广 东 省 生 态 环 境 信 息 化 标 准

生态环境智慧云平台系统集成规范
第1部分：统一身份认证

（征求意见稿）

2020-XX-XX 发布　　2020-XX-XX 实施

广 东 省 生 态 环 境 厅 发布

目　次

前　言 I
1.范围 1
2.规范性引用文件 1
3.术语和定义 1
4.接入流程 2
4.1 接入要求 2
4.1,1　统一身份认证 2
4.1.2 单点登录 2
4.1.3　默认权限集成 2
4.2 接入流程 2
4.2.1 概述 2
4.2.2 接入前准备 2
4.2.3 接入申请 3
4.2.4 接入核准 3
4.2.5 接入改造 3
4.2.6 接入联调 3
5.认证服务 3
5.1 业务流程图 3
5.2 认证接口调用 4
5.3 接口规范 4
5.3.1 获取授权码接口 4
5.3.2　授权码模式获取 access_token 5
5.3.3　校验 token 有效性 5
5.3.4 获取登录用户基本信息 6
5.3.5 获取登录用户详细信息 7
5.3.6 用户退出 10

前　言

《广东省生态环境厅智慧云平台系统集成规范》包括 2 个部分：

——第 1 部分：统一身份认证；

——第 2 部分：门户集成。

本规范是《广东省生态环境厅智慧云平台系统集成规范》的第 1 部分，介绍了广东省生态环境厅智慧云平台（以下简称智慧云平台）统一身份认证、单点登录、默认权限集成等接入要求和接入流程，便于各类读者查询、定位、理解，使各业务系统能够快速接入智慧云平台。

1. 范围

本规范作为广东省生态环境厅所有已运行系统或新建项目做集成的参考。

2. 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适 用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 1.1	标准化工作导则 第 1 部分：标准的结构和编写规则
HJ_T 416	环境信息术语
HJ 718	环境信息共享互联互通平台总体框架技术规范
GDZW 0010-2019	广东省统一身份认证平台接入规范（政务侧）

3. 术语和定义

3. 1

身份 Identity

指自然人或法人在智慧云平台中的身份标识，是智慧云平台授权的依据。

3. 2

用户 User

智慧云平台各业务系统的使用人员。

3. 3

身份信息 Identity information

指人员身份的组成内容，身份信息包括姓名、身份证号、手机号等。

3. 4

业务系统 The business system

指已集成或待集成到智慧云平台中的业务系统。

3. 5

统一身份认证 Unified identification

用户通过使用同一套用户凭证，可访问所有统一认证平台上与该用户身份对应的授权网络应用的过程。

3. 6

单点登录 Single sign-on

在多个业务系统中，平台用户登录一次就可以访问所有相互信任平台业务系统的过程。

3. 7

信任传递 Trust transfer

实现用户、业务系统的强身份鉴别、跨域条件下的信任传递。本规范特指在智慧云平台统一身份认证中心将已登录凭证传递到业务系统完成登录的过程。

3. 8

凭证 Credentials

通过门户认证的用户身份的合法标识。

4. 接入流程

4.1 接入要求

智慧平台集成规范要求业务系统完成如下集成工作：统一身份认证、单点登录、默认权限集成。

4.1.1 统一身份认证

智慧云平台通过 OAuth2.0 认证协议，提供统一认证服务，业务系统需要通过智慧云平台实现线上申请、审核、接入管理。

4.1.2 单点登录

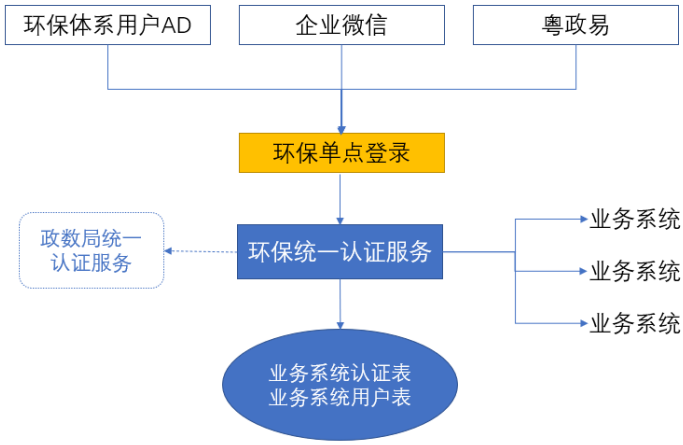

图 1 登录示意图

智慧云平台支持企业微信、广东省统一身份认证（政务侧）、环保 AD 等认证方式，为业务系统提供单点登录、统一认证服务、新用户注册、密码找回等认证相关服务。业务系统只需完成一次与平台的统一认证集成，就具备与其他业务系统实现单点登录，企业微信扫码、粤政易扫码、环保 AD 账号、广东省统一身份认证（政务侧）等登录功能。

4.1.3 默认权限集成

为确保认证登录后各业务系统能正常访问，各业务系统都需要配置一个默认角色。

4.2 接入流程

4.2.1 概述

接入工作流程主要包括接入前准备、接入申请、接入核准、接入改造、接入联调等五个阶段。

4.2.2 接入前准备

申请节点按以下要求进行准备：

a) 各节点应明确 IP 地址，制定部署方案，明确节点部署位置，确保服务器部署在安全区域内；

b) 制定接入方案，描述对接环境和应用系统，描述接口调用方案，描述 IP 网络拓扑、IP 地址、域名，描述安全防护方案。云平台、负载均衡设备、CDN 服务应单独详细描述；

c）各节点应具备信息安全等级保护二级（或以上）的安全防护能力；

d）约定接入各方的工作职责。

4.2.3 接入申请

各节点向智慧云平台申请接入，申请时根据需要包含以下内容：

a）业务系统接入广东省生态环境厅智慧云平台申请；

b）其他必须的信息。

4.2.4 接入核准

对申请节点提供的技术信息和接入方案进行评测后，智慧云平台核准是否接入，核准后节点建立以下接入要素：

申请节点的接入基础（申请账号、注册应用、获取分配的密钥和 KEY、配置回调地址等）；

b）其它必须的信息。

4.2.5 接入改造

申请节点应遵从本标准，实现接入智慧云平台统一身份认证、单点登录和默认权限集成的改造工作。

4.2.6 接入联调

应遵从本标准，申请节点与智慧云平台展开统一身份认证相关业务进行联调。

5. 认证服务

5.1 业务流程图

普通用户访问业务系统，通过统一认证服务流程如下图所示：

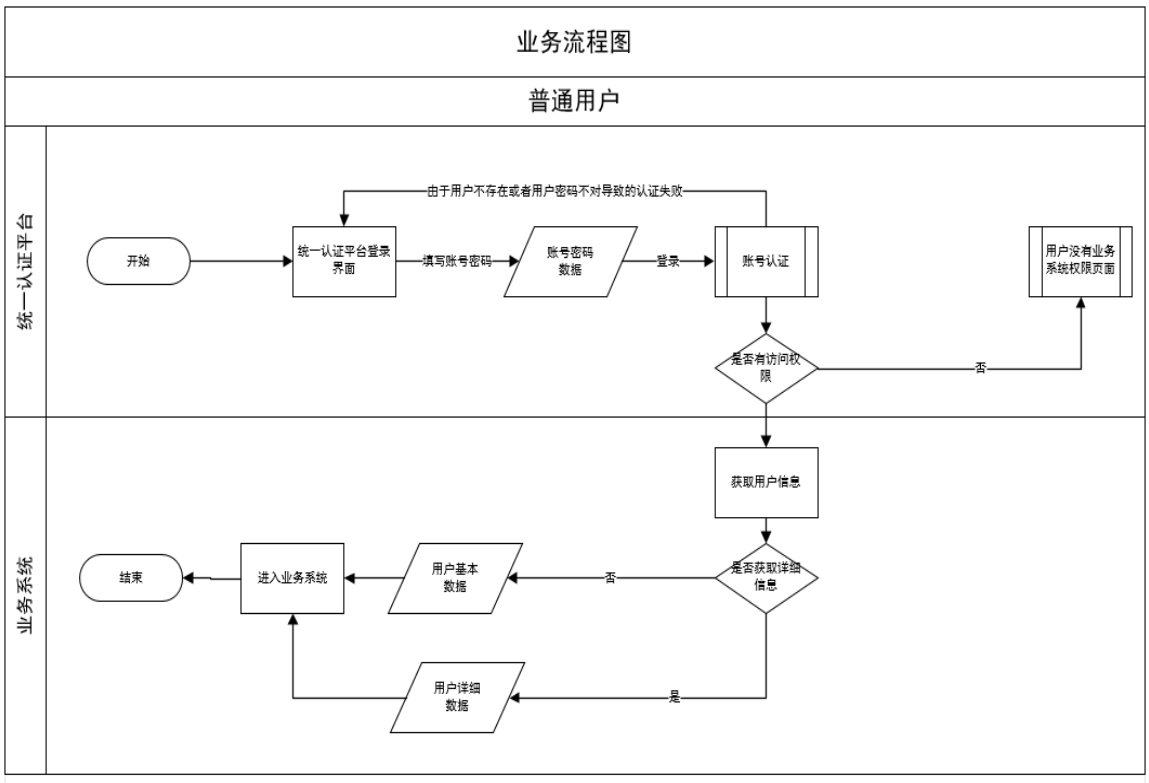

图 2 业务流程图

5.2 认证接口调用

1、获取 code

https://it.gdeei.cn/oauth/oauth/authorize?client_id="+clientId+"&response_type=code&redirect_uri="+redirectUrl+"&scope=all"

如果用户没有登录，则会跳转到统一身份认证登录页面。如果用户已登录，调用接口后，会定向到 redirect_uri，授权码会作为它的参数

2、获取 access_token

https://it.gdeei.cn/oauth/oauth/token?code="+code+"&grant_type=authorization_code&client_secret="+clientSecret+"&redirect_uri="+redirectUri+"&client_id="+clientId

3、获取用户信息

此时统一认证服务会根据该认证用户权限信息判断，确定是否返回用户信息。如果该用户不属于该应用系统，会跳转到无权限页面。否则返回用户数据以及进入系统。

获取当前登录用户基本信息：

https://it.gdeei.cn/oauth/user/simple?access_token="+access_token

获取当前登录用户详细信息包含配置的菜单权限数据：

https://it.gdeei.cn/oauth/user/detail?access_token="+access_token

5.3 接口规范

5.3.1 获取授权码接口

表 1 获取授权码接口表

接口功能	获得授权码
url	https://it.gdeei.cn/oauth/oauth/authorize
参数	scope ： 默认为 all。
	client_id ： 表示系统的 KEY，必选项
	redirect_uri ： 表示重定向 URI,其值为系统在统一配置平台里面配置的回调地址。code 授权码会当成 redirect_uri 的参数返回。
	response_type 表示授权类型，必选项，此处的值固定为 code
	state:自定义字符串参数，非必填项。重定向时也会返回该参数
	scope ： 默认为 all。
	client_id ： 表示系统的 KEY，必选项
	redirect_uri ： 表示重定向 URI,其值为系统在统一配置平台里面配置的回调地址。code 授权码会当成 redirect_uri 的参数返回。
	response_type 表示授权类型，必选项，此处的值固定为 code
	state:自定义字符串参数，非必填项。重定向时也会返回该参数
https 请求方式	GET
说明	

说明：打开连接

1、没登录。跳转到统一认证登录界面，输入账号密码认证通过后，会回调你传递的回调地址 redirect_uri，并将 code 放在其后。注意 code 只能用一次！

2、已登录。会回调你传递的回调地址 redirect_uri，刷新 code 并将 code 放在 URL 后。

如：https://manhuaceshi.dev.cn/?code=MwvK33（格式 redirect_uri?code=授权码）

如：https://manhuaceshi.dev.cn/?code=MwvK33&state=XXXXX（如果有 state 参数会原样返回）

5.3.2 授权码模式获取 access_token

表 2 以授权码模式获取 access_token 接口

接口功能	通过授权码获得访问令牌 access_token
url	https://it.gdeei.cn/oauth/oauth/token
参数	client_id ：表示客户端的 ID，必选项
	client_secret ：表示客户端的密钥，必选项
	code ：授权码
	grant_type 固定为 authorization_code
	redirect_uri ：认证完成并且用户对应用授权后返回的地址。

返回值	access_token ：访问令牌。
	token_type：获得的Token类型，Bearer
	例如：
	{
	"access_token":"114a00ef-47ba-432e-be67-4ff76375aaf5",
	"token_type": "bearer",
	"expires_in": 17822,
	"scope": "all"
	}

https 请求方式	POST
说明	

5.3.3 校验 token 有效性

表 3 校验 token 有效性接口

接口功能	校验 token 有效性接口
url	https://it.gdeei.cn/oauth/oauth/check_toke
参数	token ：token 的值，必选项
返回值	scope ：访问权限。 active：token有效性。 exp：失效时间 client_id：客户端id 返回正常，状态码200 例如： { "scope": ["all"], "active": true, "exp": 1579006198,

	"client_id": "xxxxx"
	}
	返回异常，非200状态码
	例如：
	{
	"error": "invalid_token",
	"error_description": "Token was not recognised"
	}

https 请求方式	GET
说明	

5.3.4 获取登录用户基本信息

表 4 获取用户基本信息表

接口功能	通过访问令牌 access_token 获得用户基本信息
url	https://it.gdeei.cn/oauth/user/simple
参数	access_token ：访问令牌

返回值	1、用户具有系统访问权限，返回数据示例：
	{
	"message": "操作成功",
	"data": {
	"user_code": "user1",#用户账号
	"user_name": "xxx",#用户名称
	#当前登录系统信息
	"移动应用": {
	"code": "ConfigCenter",#系统编码
	"name": "统一配置",#系统名称
	"移动应用_type": "platform",#系统类型
	"url": "https://172.20.105.204:8083",#系统地址
	"icon": "2c94e94c6b45dcab016b4614fcf5000a",#系统图标 ID
	"version": "V1.0",#系统版本
	"移动应用_desc": "采用云服务形可以避免同时开发这些模块。",#系统描述
	"is_admin": 1,#当前用户是否是系统的管理员
	"state": 1#系统状态
	},
	#用户的企业信息，没有则为 null
	"ent": {
	"id": "2c94e94c6bbac066016bc0c6d30e0030", #企业 ID
	"ent_name": "周之家",#企业名称
	"legal": "周代表",#企业法人代表
	"capital": "999",#企业注册资金
	"setup": "2019-07-04",#企业成立日期
	"register": "ASDFGHJKL",#统一社会信用代码
	"busi_state": null,#企业经验状态
	"ent_type": null,#企业类型
	"ein": null,#企业税号
	"busi_scope": null,#企业经营范围
	"province": "广东省",#企业所在身份
	"city": "广州市",#企业所在城市
	"address": "小新塘",#企业地址
	"contact": "周展贵",#企业联系人

	"contact_tel": "13660111727",#企业联系电话
	"state": 1,#企业状态
	"is_admin": 1 #当前登录用户是否是企业管理员
	},
	#用户信息
	"user": {
	"code": "user1",#用户账号
	"name": "XXX",#用户名称
	"email": "13@qq.com",#用户邮件
	"mobi_tel": "",#电话
	"user_sex": null,#性别
	"user_tel": "",#手机
	"user_addr": "北京市,北京市市辖区,小新塘123",#联系地址
	"idCard": null#身份证
	}
	},
	"status": 200,
	"time": "2019-09-29 03:06:09"
	}
	
	2、用户不具有系统访问权限，跳转到用户没有访问权限页面

https 请求方式	JSON
说明	

5.3.5 获取登录用户详细信息

表 5 获取用户详细信息表

接口功能	通过访问令牌 access_token 获得用户详细信息，包括菜单权限数据。
url	https://it.gdeei.cn/oauth/user/detail
参数	access_token ： 访问令牌

返回值	{
	"message": "操作成功",
	"data": {
	"user_code": "XXX", #账号
	"user_name": "XXXX", #账号名称
	"is_admin": false, #是否是移动应用的管理员
	#移动应用信息
	"移动应用": {
	"code": "XX",
	"name": "XX资源目录",
	"移动应用_type": "project",
	"url": "https://172.20.105.204:8085",
	"icon": "2c94e94c6b45dcab016b49c6e33a0013",
	"version": "V1.0",
	"移动应用_desc": "资源目录",
	"is_admin": 0,
	"state": 1
	},
	#用户信息
	"user": {
	"code": "XXX",
	"name": "XXXX",
	"email": "13@qq.com",

```
                "mobi_tel": "",
                "user_tel": "",
                "user_addr": "北京市,北京市市辖区,小新塘123"
            },
            #企业信息
            "ent": {
                "id": "2c94e94c6bbac066016bc0c6d30e0030",
                "ent_name": "X之家",
                "legal": "周XX",
                "capital": "999",
                "setup": "2019-07-04",
                "register": "ASDFGHJKL",
                "province": "广东省",
                "city": "广州市",
                "address": "小新塘",
                "contact": "XXX",
                "contact_tel": "13660111727",
                "state": 1,
                "is_admin": 1
            },
            #机构信息
            "org": {},
            #部门信息
            "dept": {
                "org_id": "2c94e94c6c09493f016c29db8b730058",
                "direct_id": "",
                "pid": "root",
                "area_id": "abcde38bd6904ce9a27983834c5ddd12",
                "code": "ZXLD",
                "name": "中心领导",
                "tel_phone": "",
                "leader": "",
                "dept_desc": "",
                "state": 1
            },
        #默认角色信息
        "role": {
            "name": "角色B",
            "code": "JRB",
            "org_id": "2c94e94c6c09493f016c29db8b730058",
            "dept_id": "",
            "is_admin_role": 0,
            "state": 1
        },
            #角色json数据
            "roleJson": {
            "JRA": [
                {
                    "code": "Catalog-check",
                    "menu_type": 1,
                    "children": [],
                    "name": "我的审核",
                    "icon": "fa fa-arrows",
                    "pid": "root",
                    "id": "ff808081683d3cc301683d68003a0001",
                    "url": "移动应用ly/移动应用ly"
                },
                {
                    "code": "zyml",
```

```
                        "menu_type": 1,
                        "children": [
                            {
                                "code": "ztgl",
                                "menu_type": 1,
                                "children": [],
                                "name": "主题管理",
                                "icon": "fa fa-area-chart",
                                "pid":
"ff808081683d3cc301683d6843330002",
                                "id":
"ff808081683d3cc301683d6895070003",
                                "url": "theme\\themeList"
                            },
                            {
                                "code": "zygl",
                                "menu_type": 1,
                                "children": [],
                                "name": "资源管理",
                                "icon": "fa fa-at",
                                "pid":
"ff808081683d3cc301683d6843330002",
                                "id":
"ff808081683d3cc301683d6902ea0004",
                                "url": "info/infoManger"
                            }
                        ],
                        "name": "资源目录",
                        "icon": "fa fa-archive",
                        "pid": "root",
                        "id": "ff808081683d3cc301683d6843330002",
                        "url": ""
                    }
                ],
                "JRB": []
            },

    #用户在平台具有的全部角色信息
            "roles": [
                {
                    "name": "角色B",
                    "code": "JRB",
                    "org_id": "2c94e94c6c09493f016c29db8b730058",
                    "dept_id": "",
                    "is_admin_role": 0,
                    "state": 1
                },
                {
                    "name": "角色A",
                    "code": "JRA",
                    "org_id": "2c94e94c6c09493f016c29db8b730058",
                    "dept_id": "",
                    "is_admin_role": 0,
                    "state": 1
                }
            ],
            "roleMenus": [
                {
                    "code": "Catalog-check",
```

	"menu_type": 1,
	"children": [],
	"name": "我的审核",
	"icon": "fa fa-arrows",
	"pid": "root",
	"id": "ff808081683d3cc301683d68003a0001",
	"url": "移动应用ly/移动应用ly"
	},
	{
	"code": "zyml",
	"menu_type": 1,
	"children": [
	{
	"code": "ztgl",
	"menu_type": 1,
	"children": [],
	"name": "主题管理",
	"icon": "fa fa-area-chart",
	"pid": "ff808081683d3cc301683d6843330002",
	"id": "ff808081683d3cc301683d6895070003",
	"url": "theme\\themeList"
	},
	{
	"code": "zygl",
	"menu_type": 1,
	"children": [],
	"name": "资源管理",
	"icon": "fa fa-at",
	"pid": "ff808081683d3cc301683d6843330002",
	"id": "ff808081683d3cc301683d6902ea0004",
	"url": "info/infoManger"
	}
	],
	"name": "资源目录",
	"icon": "fa fa-archive",
	"pid": "root",
	"id": "ff808081683d3cc301683d6843330002",
	"url": ""
	}
	]
	},
	"status": 200,
	"time": "2020-07-29 05:01:20"
	}

https 请求方式	JSON
说明	

5.3.6 用户退出

表 6 用户退出接口

接口功能	用户退出。**只能通过页面请求重定向才能有效**
url	https://it.gdeei.cn/oauth/oauth/logout

参数	callback ： 登出后需要跳转的地址
返回值	无
https 请求方式	
说明	