# 合肥研究院统一身份认证平台接入指南

## 平台说明

合肥研究院统一身份认证平台由信息中心研发维护，汇总研究院各类人员（职工、学生、自聘员工等）基础信息，面向研究院各类业务系统，提供统一的用户登录和身份认证服务。

统一身份认证平台融合院ARP系统、科大学生系统、本地系统等多个数据源，打通科技云通行证、科大认证系统、研究院企业微信等多个渠道，提供满足研究院多类型需求的、一站式的系统服务。

统一身份认证平台对接多个业务系统，集中解决账号注册、密码设置、身份信息维护等问题，能够显著提升用户体验。统一身份认证平台为研究院每个用户分配唯一的身份标示，贯穿于各业务系统，能够打破信息孤岛，形成一致有效的信息流，便于实现跨业务流程的统筹分析和综合管理。

## 接入步骤

### 准备条件

接入系统应已建设完成（或基本完成），在“系统注册”环节提供运行（或预览）链接地址，作为注册审核的必要条件。

若接入系统为网站，应先完成网站备案。备案操作方法：“研究院企业微信--工作台--审批--网站备案申请”。

### 系统注册

填写“研究院企业微信--工作台--审批--统一身份认证平台接入申请”，确定系统名称、简介、回调地址等信息，经系统负责人（或网站负责人）和处室领导审核后，由信息中心审核办理。

注册完成后，平台为系统分配id、secret等参数，作为接入平台的凭证，请妥善保管并防止外泄，以避免系注册信息被冒用。

### 系统接入

平台按照标准OAuth 2.0协议，实现授权码模式（authorization code）下用户对客户端（即业务系统）的授权信息访问流程。具体步骤如下：

* + 1. 认证链接。

平台认证链接为[https://passport.hfcas.ac.cn/oauth2/authorize](https://passport.hfcas.ac.cn/oauth2/authorize%EF%BC%8C) 同时接受客户端编号（client\_id）、客户端状态（client\_state）和回调地址参(redirect\_uri)参数，例如
[https://passport.hfcas.ac.cn/oauth2/authorize?client\_id=clientid&state=clientstate&redirect\_uri=http://yoursitepath/callback](https://passport.hfcas.ac.cn/oauth2/authorize?client_id=clientid&state=clientstate&redirect_uri=http:/yoursitepath/callback)

[平台自动处理该链接请求，提示用户是否同意授权该客户端（即系统）。若用户同意授权，则携带授权码（以下简称为code）重定向至redirect\_uri地址，例如
http://yoursitepath/callback?code=yourcode&state=clientstate。](https://passport.hfcas.ac.cn/oauth2/authorize?client_id=clientid&state=clientstate&redirect_uri=http:/yoursitepath/callback)

[若用户不同意授权，则关闭相关页面，终止流程。](https://passport.hfcas.ac.cn/oauth2/authorize?client_id=clientid&state=clientstate&redirect_uri=http:/yoursitepath/callback) 平台根据注册信息，判断client\_id和redirect\_uri的正确性，请保证该参数值与注册信息一致。重定向平台原值返回state，以方便系统业务处理。

另外，平台暂只提供用户基本信息授权访问，所以scope默认为basic，认证链接中无需提供该参数（若提供，则被忽略）。

* + 1. 获取授权码

系统处理回调请求，提取code参数，即为用户授权码。

* + 1. 换取令牌

系统在后台发送post请求至
<https://passport.hfcas.ac.cn/oauth2/token>，携带客户端id、secret、grant\_type、code和redirect\_uri参数信息，换取令牌（token）。例如：



若参数正确，平台返回令牌json数据，具体如下：



若参数错误，平台返回错误提示，具体如下：



* + 1. 刷新令牌

若令牌已过期，可使用refresh\_token获取新令牌。与code换取令牌类似，请求<https://passport.hfcas.ac.cn/oauth2/token>，携带客户端id、secret、grant\_type、code和redirect\_uri参数信息，刷新令牌（token）。例如：



返回令牌信息或错误提示与上节一致。

* + 1. 请求用户信息

系统请求https://passport.hfcas.ac.cn/oauth2/userinfo，采用bearer认证方式携带访问令牌，获取用户信息。例如：



若令牌正确，平台返回用户信息json数据，具体如下：



若令牌错误，平台返回错误提示，具体如下：



### 系统注销

填写“研究院企业微信--工作台--审批--统一身份认证平台接入注销”，确定系统名称、注销原因等信息，经系统负责人（或网站负责人）和处室领导审核后，由信息中心审核办理。

注销完成后，平台系统分配的id、secret等参数立即失效，不再具有访问平台用户信息的权限。

## 注意事项

### 用户隐私保护

平台返回的用户信息包括用户姓名、邮箱、单位、部门等数据，属于用户隐私信息，请接入系统妥善处理，防止隐私数据滥用或外泄。

### 网络安全防护

接入系统应具有较好的网络攻击防护能力，避免因本身安全问题，被动攻击统一身份认证平台或其他业务系统。

## 联系方式

若平台接入过程中遇到问题，请联系信息中心协助解决：电话61220，邮箱zxzhang@hfcas.ac.cn。