**统一身份认证系统**

**应用接入**

**标准规范**

版本历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本/状态 | 作者 | 参与者 | 起止日期 | 备注 |
| 编目 | 朱德文 |  | 2018-6-23 | 初始做成 |
| 修改 | 赵北辰 |  | 2018-11-8 | 针对REST接口中，自然人注册，法人注册，自然人信息修改，法人信息修改，密码修改以及登录六个接口的改动 |
| 增加 | 赵北辰 |  | 2018-11-20 | 增加了四个用于添加和查询邮寄地址的REST接口 |
| 修改 | 赵北辰 |  | 2019-03-27 | 修改用于全区对接，增加全区对接内容 |
| 修改 | 赵北辰 |  | 2019-04-02 | 细化了REST接口错误代码的种类，移除了部分发送短信和短信验证接口 |
| 增加 | 赵北辰 |  | 2019-6-12 | 增加自然人，法人，社保，公积金四个实名核验接口 |
| 增加 | 赵北辰 |  | 2019-6-14 | 增加出入境证件接口 |
| 修改 | 赵北辰 |  | 2019-8-1 | 针对之前遗漏的细节，做了更详细的补充描述 |
| 增加/修改 | 赵北辰 |  | 2019-10-30 | 更新认证接口，旧的接口可能已不可用。另外增加【大厅注册接口】 |
| 删除 | 赵北辰 |  | 2019-11-22 | 移除认证接口 |
| 添加 | 赵北辰 |  | 2019-12-23 | 增加里法人代理人的字段描述 |
| 添加 | 赵北辰 |  | 2020-7-21 | 针对对接方经常疑惑的点，增加了描述 |

目录

[一、 统一认证系统说明 3](#_Toc4592802)

[二、 接入规范 4](#_Toc4592803)

[三、 第三方应用编写 7](#_Toc4592804)

[四、 多个第三方应用的交互 11](#_Toc4592805)

[五、 总结 14](#_Toc4592806)

[六、 附录 16](#_Toc4592807)

# 统一认证系统说明

## 简介

统一认证系统主要为全自治区提供统一的用户注册、登录认证以及实名核验功能，解决用户在办理不同地区的事项时需要多点注册，多次认证所导致的个人信息孤岛问题。促进互联网+政务服务深入开展，支撑政务的全程网办。建立后端权威、前端可信的认证体系，服务自然人和法人 “一地注册、各地互认”和“一次认证、全网通办”。通过“统一认证”和“信任传递”实现“单点登录，全网通办”。

# 接入规范

当进行注册、登录、登出等时，分别访问以下网址：

对接方易错点：下方所有接口地址都自带一个sso，而统一认证地址本身也带一个sso，例如测试环境地址为<http://10.12.23.141:8081/sso>，也就说拼接完地址中有**两个sso**！！例如<http://10.12.23.141:8081/sso>/sso/login

1、统一注册（用来访问统一认证注册页面）

https://统一身份认证地址/sso/register?utype=【用户类型代码】&client\_id=【接入应用系统接入代码】&goto=【接入应用保留参数】

补充：【用户类型代码】：0 – 自然人 1 – 法人

2、统一登录（用来访问统一认证登录页面

https://统一身份认证地址/sso/login?utype=【用户类型代码】&client\_id=【接入应用系统接入代码】&goto=【接入应用保留参数】

3、统一登出

**登出场景一**：第三方网站在登出按钮上绑定该地址

http://统一身份认证地址/sso/logout?utype=【用户类型代码】&client\_id=【接入应用系统接入代码】&goto=【登出后跳转地址】

用户点击后，实现当前网站和统一身份认证系统的登出。

**登出场景二**：例子：当前有A，B两个系统与统一认证对接，并且已经登录。在A站点击登出后，统一认证会调用B网站登出地址，最后统一认证登出。

**场景解析和对接注意事项**：统一身份认证登出后，会调用当前已经登录的其它信任平台的登出地址，完成统一登出。该登出地址必须为POST方法，且会由统一身份认证服务器后台直接调用，所以对接平台需要注意Session跨域的问题，防止找不到Session导致的注销失败。登录时统一身份认证会给第三方应用传递统一身份认证SessionID作为标识，参数名为SSOSign（登出时也会传），第三方应用与自身SessionID绑定后，方便统一登出时销毁Session。

4、找回密码：（用来访问统一认证忘记密码页面）

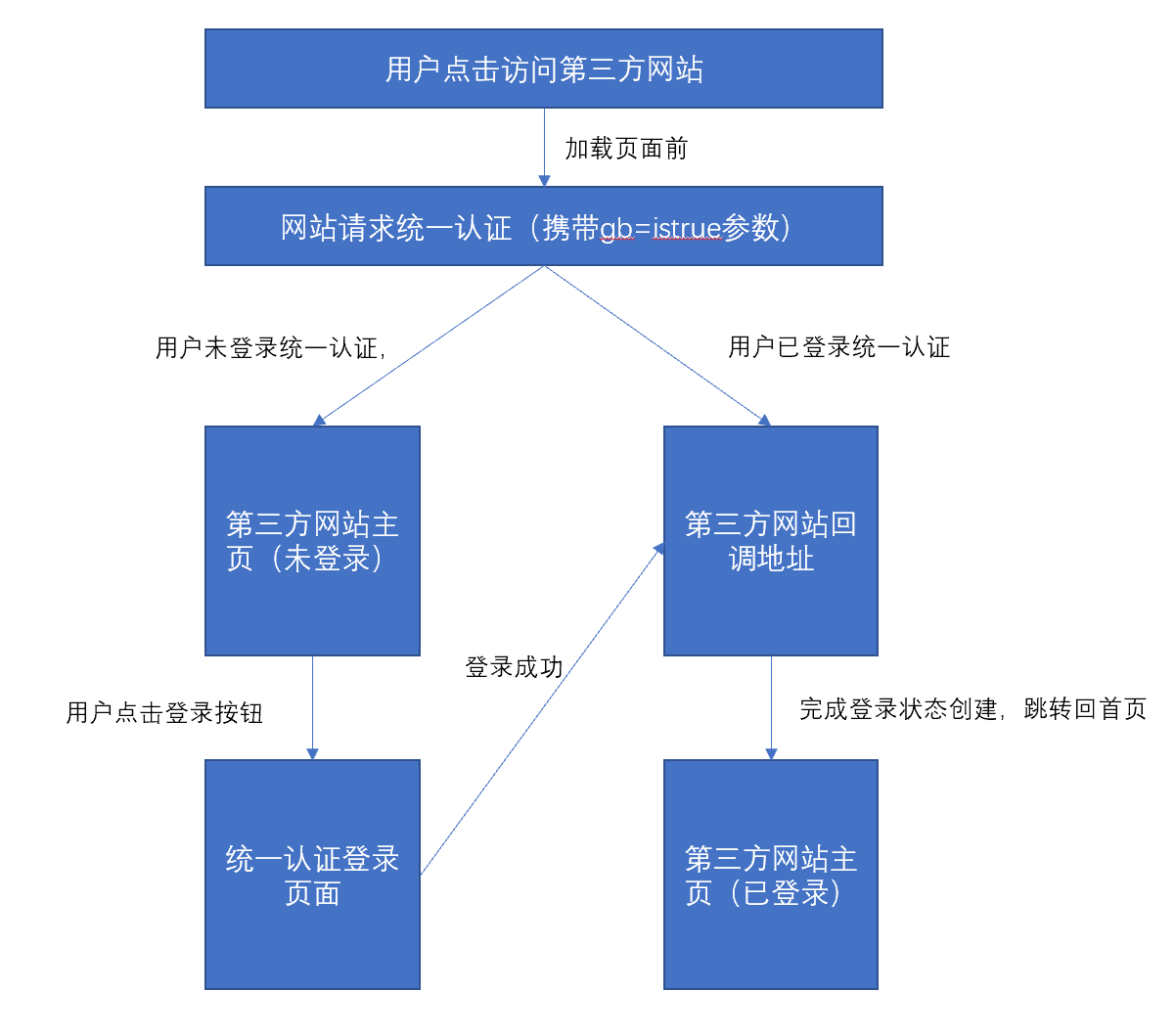
https://统一身份认证地址/sso/forgot?utype=【用户类型代码】&client\_id=【接入应用系统接入代码】&goto=【接入应用系统跳转地址】

5、用户信息主页：（用来访问统一认证用户中心页面）

https://统一身份认证地址/sso/main?utype=【用户类型代码】&client\_id=【接入应用系统接入代码】&goto=【保留参数】。这里传输client\_id和goto，用来方便用户在统一认证系统完成操作后，点击页面返回按钮返回第三方系统。注意：这里会返回第三方系统的回调地址，而不会直接返回goto地址。

6、信任传递

信任传递的实现需要对接平台进行改造，其流程为：在对接平台加载主页之前，先请求一次统一身份认证的登录地址（就是上述统一登录的地址，但是需要加上gb=istrue 参数，这样才会自动返回，否则如果没有登录，则会停留在登录页面），如果已经有登录状态，统一身份认证会直接返回用户信息，对接平台可直接创建自己的登录状态，然后加载页面。如果没有检测到登录状态，系统会返回对接平台的应用主页，注意：此时对接平台需检测返回请求是否包含record字段（由统一身份认证系统返回，作为已经请求过的标识），检测到后，证明已经请求过统一身份认证，即可正常加载页面，否则会导致页面递归调用。另外：该功能要做成可开关式，防止国办出现故障，影响自治区系统登录



**补充：**

【统一认证中心地址】为统一身份认证系统地址，联调时使用测试环境地址，上线后更换为生产环境地址。

utype：为用户类型（0：自然人；1：法人），

client\_id：即为在管理端中接入的应用的应用编码，

对接方易错点：goto字段。在登录时，该字段为保留字段，接入应用可用来保留一些必须的参数，该字段登录后会原封不动返回给接入应用的回调地址中，**这里的回调地址是对接方提交申请表时，里面填写的回调地址，不是goto地址！统一认证登录后不会跳转goto地址，只有登出才会跳转goto！**goto可以是各种值，如果是一个URL地址，尽量不要携带过多参数，如果必须携带超过一个参数，请对整个地址做URL编码，否则会造成参数丢失。

在完成注册或登录后，统一认证中心会访问回调地址并将用户的信息返回到回调页面。

当访问登出的地址时，如果参数中有goto则统一认证在登出用户后会直接访问goto地址，否则会回到自治区政务服务网

# 第三方应用编写

## 1、访问互联网端

**（直接以超链接形式访问上述各种场景地址即可）**

## 2、回调页面（方法）

**注意：回调方法必须支持POST访问。**

在具体的回调页面中会得到来自统一认证中心的参数：

goto：保留参数，登录后原封不动返回给第三方

assertion：加密后的用户信息（登出时需要的SSOSign在里面）；

qtype：判断用户是来自登录还是注册（值分别为login和register）。

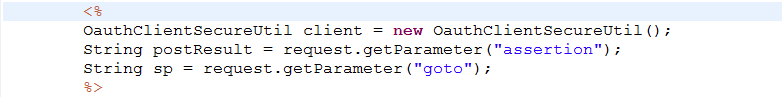
通过以下步骤进行用户信息的获取：

（需要用到dzzw-oauth-1.0.1.jar，见*附录一*）

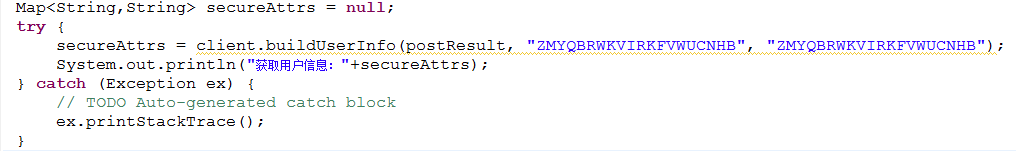
导入相关类：



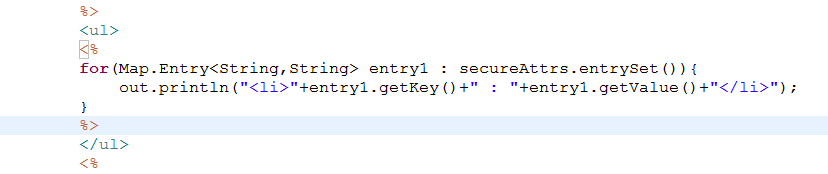
获取url参数：（此处为JSP演示，具体看逻辑，不必纠结必须使用JSP）



根据client\_secret（应用密钥）解密用户信息：

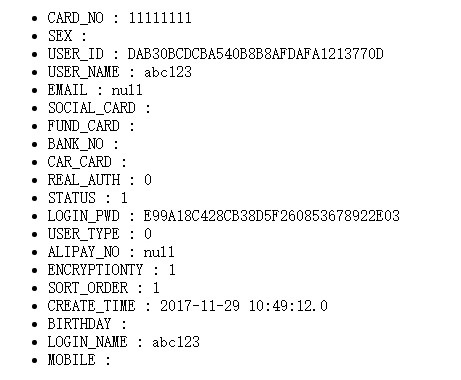


输出用户信息：

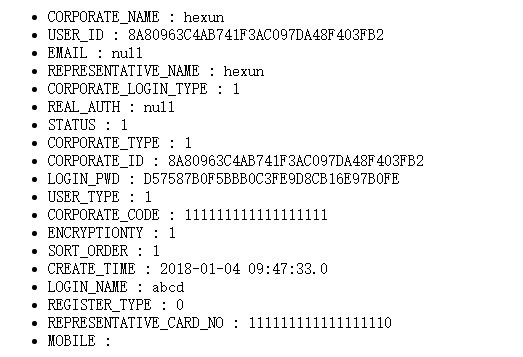


获得的用户信息如下：（解密出来后为Map类型，图片中的字段在文档附录二有介绍，这里提示一下：其中的USER\_TYPE字段可以用来分辨用户类型，0为自然人，1为法人。代理人用户也是1，因为代理人用户也传输法人信息，具体差别看附录二）

【自然人信息】



【法人信息】

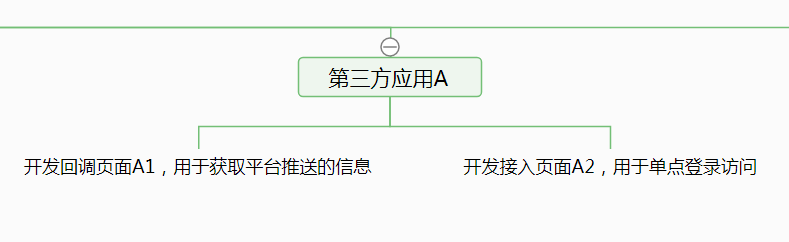


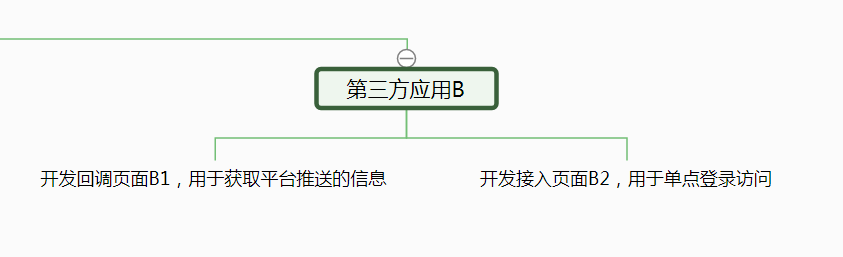
# 多个第三方应用的交互

## 结构

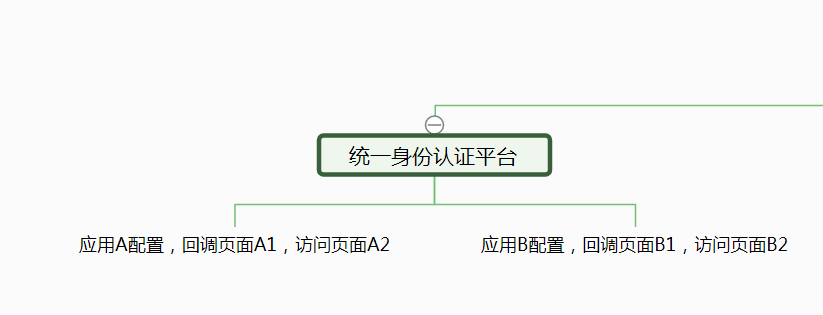


第三方应用A、B接入统一身份认证（面向互联网），即统一身份认证的互联网端。

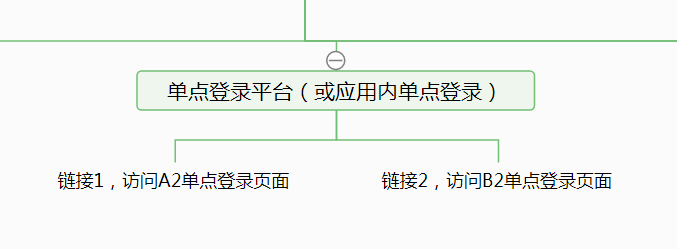




每个应用分别开发回调页面来获取信息和接入页面用于单点登录访问。



在统一身份认证平台（管理端）内配置每个应用的回调页面和访问页面。



在单点登录平台内访问应用的单点登录页面，或者从某一应用内单点登录到另一应用。

## 流程

假定有两个第三方应用A、B，如果应用A需要访问应用B的某个页面，则流程如下：

1. 应用A先在统一认证平台登录
2. 统一认证平台将用户信息返回到应用A的回调页面
3. 应用A处理用户的信息
4. 应用A访问应用B的某个页面
5. 应用B访问统一认证平台获取用户的信息
6. 统一认证平台直接返回已经登录的用户的信息到应用B的回调页面
7. 应用B处理用户的信息
8. 应用B处理应用A的请求

## 解释

* 单点登录的状态（JSESSIONID）是保存在cookie中的，即当应用换浏览器或清除cookie之后则需要重新登录。cookie的检查由统一认证平台完成。
* 当出现某一应用需要调用另一应用的其他页面时，则只需要修改goto参数指向被调用的页面即可。页面所需的参数由应用共同确定。
* 如果某两个应用都有登录验证，那么可以在应用页面被访问时请求统一认证的页面获取用户的信息来完成登录验证。
* 在goto参数中添加跳转地址可以加上跳转地址所需参数，但如果参数多余一个，则需要进行URL编码再传输。

# 总结

统一模式适用于在网站上直接访问统一认证的页面进行统一的登录注册等的web应用，对接工作量小，逻辑简单可靠。

## 接入过程

应用接入分为以下几个步骤。

【统一模式】

1. 申请注册应用，获得client\_id、client\_secret；
2. 通过client\_id、utype、goto参数构造url访问统一认证互联网端进行统一的登录注册等；
3. 保存统一认证返回的用户信息，然后继续通过goto进行跳转；
4. 由第三方应用单点登录到其他第三方应用进行其他操作。

## 参数

【统一模式】

* 请求时需要的参数有client\_id、utype、goto；
* 回调时的参数有goto、assertion、qtype，在解析assertion参数中的用户数据时需要client\_secret；
* 用户信息的各种参数参考附录二**；**
* 需要使用dzzw-oauth-1.0.1.jar（附录）。

# 附录

## 附录一 依赖包

🡨 这个是真的包，不是图片，右键可复制到桌面

## 附录二 服务对象基础表结构

### 1、自然人

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **说明** | **字段** | **检查** |
| 1 | 用户ID | USER\_ID |  |
| 2 | 登录账号 | LOGIN\_NAME | 以字母开头的6-30位字母、数字或下划线的组合 |
| 3 | 登录密码 | LOGIN\_PWD | 界面方式：8-20位大写字母、小写字母、数字、符号中的三种或三种以上的组合，REST接口传递具体看接口要求 |
| 4 | 创建时间 | CREATE\_TIME |  |
| 5 | 用户姓名 | USER\_NAME |  |
| 6 | 手机号 | MOBILE | 合法手机号 |
| 7 | 证件号码 | CARD\_NO | 合法证件号 |
| 8 | 状态（0:无效 1:有效） | STATUS |  |
| 9 | 排序 | SORT\_ORDER |  |
| 10 | 密码加密类型  1：MD5  2：SHA-1  3：SM3 | ENCRYPTIONTY |  |
| 11 | 实名认证类型（以逗号分隔）  0：未认证  1:电信运营商实名认证  2:银联卡实名认证  3:社保卡实名认证  4:公积金账号实名认证  5:驾驶证实名认证  **6:身份证认证**  7:人脸核验  9:实体大厅现场审核验证 | REAL\_AUTH |  |
| 12 | 性别  0：女  1：男 | SEX |  |
| 13 | 出生日期 | BIRTHDAY |  |
| 14 | 银行卡号 | BANK\_NO |  |
| 15 | 邮箱 | EMAIL | 合法邮箱格式 |
| 16 | 支付宝账号 | ALIPAY\_NO |  |
| 17 | 创建者ID | CREATOR |  |
| 18 | 社保卡号 | SOCIAL\_CARD |  |
| 19 | 公积金账号 | FUND\_CARD |  |
| 20 | 驾驶证号 | CAR\_CARD |  |
| 21 | 注册来源  0：网上自主注册  1：实体大厅现场注册 | REGISTER\_TYPE | 值为0或1 |
| 22 | 证件类型 | CARD\_TYPE | 111（身份证）,414（护照）,511（台湾居民来往大陆通行证）,516（港澳居民来往内地通行证） |

### 2、法人

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **说明** | **字段** | **检查** |
| 1 | 法人用户ID | CORPORATE\_ID |  |
| 2 | 法人名称 | CORPORATE\_NAME |  |
| 3 | 统一社会信用代码 | CORPORATE\_CODE | 18位大写字母、数字组合 |
| 4 | 法定代表人姓名 | REPRESENTATIVE\_NAME |  |
| 5 | 法定代表人身份证号 | REPRESENTATIVE\_CARD\_NO | 合法身份证号 |
| 6 | 登录账号 | LOGIN\_NAME | 以字母开头的6-30位字母、数字或下划线的组合 |
| 7 | 登录密码 | LOGIN\_PWD | 界面方式：8-20位大写字母、小写字母、数字、符号中的三种或三种以上的组合，REST接口传递具体看接口要求 |
| 8 | 状态（0:无效 1:有效） | STATUS |  |
| 9 | 创建时间 | CREATE\_TIME |  |
| 10 | 排序 | SORT\_ORDER |  |
| 11 | 法人类型  1:企业法人  2:机关事业单位法人  3:社团法人  4:个体工商  5: 其它单位组织 | CORPORATE\_TYPE | 值为1、2、3、4和5 |
| 12 | 邮箱 | EMAIL | 合法邮箱格式 |
| 13 | 手机号 | MOBILE | 合法手机号 |
| 14 | 密码加密类型  1：MD5  2：SHA-1  3: SM3 | ENCRYPTIONTY |  |
| 15 | 创建者ID | CREATOR |  |
| 16 | 联系电话 | CORPORATE\_PHONE |  |
| 17 | 注册地址 | REGISTER\_ADDRESS |  |
| 18 | 审批机关 | REGISTER\_AGENCY |  |
| 19 | 办理人姓名 | AGENT\_NAME |  |
| 20 | 办理人手机 | AGENT\_MOBILE | 合法手机号 |
| 21 | 办理人身份证号 | AGENT\_CARD\_NO | 合法身份证号 |
| 22 | 法人证照 | CORPROATE\_PICTURE |  |
| 23 | 实名认证类型（以逗号分隔）  0：未认证  1: 网上实名认证  9: 线下材料审核验证 | REAL\_AUTH |  |
| 24 | 注册来源  0：网上自主注册  1：实体大厅现场注册 | REGISTER\_TYPE | 值为0或1 |
| 25 | 法定代表人证件类型 | REPRESENTATIVE\_CARD\_TYPE | 111（身份证）,414（护照）,511（台湾居民来往大陆通行证）,516（港澳居民来往内地通行证） |

### 3、法人代理人

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **说明** | **字段** | **检查** |
| 1 | 代理人用户ID | USER\_ID |  |
| 2 | 法人名称 | CORPORATE\_NAME | 来自其法人母账号 |
| 3 | 统一社会信用代码 | CORPORATE\_CODE | 来自其法人母账号 |
| 4 | 法定代表人姓名 | REPRESENTATIVE\_NAME | 来自其法人母账号 |
| 5 | 法定代表人身份证号 | REPRESENTATIVE\_CARD\_NO | 来自其法人母账号 |
| 6 | 法定代表人证件类型 | REPRESENTATIVE\_CARD\_TYPE | 来自其法人母账号 |
| 7 | 法定代表人用户名 | CORPORATE\_LOGIN\_NAME | 来自其法人母账号 |
| 8 | 登录账号 | LOGIN\_NAME | 以字母开头的6-30位字母、数字或下划线的组合 |
| 9 | 登录密码 | LOGIN\_PWD | 界面方式：8-20位大写字母、小写字母、数字、符号中的三种或三种以上的组合，REST接口传递具体看接口要求 |
| 10 | 状态（0:无效 1:有效） | STATUS |  |
| 11 | 创建时间 | CREATE\_TIME |  |
| 12 | 排序 | SORT\_ORDER |  |
| 13 | 代理人级别 | AGENT\_TYPE | 值为1、2或3，分别代表一级代理人，二级代理人，三级代理人 |
| 14 | 邮箱 | EMAIL | 代理人合法邮箱格式 |
| 15 | 手机号 | MOBILE | 代理人合法手机号 |
| 16 | 密码加密类型  1：MD5  2：SHA-1  3： SM3 | ENCRYPTIONTY |  |
| 17 | 创建者ID | CREATOR |  |
| 18 | 代理人身份证号 | CARD\_NO |  |
| 19 | 所属法人ID | CORPORATE\_ID |  |
| 20 | 所属上级ID | PARENT\_ID |  |
| 21 | 代理人姓名 | AGENT\_NAME |  |