获取到 authCode，然后调用回调地址。

app 登录：

需在浙政钉 app 开发前端调用获取浙政钉免登 code，然后传入回调地址中。

2.2 认证配置

//新加用户的机构 id（查询 bt_department 表获取，默认为公众用户，有多个用逗号隔开）
dingtalk.deptIds = 9aa9e30e-5b5a-11e9-bf20-54a05055f480
//新加用户的角色 id（查询 bt_role 表，多个用逗号隔开，默认配置可能现场

```
没有当前角色 id，此项必须修改）
dingtalk.userRoles = 02fdb956-8bc5-11e7-90b6-74d02b7c2db7
//浙政钉 accesskey（应用上架后提供）
dingtalk.accessKey=testcode_dingoa-HPcv9p82raieem
//浙政钉应用 secretkey（应用上架后提供）
dingtalk.secretKey=7ou5J8E0X9T60SkuVZ1gcq8EvvnS4944zen263E4
//浙政钉接口域名（正式环境域名为 openplatform-pro.ding.zj.gov.cn）
dingtalk.domainName=openplatform.dg-work.cn
//请求协议（此处一般不用修改）
dingtalk.protocal=https
```

2.3 接口说明

GET：http://ip:19088/auth/auth/auu/authCode?authCode=

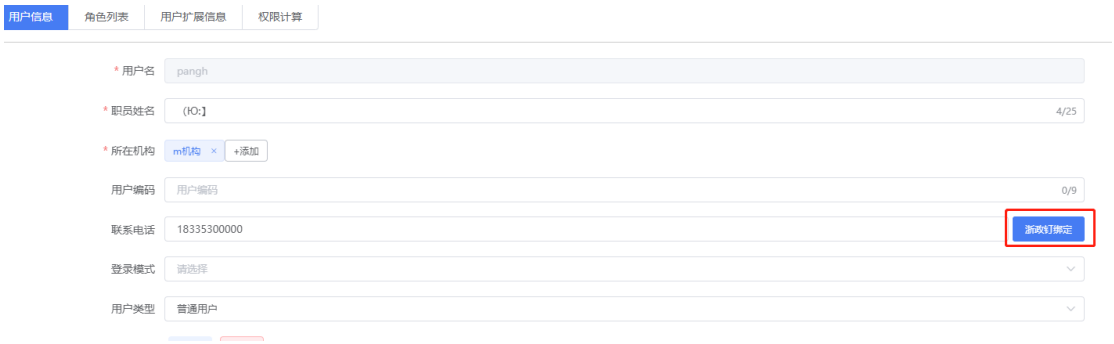
其中 authCode 为 app 登录前端获取的免登 code 或扫码后获得的 code 扫码登录和 app 登录使用同一个接口，认证成功后如需直接返回中台认证后的 token，需要在接口后添加参数?type=token，不加则默认重定向到指定页面。

认证成功后如需重定向到指定页面，需在接口后添加参数?sp={redirect_url}，如不加且没有加 type=token 会重定向到默认配置 sso.redirecturl（默认重定向地址是 http://192.168.11.73:9081，可通过 apollo 中 oauth2-server 的此配置项修改）。

2.4 用户同步

用户首次通过浙政钉登录时（在框架数据库中没有此用户），会默认创建一条用户记录。

如系统中已有部分用户，浙政钉登录的用户需要与现有用户做关联，则需要在用户管理中将现有用户的手机号录入（此手机号需为当前用户浙政钉登录的手机号），点击绑定浙政钉，后面通过 app 或扫码登录都会返回当前用户信息，而不会重新创建。



如系统中已有部分用户，浙政钉登录后要与已有用户关联，但是不想在用户管理中手动绑定时（比如已有用户的浙政钉手机号无法获取），可以在接口中添加参数 relateDingId=true（此配置只用在扫码登录），如 http://ip:19088/auth/auth/auu/authCode?relateDingId=true，添加此配置后如果通过扫码登录，后台发现当前用户为关联浙政钉，则会提示用户输入账号密码进行绑定，详细配置参考

<<浙政钉扫码登录.docx>>

2.5 常见问题

2.5.1 浙政钉和专有钉钉区别

专有钉钉为浙政钉的测试环境，在公司开发测试均在专有钉钉上进行测试，正式环境中需要申请浙政钉应用（由客户进行申请）。

2.5.2 多应用配置

如果在浙政钉中上架了多个应用，且使用同一套认证系统（即 oauth2-server 使用的是同一个），由于不同的应用对应的 accesskey 和 secretkey 不同，需要将不同应用的参数配置到 apollo 中，并将应用标识通过请求接口传过来。比如在浙政钉上架了两个应用，分别为一张图应用和一体化审批应用，对应的应用标识为 YZT 和 YTHSP，首先需在 apollo 中的 oauth2-server 添加对应的配置，如：

```
YZT.accessKey=testcode_dingoa-HPcv9p82raieem
YZT.secretKey=7ou5J8E0X9T60SkuVZ1gcq8EvvnS4944zen263E4
YZT.domainName=openplatform.dg-work.cn
YZT.protocal=https

YTHSP.accessKey=testcode_dingoa-HPcv9p82raieem
YTHSP.secretKey=7ou5J8E0X9T60SkuVZ1gcq8EvvnS4944zen263E4
YTHSP.domainName=openplatform.dg-work.cn
YTHSP.protocal=https
```

Key 由 dingtalk.换成了对应的应用标识.如不配置则使用默认的 dingtalk.

请求地址中需携带对应的应用标识参数，如：

http://ip:19088/auth/auth/auu/authCode?zzdAppCode=YZT

http://ip:19088/auth/auth/auu/authCode?zzdAppCode=YTHSP

2.5.3 内网无法访问互联网问题

由于项目中 oauth2-server 所部署的服务器在政务内网，因为获取浙政钉用户信息对应的请求在互联网上，可能遇到网络不通的情况，需要申请 oauth2-server 所在服务器访问 https://openplatform.dg-work.cn 的权限，如果无法申请只能通过代理的方式解决。

浙政钉接口互联网代理添加方式：

首先在能访问互联网的服务器上部署一个 nginx（首先需确认此服务器与 oauth2-server 网络能互通），在里面配置 https://openplatform.dg-work.cn 的代理，然后将 apollo 中 oauth2-server 的配置 dingtalk.domainName 和 dingtalk.protocal 修改为代理后的，需注意此代理必须代理到根路径。

代理配置示例：

比如 oauth2-server 部署的服务器 ip 为 192.168.11.73（内网服务器，无法访问互联网），有一台互联网服务器 122.224.233.68（能访问互联网，并且能访问到 192.168.11.73），则需要在 122.224.233.68 服务器上部署一个 nginx 代理，里面添加浙政钉相关代理：

```
location / {
            root   html;
            index  index.html index.htm;
            proxy_pass https://openplatform.dg-work.cn;
}
```

如：

```
server {
    listen       8081;
    server_name  gisqtest.com;

    #charset koi8-r;

    #access_log  logs/host.access.log  main;

    location / {
        root   html;
        index  index.html index.htm;
        proxy_pass https://openplatform.dg-work.cn;
    }
```

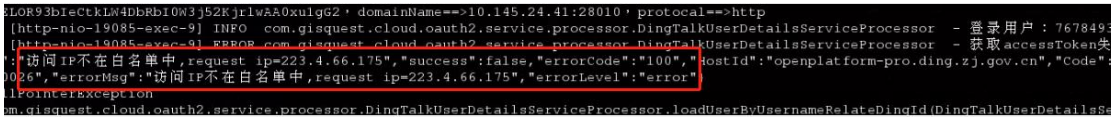
注意，localtion 后必须为/，不可添加路径，否则接口无法调用。

代理配置好后修改 apollo 中的 oauth2-server 配置为

```
dingtalk.domainName=122.224.233.68:8081
//请求协议（根据代理的情况修改为 https 或 http）
dingtalk.protocal=http
```

2.5.4 访问 ip 不在白名单的问题

由于浙政钉正式环境需要配置访问白名单才可以调用接口，如没配置在登录时会报如下错误：



遇到此情况需联系浙政钉相关负责人（目前是联系吕剑豪）进行白名单的配置，一般将错误信息中对应的 ip 配置上即可，如果有多个出口 ip 需要联系大数据局获取出口 ip 再进行配置。

2.5.5 扫码登录应用申请

扫码登录和 app 登录应用不同，需要提交申请扫码登录流程，申请时会要求提供回调地址，回调地址一般填写

http://ip:19088/auth/auth/auu/authCode（后面对应的参数，如 sp=根据实际情况添加）

2.5.6 扫码登录二维码地址

专有钉钉二维码地址：

https://login.dg-work.cn/oauth2/auth.htm?response_type=code&client_id=testcode_dingoa&redirect_uri=http://192.168.9.83:19088/auth/auth/auu/authCode?type=token&scope=get_user_info&authType=QRCODE&embedMode=true

其中 client_id 为应用标识

浙政钉二维码地址：

https://login-pro.ding.zj.gov.cn/qrlogin/webAppLogin.htm?APP_NAME=ymgd_dingoa&protocolKey=3b7e51cc-7c2a-4ea7-9f75-0da087dd7b27&protocol=oauth2&BACK_URL=http://172.23.31.21:19088/auth/auth/auu/authCode?type=token&scope=get_user_info&state=&embedMode=true

其中 APP_NAME 为应用标识，申请扫码登录应用后可以得到