统一身份认证平台应用系统集成规范

1　范围

本标准规定了各信息系统与统一身份认证平台进行集成单点登录与数据同步时所遵循的规范标准，并明确接口对接的方式与参数。各信息系统与统一身份认证平台进行对接时，应遵循此规范标准。

本标准适用于山东京博控股集团有限公司（以下简称“集团”）、各产业公司及其关联公司（以下简称“各公司”）。

2　规范性引用文件

无

3　术语和定义

3.1 IAM 平台

IAM（Identity and Access Management 的缩写），即“身份识别与访问管理”。IAM 平台指统一身份认证平台。

3.2 应用系统

指与 IAM 平台进行集成的各信息系统。

3.3 应用系统账号

指各应用系统下的用户账号。

3.4 SSO 单点登录

单点登录(SingleSignOn，SSO)，指通过用户的一次性鉴别登录。

4　集成范围和概述

统一身份认证平台集成范围如下：

集成场景	功能描述	生产方	消费方	中间方
单点登录	各应用系统采用 IAM 系统标准的 OAuth2.0 协议进行集成单点登录集成	IAM 系统	各应用系统	融合集成平台
数据同步	各应用从 IAM 系统同步数据，	各应用系统	IAM 系统	融合集成

	可同步的数据包括用户数据和组织数据			平台

4.1 集成步骤

各应用系统与 IAM 平台对接手顺如下：

① 阅读本集成规范，明确对接内容及步骤；

② 填写应用对接申请表（参见附件 1），进行应用注册；

③ IAM 平台进行应用注册和对接信息反馈；

④ 各应用系统根据 IAM 平台反馈对接信息，按需进行对接。

其中主体集成对接内容分两部分：

（一）单点登录集成步骤

① 应用方按照本集成规范组装认证地址，通过浏览器重定向到 IAM 申请认证 code；

② 应用方通过融合集成平台调用 IAM 接口使用认证 code 获取 token；

③ 应用方通过融合集成平台调用 IAM 接口使用 token 换取用户信息。

获取最终用户信息即为需要登录应用的账号。

（二）数据同步集成步骤

① 应用方按照本集成规范要求，提供数据接收接口；

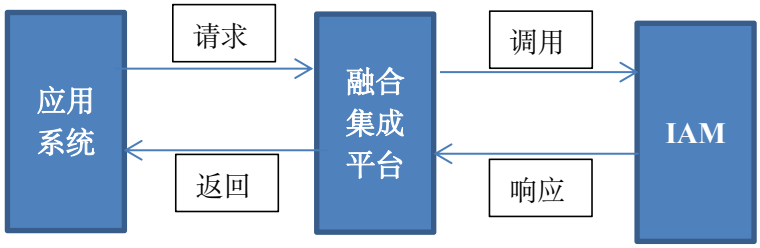
② IAM 系统依照本集成规范要求，生成 jwt token；

③ IAM 携带 jwt token 通过融合集成平台调用应用系统数据接收接口，进行数据分发；

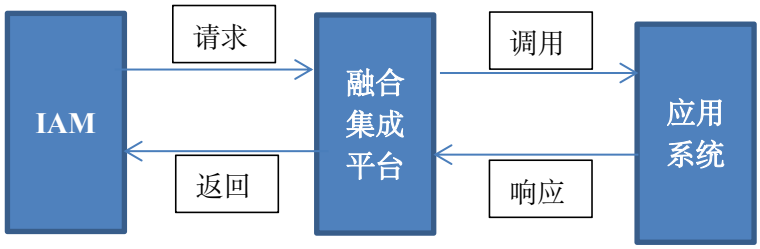
④ 各应用系统接收数据，进行 jwt token 鉴权，鉴权通过，进行逻辑处理。

4.2 接口调用顺序

➢ IAM 作为服务方，各应用系统作为消费方，例如单点登录的获取 token 和获取用户信息接口：



➢ 各应用系统作为服务方，IAM 作为消费方，例如数据同步接口：



4.3 接口鉴权说明

整个接口交互过程分三个角色：

① 接口调用方

② 接口提供方

③ 融合集成平台

各角色定义及说明：

接口提供方需对本身提供的接口进行 jwt token 鉴权，目的在于接收数据时对数据发送方的身份进行合法校验，以保证系统安全性。

融合集成平台本身会进行接口调用鉴权，目的在于控制接口调用方能否通过融合集成平台调用第三方接口，从而保证接口链路的安全性。

5 应用单点登录集成规范

5.1 概述

IAM 平台作为认证服务端，支持 OAuth2.0、SAML2.0 标准认证协议，协议对比如下：

协议	特性	优势	劣势
OAuth2.0	基于 access_token，安全不可仿冒，code 一次有效	主流认证协议，适用范围广，安全性高，流程简单集成快捷	---
SAML2.0	XML 格式 通过加密和签名等多重机制保障安全	安全性高	开发集成较为复杂,适用限制多

要求应用优先使用 OAuth2.0 协议进行单点登录对接。

5.2 OAuth2.0 单点对接

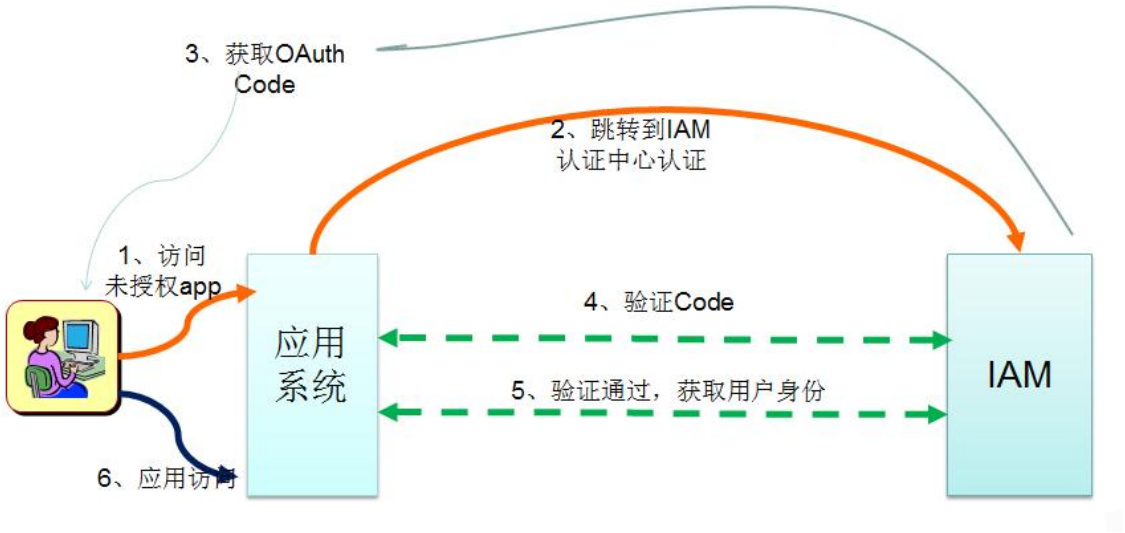
5.2.1概述

各应用系统单点登录集成采用统一身份认证平台标准的 OAuth2.0 协议进行集成。

OAuth2.0（开放授权）是一种国际通用的授权方式，是一个开放标准。用户授权后，第三方应用无需获取用户的用户名和密码，就可以访问该用户在某一网站上存储的资源。官方技术说明可参看http://oauth.net/2/。

OAuth2.0 认证具有平台无关性、环境多样性，支持 Web、手机、移动设备等，如 Apple iOS，Andriod 等，将认证能力从 B/S 到移动应用全面覆盖。

OAuth2.0 开放认证的登录步骤可参考下图：



1) 用户访问业务系统的地址时，浏览器重定向请求到 SSO 的认证地址；

2) OAuth2.0 验证重定向的参数，验证通过浏览器携带 code 跳转到应用；

3) 应用在获取 code 后，应用通过 code 去认证地址换取访问 token；

4) 在获取访问 token 后，携带 token 通过调用接口获取认证用户信息；

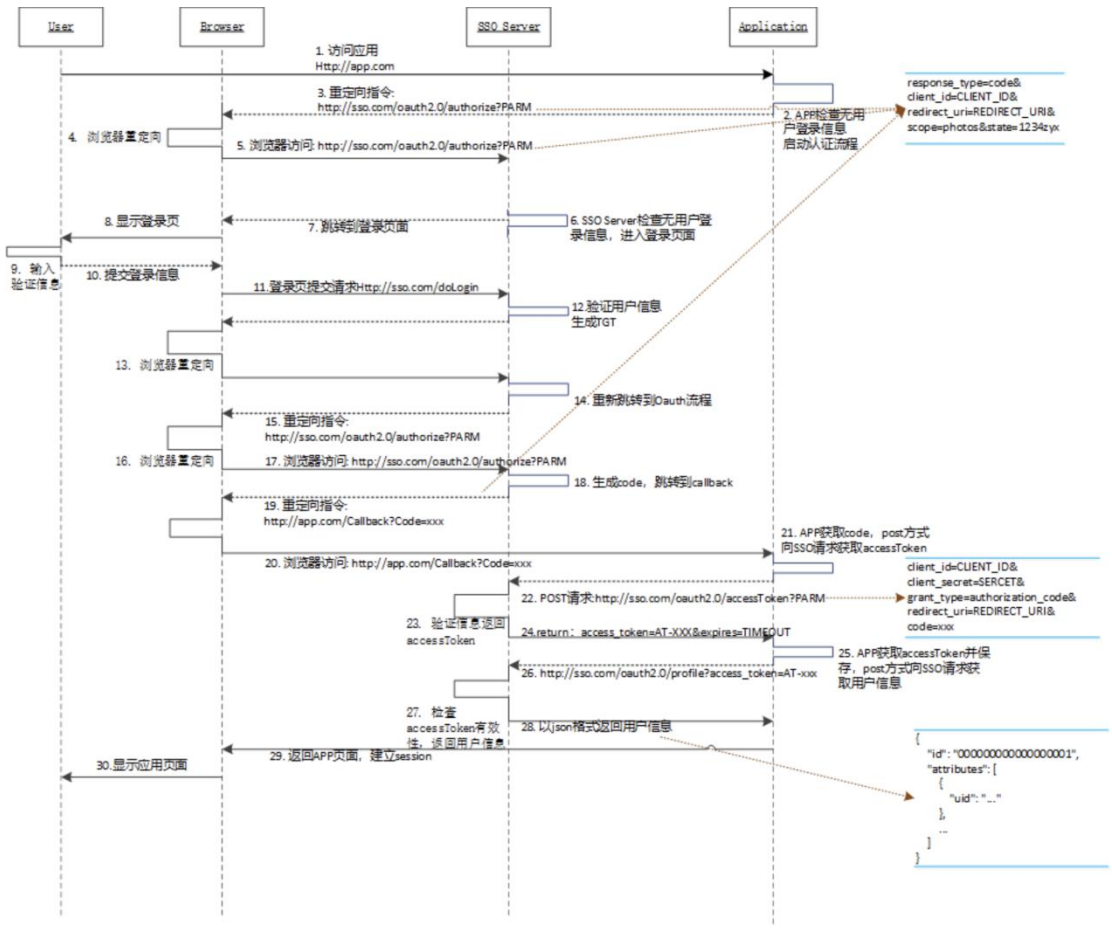
5) 应用获取用户信息，认证完成，应用系统将获取到的用户数据与自身的数据完成匹配，用户即可正常访问应用系统。

交互过程中用到的参数说明：

参数	提供方	说明

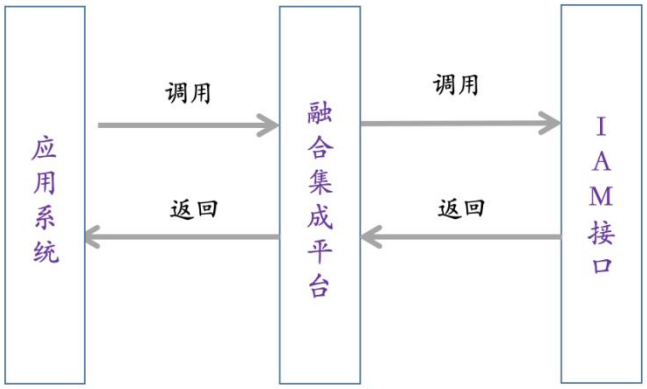
client_id	IAM 平台	应用调用 IAM 接口所需参数
client_secret	IAM 平台	应用调用 IAM 接口所需参数
入口地址	应用系统	用于 IAM 系统触发通知应用开始单点交互流程
回调地址	应用系统	用于接收 code，继续 OAuth 交互逻辑处理

5.2.2授权流程



5.2.3接口调用流程

单点登录过程除下方 5.2.4 章节接口（获取 code）与 5.2.7 章节接口调用方式为浏览器重定向，其余接口均通过融合集成平台进行调用，流程如下图所示：



5.2.4 oauth2.0/authorize 重定向请求认证 code

5.2.4.1 URL 接口格式

https://地址:端口/esc-sso/oauth2.0/authorize?client_id=[appKey]&response_type=code&redirect_uri=[appRedirectUrl]&oauth_timestamp=[oauth_timestamp]&state=[target_uri]

说明：调用方式为浏览器重定向。

5.2.4.2 URL 参数说明

参数	类型	必填	说明
appKey	string	是	注册业务系统的 KEY，由统一身份认证平台后台管理注册应用时生成。
appRedirectUrl	string	是	应用单点登录时的回调地址，单点登录验证通过后跳转到应用系统的地址（由业务系统提供）。
oauth_timestamp	string	否	当前时间戳，单位：毫秒(13 位)。如：1572232273705
target_uri	String	否	额外参数，如果传递 http 需要转义 URL ENCODE，用户目标访问 URL

5.2.4.3 响应参数说明

参数	类型	必填	说明

code	string	是	交互 token 验证码
state	string	否	额外参数（如果 authorize 接口传递了参数，这里就会返回）

5.2.5 oauth2.0/accessToken 获取 token 接口

5.2.5.1 URL 接口格式

https://地址:端口/env-201/open-apiportal/iamopen/oauth/accessToken?grant_type=authorization_code&oauth_timestamp=[oauth_timestamp]&client_id=[appKey]&client_secret=[appSecret]&code=[code]&redirect_uri=[appRedirectUrl]

5.2.5.2 URL 参数说明

HTTPS 请求，方式为 Post。

参数	类型	必填	说明
appKey	string	是	注册业务系统的 KEY，由统一身份认证平台后台管理注册应用时生成。
appSecret	string	是	应用注册密钥 appSecret，由统一身份认证平台后台管理注册应用时生成。
code	string	是	交互 token 验证码，SSO 认证接口生成并推送给应用的单点登录回调接口中。
appRedirectUrl	string	是	应用单点登录回调地址，单点登录验证通过后跳转到集成应用的地址（由业务系统提供）。
oauth_timestamp	string	是	当前时间戳，单位：毫秒(13 位)。如：1572232273705

5.2.5.3 响应参数说明

参数	类型	含义	说明
access_token	string	token 值	


```
{
  "access_token":"AT-30-dLZ2HdytEclP2UG2DQGihTcUbsU5Kb",
  "token_type":"bearer",
  "expires_in":86400
}
```

5.2.6 oauth2.0/profile 获取用户信息接口

5.2.6.1 URL 接口格式

https://地址:端口/env-201/open-apiportal/iamopen/oauth/profile?access_token=[token]

5.2.6.2 URL 参数说明

HTTPS 请求,方式为 Get。

参数	类型	必填	说明
token	string	是	由获取 token 接口获取

5.2.6.3 响应参数说明

参数	类型	含义	是否必有值	说明
token_expired	string	token 有效期	是	秒单位
token_gtime	string	时间戳	是	Long 类型时间戳
accountNo	string	应用系统 账号	是	账号
userName	string	用户姓名	是	用户姓名
id	string	统一认证平台账号	是	

该响应参数可配置，应用集成时可按需沟通

```
{
   "attributes" : {
      "accountNo" : "103234",
      "token_expired" : "7200",
      "token_gtime" : 1621000246591,
       "userName" : "张三"
   },
   "id" : "103234"
}
```

5.2.7单点退出

门户系统在会话超时或主动退出时，须调用 IAM 接口注销 IAM 会话。

5.2.7.1 URL 接口格式

1）https://地址:端口/esc-sso/logout

2）https://地址:端口/esc-sso/logout?service=[redirectUrl]

调用方式为浏览器重定向。

5.2.7.2 URL 参数说明

参数	类型	必填	说明
redirectUrl	string	否	退出后的跳转地址

5.2.8会话保持

为保证门户系统与 IAM 系统会话的一致性，门户系统根据用户活动状态调用 IAM 接口，进行 IAM 会话续期，以保证其他系统单点登录效果。

5.2.8.1 URL 接口格式

https://sso.xxx.com.cn/esc-sso/api/v1/loginLog/checkAccessToken

5.2.8.2 URL 参数说明

参数	类型	必填	说明
accesstoken	string	是	需要续期 tgt 的 token

5.2.8.3 响应参数说明

参数	类型	必填	说明
errorCode	string	是	编码
errorMsg	string	是	返回信息
version	string	是	版本号
timestamp	string	是	时间戳
data	String	是	用户名

5.3 SAML2.0 单点对接

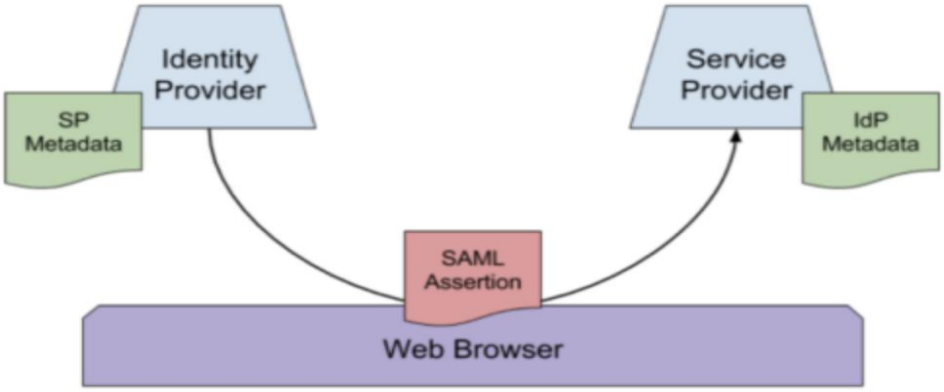
5.3.1定义和术语

名词术语	英文全称	描述
SSO	Single Sign-On	单点登录，一次登录访问所有应用
SP	Service Provider	用户打算访问的服务，如各种 SaaS 服务
SAML	Security Assertion Markup Language	SAML 是一种开放的协议，为桌面程序或者基于 B/S 的 web 应用提供了企业级，标准的方式实现单点登录功能
metadata		IdP 或者 SP 提供给对方的一组信息，定义了 SAML 交互过程中需要用到的各种信息，如证书，支持的 profile，定义 endpoint 等等。
IdP	Identity Provider	此处 IAM 登录平台即为 IdP,提供认证服务并实现单点登录。
IAM	Identity and Access Management	身份与访问控制
Entity Id		全球唯一的标识名称，用于标识身份提供商或者应用提供商

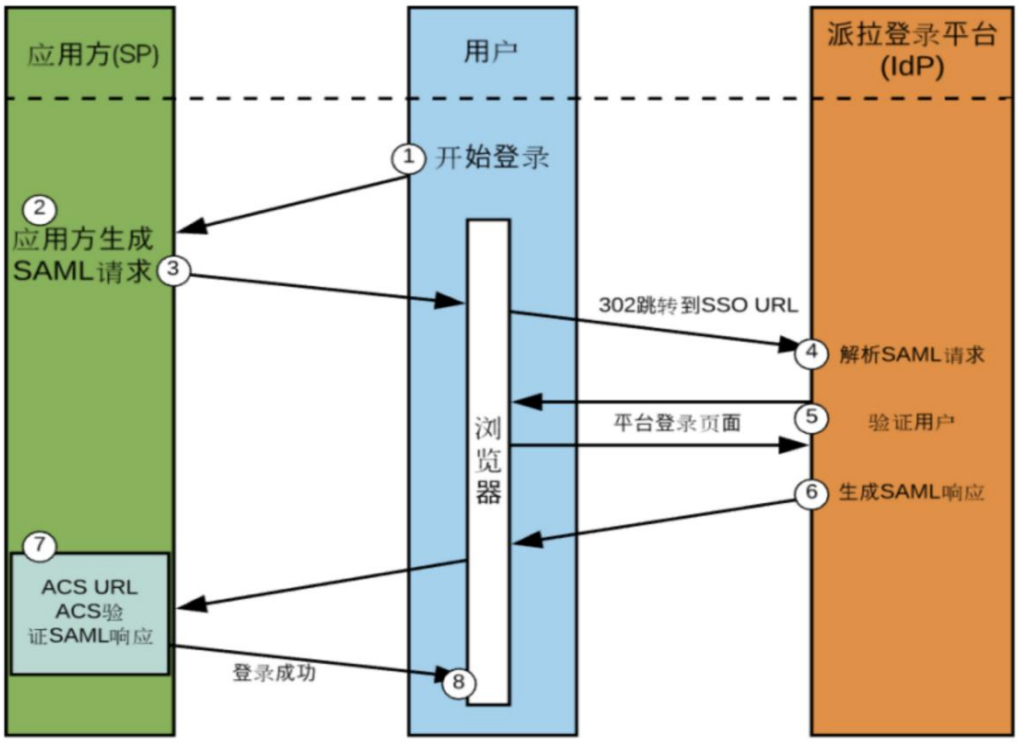
5.3.2认证集成过程

下图为 SAML2.0 认证交互过程图：

1）配置阶段： 服务方和认证方交换 metadata,建立信任。



2）使用阶段： 认证过程



流程说明：

1. 用户试图访问 IAM 的应用方，如 HMS。
2. 应用方生成一个 SAML 身份验证请求。SAML 请求编码并嵌入到 URL。RelayState 参数包含编码的合作伙伴应用程序，用户尝试访问的 URL 也被嵌入在 SSO URL。RelayState 参数是一个不透明的标识符，不作任何修改或检查传回的。
3. 应用方发送重定向到用户的浏览器。重定向 URL 编码 SAML 身份验证请求的，应提交到 SSO (IAM) 服务。
4. SSO (IAM) 的 SAML 请求进行解码，并提取两个断言消费服务 (ACS) 和用户的目标 URL (RelayState 参数）的 URL。
5. SSO（IAM）的用户进行身份验证。SSO（IAM）可以通过要求有效的登录凭据，或通过检查有效的会话对用户进行身份验证。
6. IAM 生成一个 SAML 响应，其中包含身份验证的用户名。按照 SAML 2.0 规范，这种反应是应用方的 DSA / RSA 密钥数字签名的。IAM SAML 响应和 RelayState 参数进行编码，并将该信息返回到用户的浏览器。
7. 应用方的 ACS 使用 IAM 的公钥验证 SAML 响应。如果成功验证的响应，ACS 将用户重定向的目标 URL。
8. 用户被重定向的目标 URL，并记录在应用方应用程序。

5.3.3请求 URL 实例及参数说明

idp/profile/SAML2/POST/SSO		
[POST]		
处理SP发起的WEB SSO PROFILE POST请求		
参数	类型	描述
SAMLRequest	String	由SP发出的AuthnRequest
返回		
	302	跳转到登录页面，如果登录成功返回SAML Response

/idp/profile/SAML2/Redirect/SSO		
[GET]		
处理SP发起的WEB SSO PROFILE Redirect请求		
参数	类型	描述
SAMLRequest	String	由SP发出的AuthnRequest
返回		
	302	跳转到登录页面，如果登录成功返回SAML Response

/idp/profile/SAML2/Unsolicited/SSO		
[GET]		
由idp发起的SSO请求		
参数	类型	描述
providerId	String	urlencode编码的SP注册entity id
返回		
	302	生成SAML Response，跳转到SP应用。

5.4 注意事项

- 应用系统普通用户通过统一身份认证进行单点登录；
- 建议应用管理员账号仍使用应用单独登录入口进行认证；
- 非门户系统退出时只需退出自身会话，并关闭系统当前浏览器标签页即可；
- 门户系统退出会话时，需调用单点退出接口进行 IAM 会话注销。

6 OAuth2.0 单点登录接口调用样例

6.1 准备工作

模拟场景：

- 业务系统地址（入口地址）为：http://app.com/login
- 业务系统回调地址为：http://app.com/callback

应用系统提供以上信息进行 IAM 应用注册，IAM 反馈以下信息：

- client_id ： fd51ce2b60e5514ab998
- client_secret ： 5ea5f4b284ace74590aa99ec69f7082c3bc6
- IAM 系统访问地址为：http://iam.paraview.cn
- 测试账号：zhangsan 姓名：张三

6.2 应用系统申请 code

第一步：

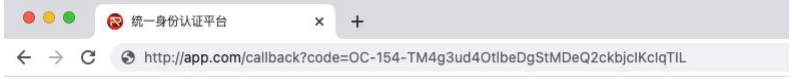
用户通过浏览器访问业务系统地址 http://app.com/login，此时业务系统应组合认证请求，通过浏览器重定向到 IAM 进行认证并申请 code。

组合认证请求（重定向地址）为 http://iam.paraview.cn/esc-sso/oauth2.0/authorize?client_id=fd51ce2b60e5514ab998&response_type=code&redirect_uri=http://app.com/callback&oauth_timestamp=1572232273705&state=1。

第二步：

IAM 接收请求后会进行登录检查，若未登录则会展示 IAM 登录页让用户进行认证。认证成功后生成 code，通过浏览器重定向到业务系统回调地址反馈 code，如已登录则直接生成 code，通过浏览器重定向到业务系统回调地址反馈 code。

假如此时 IAM 认证成功后，生成的 code 为“OC-154-TM4g3ud4OtlbeDgStMDeQ2ckbjcIKcIqTIL”，则携带 code 通过浏览器重定向到业务系统回调地址为 http://app.com/callback?code=OC-154-TM4g3ud4OtlbeDgStMDeQ2ckbjcIKcIqTIL。



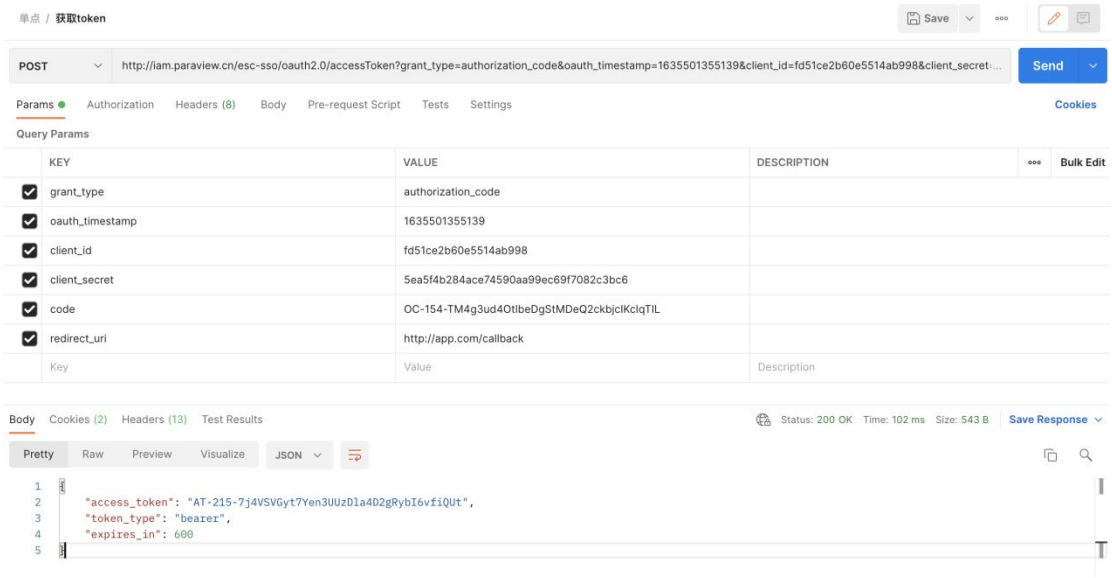
6.3 应用系统使用 code 换取 access_token

业务系统获取到 code 后，调用 IAM 平台 oauth2.0/accessToken 获取 token 接口，用 code 来换取 access_token。

请求 URL 为 http://iam.paraview.cn/esc-sso/oauth2.0/accessToken?grant_type=authorization_code&oauth_time

stamp=1635501355139&client_id=fd51ce2b60e5514ab998&client_secret=5ea5f4b284ace74590aa99ec69f7082c3bc6&code=OC-154-TM4g3ud4OtlbeDgStMDeQ2ckbjcIKcIqTIL&redirect_uri=http://app.com/callback。

postman 模拟调用如图所示：



接口响应：

{
"access_token": "AT-215-7j4VSVGyt7Yen3UUzDla4D2gRybI6vfiQUt",
"token_type": "bearer",
"expires_in": 600
}

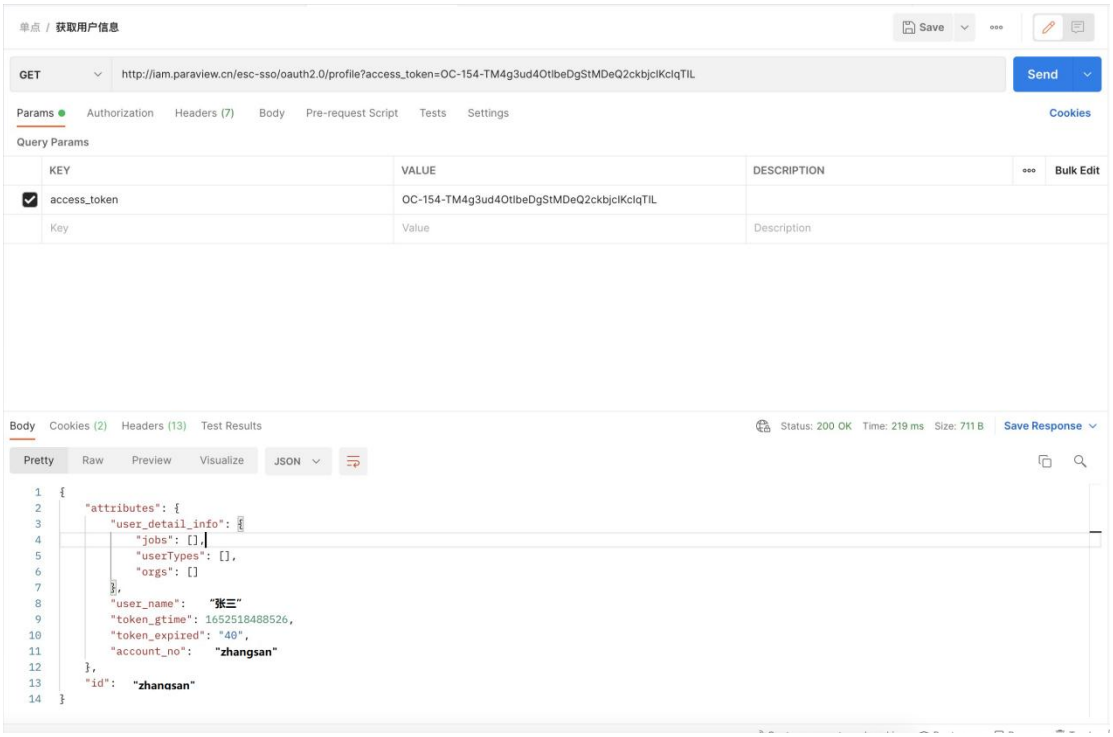
通过接口响应，获取 access_token 为“AT-215-7j4VSVGyt7Yen3UUzDla4D2gRybI6vfiQUt”。

6.4 应用系统使用 access_token 获取当前登录用户信息

各应用系统获取到 access_token 后，调用 IAM 平台 oauth2.0/profile 获取用户信息接口，使用 access_token 换取当前登录用户信息。

请求 URL 为 http://iam.paraview.cn/esc-sso/oauth2.0/profile?access_token=OC-154-TM4g3ud4OtlbeDgStMDeQ2ckbjcIKcIqTIL。

postman 模拟调用如图所示：



接口响应：


```
{
    "attributes": {
        "user_detail_info": {
            "jobs": [],
            "userTypes": [],
            "orgs": []
        },
        "user_name": "张三",
        "token_gtime": 1652515293525,
        "token_expired": "40",
        "account_no": "zhangsan"
    },
    "id": "zhangsan"
}
```


通过接口响应，获取当前登录账号为“zhangsan”。各应用系统匹配用户信息，建立会话，根据账号权限展示对应业务系统页面即可。

6.5 常见问题

6.5.1App 未找到子账号

进行 IAM 认证后页面显示：

表示该用户未开通此业务系统访问权限，联系对应管理员添加对应应用账号即可。

6.5.2error=invalid_grant

获取 code 后，使用 code 换取 access_token 时接口返回"error=invalid_grant"，表示 code 已失效，重新获取 code 即可。

6.5.3error=invalid_request

获取 code 后，使用 code 换取 access_token 时接口返回"error=invalid_request"，表示应用在组合请求地址时 redirect_uri 回调地址与提供给 IAM 系统做应用注册时的 redirect_uri 回调地址不一致，需保持一致。

6.5.4expired_accessToken

获取 access_token 后，使用 access_token 换取用户信息时接口返回"error=expired_accessToken"，表示 access_token 已过期，重新获取 access_token 即可。

6.5.5redirect_uri error.

进行 IAM 认证后页面显示：

表示应用在组合请求地址时 redirect_uri 回调地址与提供给 IAM 系统做应用注册时的 redirect_uri 回调地址不一致，需保持一致。

6.5.6client_id error.

进行 IAM 认证后页面显示：

表示应用在组合请求地址时 client_id 参数填写错误，需核实参数。

6.5.7unauthorized.

获取 code 后，使用 code 换取 access_token 时接口返回：

```
{
    "timestamp": "2022-05-14T17:25:09",
    "status": 401,
    "error": "Unauthorized",
    "message": "No message available",
    "path": "/esc-sso/oauth2.0/accessToken"
}
```

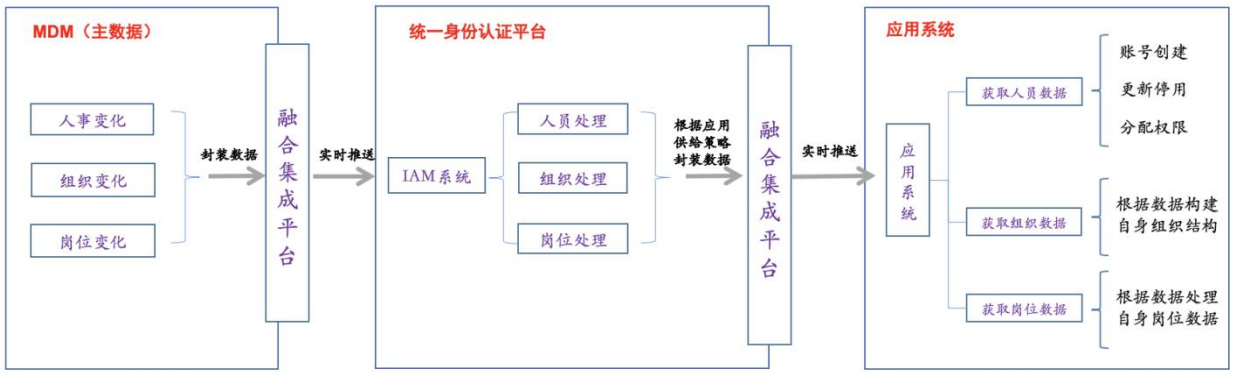
表示应用在调用接口时 client_id 参数或 client_secret 参数填写错误，需核实参数。

7　应用数据同步集成规范

7.1 概述

为实现集团统一账号管理，IAM 平台将作为集团各应用系统的基础数据源，为业务系统提供组织、人员、职位基础数据，用于各应用系统创建本系统账号体系。

对接 IAM 账号管理的应用各系统账号创建、更新、启用停用等内容，统一由 IAM 系统发起，具体流程如下：



1）IAM 与应用系统间的数据同步，IAM 作为数据发送方，为应用系统实时推送数据；

2）应用系统作为数据接收方，需按照 IAM 系统的集成规范开发对应数据接收接口。

注：

①以下数据同步接口调用方式为固定方式，数据属性可能会随着需求及项目推进做调整，调整方式为新增属性或使用扩展字段，不影响原有调用方式和数据属性。

②应用系统集成用户数据同步进行账号创建时，IAM 不做密码信息同步，应用方需按照本身初始密码规则创建账号初始密码，以备后续本地应急认证使用。

7.2 接口鉴权

7.2.1目的

为保证接口调用者身份合法性，应用系统需对自身数据接收接口进行调用鉴权。

7.2.2鉴权方式

jwt token

7.2.3鉴权方法

- 添加 JWT 依赖包

```
<dependency>
    <groupId>com.auth0</groupId>
    <artifactId>java-jwt</artifactId>
    <version>3.10.2</version>
</dependency>
```

- token 生成方法（IAM 系统生成）

```
String token = JWT.create().withIssuer(AppID).withIssuedAt(new Date()).withJWTId(UUID.randomUUID().toString()).sign(Algorithm.HMAC256(AppSecret));
```

- token 校验方法（应用方校验）

```
public void verify(String token, String secretKey) {
    StrUtil.removePrefix(token, "Bearer").trim();
    DecodedJWT decode = JWT.decode(token);
    int jwtTimeout = 60000;
    try {
        Date date = decode.getIssuedAt();
        JWTVerifier jwtVerifier = JWT.require(Algorithm.HMAC256(secretKey)).acceptIssuedAt((long)(jwtTimeout / 1000)).build();
        jwtVerifier.verify(token);
```

```
        } catch (JWTVerificationException var6) {
            log.error("Exception occurred:", var6);
        }
}
```

备注：

1. 允许的时间偏差建议为 60 秒 可以根据实际情况调整；
2. token 验证 需要去 Bearer 空格；
3. secretKey 在应用对接时由 IAM 进行颁发。

7.3 组织数据同步

7.3.1接口信息

接口名称： /org

请求方式： POST Content-Type: application/json

请求 Url： http://地址:端口/org?access_token= ACCESS_TOKEN

请求体示例：


```
{
    "addressCode": "",
    "incorporationTime": "",
    "internal": "",
    "orgName": "SL 天元上东城二店",
    "orgPath": "/京博集团组织结构/山东京博商联商贸有限公司/SL 经营管理部/SL 博兴二片区
/SL 天元上东城二店",
    "directorCode": "",
    "nature": "",
    "orgName1": null,
    "companyName": "",
    "orderNum": 100,
    "remark": null,
    "leaderCode": "",
    "parentCode": "081000017000",
    "directorName": "",
    "leaderName": "",
    "orgCode": "081000017100",
    "actionFlag": 1,
    "addressName": "",
    "abbr": "",
    "actionDesc": "管理员操作-修改组织",
    "status": 1
}
```

请求参数说明：

序号	IAM 属性名称	主数据字段	描述	类型	备注
1	orgCode	CODE	部门编码	String	
2	orgName	DESC1	组织名称的值	String	
3	addressCode	DESC10	地点的值	String	
4	addressName	DESC11	地点地址的值	String	
5	incorporationTime	DESC12	成立日期的值	String	
6	remark	DESC16	备注	String	
7	status	DESC17	组织状态的值	String	1 正常 0 停用
8	orderNum	DESC18	排序的值	String	
9	orgName1	DESC19	组织名称 1 的值	String	
10	companyName	DESC2	公司的值	String	
11	nature	DESC3	组织性质的值	String	
12	directorCode	DESC4	部门负责人的值	String	
13	directorName	DESC5	部门负责人姓名的值	String	
14	leaderCode	DESC6	部门分管领导的值	String	
15	leaderName	DESC7	部门分管领导姓名的值	String	
16	abbr	DESC8	组织简称的值	String	
17	internal	DESC9	内部/外部的值	String	
18	parentCode	PARENTCODE	父节点编码的值	String	
19	parentName	PARENTDESC	父节点名称的值	String	
20	orgPath	ORGPATH	组织全路径	String	

返回结果：

```
{
  "code":"0",
  "msg":"提示信息"
}
```

注意：返回 code 为 0 时，IAM 系统会认为下游系统已经处理组织成功，非 0 时认为下推失败，把错误信息放入 msg 返回，以下接口返回类似。

```
{
  "code":"-1",
  "msg":"组织不存在"
}
```

响应参数:

参数	类型	说明
code	string	“0”代表成功,其余均为失败
msg	string	处理结果提示信息

7.4 用户数据同步

7.4.1接口信息

接口名称: /user

请求方式: POST Content-Type: application/json

请求 Url : http://地址:端口/users?access_token= ACCESS_TOKEN

请求体示例:


```
{
   "englishName": "YunTian LAN",
   "gender": 0,
   "censusRegister": "山东省滨州市博兴县",
   "skillDuytName": null,
   "companyName": "山东邦维信息科技有限公司",
   "back": "否",
   "remark": "",
   "userTypes": [{"userType":"内部用户"}],
   "identityCode": "372328190010101010",
   "uid": "lanyuntian",
   "topDutyDesc": "",
   "officePhone": "",
   "managementDutyName": "无",
   "employmentNature": "合同工",
   "accountNo": "36549",
   "actionFlag": 1,
   "email": "weihao.wang@chambroad.com",
   "jobName": "高级 ERP 实施管理员",
   "companyCode": "077000000000",
   "hireDate": {"year":2014,"month":7,"day":7},
   "politicalStatus": "",
   "jobs": [
     {
         "code": "077000001000012",
         "orgName": "BWERP 实施部",
```

```
        "orgCode": "077000019000",
        "orgName1": "ERP 实施部",
        "name": "高级 ERP 实施顾问",
        "jobType": 1
    },
    {
        "code": "010004081012009",
        "orgName": "WL 数字化研究所",
        "orgCode": "010004081012",
        "orgName1": "数字化研究所",
        "name": "高级软件开发员",
        "jobType": 0
    },
    {
       "code": "001008100500005",
       "orgName": "KG 技术与创新科",
       "orgCode": "001008100500",
       "orgName1": "技术与创新科",
       "name": "技术架构师",
       "jobType": 0
    }
  ],
  "mobile": "13366666666",
  "levelName": "高级（员）工",
  "userName": "兰云天",
  "temporaryPost": "",
  "jobLevelType": "高级（员）工",
  "nationality": "",
  "actionId": 1778426544297918529,
  "orgs": [
     {
         "orgName": "BWERP 实施部",
         "orgCode": "077000019000",
          "orgName1": "ERP 实施部"
       },
       {
         "orgName": "WL 数字化研究所",
         "orgCode": "010004081012",
         "orgName1": "数字化研究所"
       },
       {
          "orgName": "KG 技术与创新科",
          "orgCode": "001008100500",
```

```
            "orgName1": "技术与创新科"
        }
    ],
    "actionDesc": "管理员操作-修改主帐号",
    "jobLevelName": "高级（员）工",
    "status": 1
}
```


请求参数说明：

序号	IAM 属性名称	主数据字段	描述	类型	备注
1	uid	CODE	主编码的值 (IAM 登录名)	String	人员主数据
2	userName	DESC1	姓名的值	String	人员主数据
3	hireDate	DESC16	入司时间的值	String	人员主数据
4	censusRegister	DESC17	籍贯的值	String	人员主数据
5	employmentNature	DESC18	用工性质的值	String	人员主数据
6	identityCode	DESC19	身份证号码的值	String	人员主数据
7	companyName	DESC2	公司的值	String	人员主数据
8	mobile	DESC21	手机的值	String	人员主数据
9	back	DESC22	是否二次入司的值	String	人员主数据
10	nationality	DESC29	国籍的值	String	人员主数据
11	orgCode	DESC3	部门编码的值	String	人员主数据
12	officePhone	DESC32	办公电话的值	String	人员主数据
13	email	DESC33	电子邮箱的值	String	人员主数据
14	remark	DESC38	备注的值	String	人员主数据
15	politicalStatus	DESC39	政治面貌的值	String	人员主数据
16	orgName	DESC4	部门名称的值	String	人员主数据
17	status		账号状态的值	String	1 正常 0 停用
18	managementDutyName	DESC47	管理职务的值	String	人员主数据
19	jobName	DESC5	职位的值	String	人员主数据
20	topDutyDesc	DESC50	最高职务说明的值	String	人员主数据
21	orgName1	DESC51	部门名称 1 的值	String	人员主数据
22	englishName	DESC55	英文名的值	String	人员主数据
23	jobLevelName	DESC56	职级的值	String	人员主数据
24	jobLevelType	DESC57	职级分类的值	String	人员主数据
25	temporaryPost	DESC6	挂职岗位的值	String	人员主数据
26	skillDuytName	DESC7	技能职务的值	String	人员主数据
27	levelName	DESC8	层级的值	String	人员主数据
28	gender	DESC9	性别的值	String	人员主数据 0 男 1

					女
30	companyCode	DESC3	公司编码的值	String	人员职位主数据
31	code	DESC7	职位编码的值	String	人员职位主数据
32	name	DESC8	职位名称的值	String	人员职位主数据
33	jobType	DESC9	是否主职的值	String	人员职位主数据
34	accountNo		应用系统登录账号	String	默认与 uid 一致

返回结果:

```
{
   "code":"0",
   "msg":"提示信息"
}
```

注意：返回 code 为 0 时，IAM 系统会认为下游系统已经处理账号成功，非 0 时认为下推失败，把错误信息放入 msg 返回，以下接口返回类似。

```
{
   "code":"-1",
   "msg":"账号不存在"
}
```

响应参数:

参数	类型	说明
code	string	“0”代表成功,其余均为失败
msg	string	处理结果提示信息

7.5 职位数据同步

7.5.1接口信息

接口名称: /job

请求方式: POST Content-Type: application/json

请求 Url : http://地址:端口/job?access_token= ACCESS_TOKEN

请求体示例:

```
{
```

```
    "companyCode": "079000000000",
    "code": "079000000039004",
    "companyName": "山东京博中聚新材料有限公司",
    "passagewayName": "经营",
    "dutyCode": "3222",
    "jobCode": "315",
    "sequenceName": "市场",
    "jobLevel": "高级经理",
    "passagewayCode": "2975",
    "sequenceCode": "2960",
    "postName": "市场技术经理",
    "name": "高级市场技术经理",
    "actionFlag": 1,
    "duty": "无",
    "actionId": 1778426544297919413,
    "postCode": "3166",
    "orgs": [
      {
        "orgName": "ZJ 市场技术部",
        "orgCode": "079000000039"
      }
    ],
    "dutyLevel": "19",
    "actionDesc": "管理员操作-修改岗位",
    "status": 1
}
```


请求参数说明：

序号	IAM 属性名称	主数据字段	描述	类型	备注
1	code	CODE	主编码的值	String	
2	name	DESC1	职位名称的值	String	
3	jobLevel	DESC10	职位等级名称的值	String	
4	orgCode	DESC11	部门编码的值	String	
5	orgName	DESC12	部门名称的值	String	
6	dutyCode	DESC15	职务等级编码的值	String	
7	duty	DESC16	职务等级名称的值	String	
8	companyCode	DESC17	公司编码的值	String	
9	companyName	DESC18	公司名称的值	String	
10	dutyLevel	DESC19	职级排序号的值	String	
11	status	DESC2	状态的值	String	
12	sequenceCode	DESC3	序列编号的值	String	

13	sequenceName	DESC4	序列名称的值	String	
14	passagewayCode	DESC5	通道编号的值	String	
15	passagewayName	DESC6	通道名称的值	String	
16	postCode	DESC7	岗位编码的值	String	
17	postName	DESC8	岗位名称的值	String	
18	jobCode	DESC9	职位等级编码的值	String	

返回结果:

```
{
   "code":"0",
   "msg":"提示信息"
}
```

注意：返回 code 为 0 时，IAM 系统会认为下游系统已经处理职位成功，非 0 时认为下推失败，把错误信息放入 msg 返回，以下接口返回类似。

```
{
   "code":"-1",
   "msg":"职位不存在"
}
```

响应参数:

参数	类型	说明
code	string	“0”代表成功,其余均为失败
msg	string	处理结果提示信息

附件清单:

1、应用对接申请表