ICS 35.240.01
CCS L 70

SCIE

智 慧 城 市 产 业 生 态 圈 联 盟 标 准

SCIE 6.2—2021

统一身份管理与访问控制平台 第2部分：应用对接规范

Unified identity management and access control platform—Part 2: Application Integeration Specification

2021－10－17 发布　　2021－10－17 实施

智慧城市产业生态圈　　发 布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由智慧城市产业生态圈提出并归口。

本文件主要起草单位：深圳竹云科技有限公司、西安电子科技大学、华为技术有限公司、深圳市标准技术研究院、山东省计算中心（国家超级计算济南中心）

本文件主要起草人：赵静谧、史晓婧、徐曲莎、张涛、张志为、黄敏、胡露、侯义荣、杨叶、史丛丛

统一身份管理与访问控制平台 第2部分：应用对接规范

1 范围

本文件提供了统一身份管理与访问控制平台与各个业务应用系统对接的规范，介绍了应用系统与统一身份管理与访问控制平台对接的总体框架、应用对接流程、身份数据同步对接要求、应用认证对接要求及应用对接接口说明，为系统集成人员提供技术指导。

本文件适用于集成方项目经理、开发人员、测试人员进行应用集成的技术对接。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

统一身份管理与访问控制平台 unified identity management and access control platform

是管理自然人及应用系统的平台，通过对人员所属的组织、角色、岗位、身份、账号、权限、身份认证等进行统一的管理，将不同维度的人员纳入统一的安全管控体系，合理控制自然人访问应用系统资源的权限，并对异常访问行为进行有效防范。

3.2

供应 provide

统一身份管理与访问控制平台将用户、账号、角色、组织信息等同步到对接的各个应用系统。

3.3

回收 recover

各应用系统将用户、账号、角色、组织信息等同步到统一身份管理与访问控制平台。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）
IAM: 身份识别与访问管理（Identity and Access Management）
JDBC：JAVA数据库连接（Java Database Connectivity）
LDAP：轻型目录访问协议（Lightweight Directory Access Protocol）
OAuth：开放授权(Open Authorization)
RESTFUL：表述性状态转移（Representational State Transfer）
SDK：软件开发工具包（Software Development Kit）
SAML：安全断言标记语言（Security Assertion Markup Language)
WS：基于网络的、分布式的模块化组件（Web Service）

5 总体框架

统一身份管理与访问控制平台（以下简称为IAM平台）与各个应用系统对接，包含身份数据同步对接及应用认证集成对接两部分。IAM平台应用集成总体架构见图1。

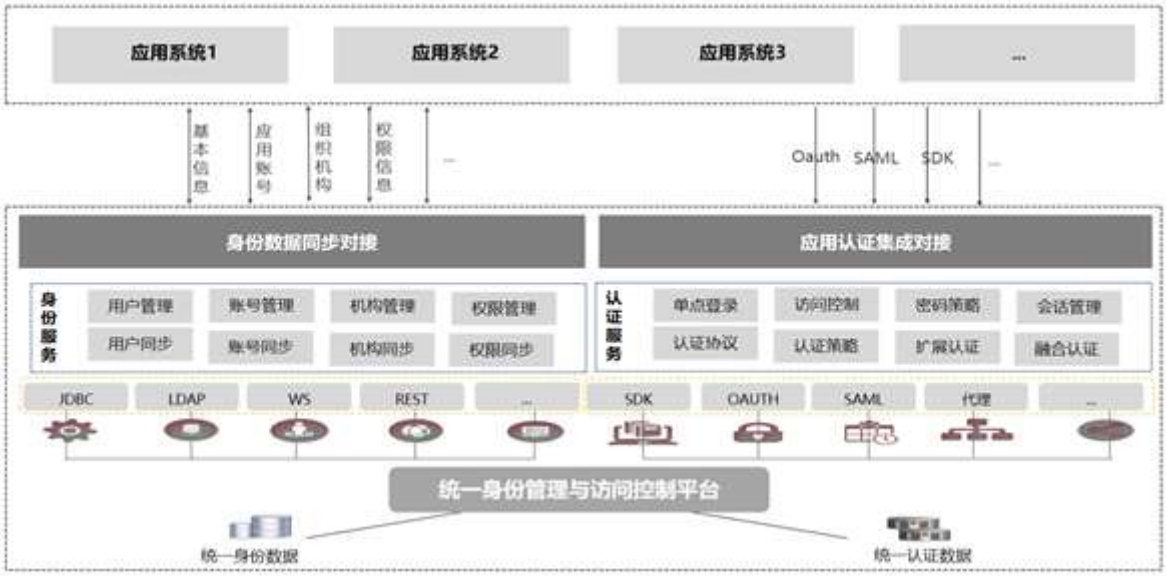

图1　IAM 平台应用对接总体架构

IAM 平台应用对接总体架构各部分描述如下：

a) 身份数据同步对接：完成 IAM 平台与各个应用系统间的身份数据对接，实现用户身份信息（包括用户基本信息、应用账号、组织机构及用户权限等）的同步。身份数据同步方式支持 IAM 平台主动同步模式和应用系统主动同步模式，两种模式均应支持 JDBC/LDAP 标准接口及 WS/REST 外部接口。若应用系统需实时同步身份数据，并且可按 IAM 平台提供的规范开发身份相关接口，推荐选择 IAM 平台主动同步模式，若应用系统不需要实时同步身份数据，推荐选择应用系统主动同步模式。

b) 应用认证集成对接：完成 IAM 平台与各个应用系统间的认证集成，实现应用系统的单点登录、认证等级及认证方式扩展（如证书、短信、生物认证等）。应用认证集成方式支持标准协议集成（如 OAuth、SAML 等）及认证接口集成。若应用系统支持 OAuth、SAML 等标准认证协议，并可配合 IAM 平台进行相关登录页面改造、登录逻辑改造或修改应用系统认证配置，则推荐使用标准协议对接方式，若应用系统不支持标准认证协议，则推荐使用 SDK 接口对接方式。

注：人脸、声纹、指静脉等AI认证以及数字证书、邮箱、短信等认证均需要第三方提供算法或者服务，IAM平台仅提供对接能力。

6　应用对接流程

应用标准对接流程涵盖数据源调研、用户调研、应用调研、平台部署、集成开发、上线验收 6 个阶段。各阶段工作内容见图 2。

图2　IAM 平台应用对接流程

应用对接过程中，各阶段工作内容描述如下：

a) 数据源调研：调研 IAM 平台初始化用户身份数据来源，包含用户数据来源、机构数据来源、账号数据来源、角色数据来源；
b) 用户调研：调研 IAM 平台用户管理范围及流程，包含用户数量、用户类型、用户与账号关联关系、用户增删查改流程及用户管理相关业务功能需求；
c) 应用调研：调研 IAM 平台拟接入应用系统情况，包含应用系统名称、系统建设厂商、应用对接需求、应用配合情况、接口开放情况，通过应用调研确定接入方案；
d) 平台部署：进行 IAM 平台部署，并完成待集成应用系统的注册、初始化身份数据；
e) 集成开发：完成 IAM 平台定制界面及功能开发工作；完成应用系统集成环境的准备，试点应用系统完成与 IAM 平台的对接测试；
f) 上线验收：完成 IAM 平台的验收测试、项目文档交付及相关培训工作，最终进行项目验收。

应用对接过程中，涉及到IAM平台项目组、需求方项目组、应用项目组间的协调配合，各方工作内容描述如下：

a) IAM 平台项目组：负责数据源调研、用户调研、应用调研及整体项目设计、平台部署设计、应用对接方案及平台部署、测试、平台相关培训及项目文档交付；
b) 需求方项目组：参与项目内容讨论，协调应用开发商配合 IAM 平台的集成工作，参与整体项目验收及培训；
c) 应用项目组：参与数据源调研、用户调研、应用调研及方案设计，配合 IAM 平台进行集成改造并参与验收及测试。

7 身份数据同步对接要求

7.1 身份数据同步

IAM 平台与应用系统间通过身份 API 进行交互，实现身份数据的集中管理及 IAM 平台与应用系统间身份数据同步。

应用系统与 IAM 平台完成身份数据同步集成后，应满足以下功能要求：

a) 用户的新增、修改、禁用、启用、删除的集中管理；
b) 应用系统账号的新增、修改、禁用、启用、删除的集中管理；
c) 组织机构的新增、修改、删除的集中管理；
d) 用户权限的集中管理；
e) IAM 平台与应用系统的用户、账号、机构、权限同步。

7.2 身份服务

身份服务为 IAM 平台与应用系统的身份数据同步提供后台服务，主要提供：用户管理、账号管理、机构管理、权限管理、用户同步、账号同步、机构同步、权限同步功能。

身份服务通过与应用系统进行数据同步对接，实现用户身份信息的同步。身份服务与应用系统对接，宜分为两种模式：

a) 第一种模式是 IAM 平台主动将身份数据实时推送到应用系统。需应用系统按照 IAM 平台提供的规范开发账号、机构、角色的管理接口；
b) 第二种模式是应用系统主动获取 IAM 平台身份数据，应用系统可自定义设置获取身份数据的频率，为非实时的数据同步。需应用系统定期通过 IAM 平台提供的身份数据接口从消息队列中获取数据的变化。

7.3 数据同步对接流程

IAM 平台与应用系统完成身份数据同步对接流程主要分为五步：应用调研、应用注册、集成对接、集成测试及上线。分别完成如下工作：

a) 应用调研：调研应用基本情况，确认集成范围与集成方案；
b) 应用注册：应用系统提供注册的基本信息，含应用中文名称、应用英文简称、应用系统账号创建时需要的属性、应用系统账号创建策略等，并在 IAM 平台注册应用系统；
c) 集成对接：应用系统与 IAM 平台进行身份 API 交互；
d) 集成测试：IAM 平台与应用系统对接功能进行联调，确认在功能和业务上满足相关要求；
e) 上线：IAM 平台与应用系统共同完成集成内容的上线。

7.4 数据同步对接分工

数据同步对接工作会涉及到 IAM 平台项目组、需求方项目组、应用项目组间的协调配合，各方工作内容描述如下：

a) IAM 平台项目组：进行应用调研，明确应用对接方案及应用对接规范，完成待对接应用系统的注册并提供应用注册后的信息、提供数据同步接口开发规范/提供数据同步外部接口供应用系统调用、完成与应用系统数据同步联调测试及上线工作；
b) 需求方项目组：参与应用调研，确认应用对接范围与对接方案，待 IAM 平台与应用系统完成数据同步联调测试后，测试数据同步效果，确认是否满足业务要求，配合完成应用对接后的上线工作；
c) 应用项目组：参与应用调研，确认应用对接范围与对接方案，提供应用系统注册基本信息，根据 IAM 平台提供的数据同步接口规范开发数据同步接口/调用 IAM 平台发布的数据同步外部接口完成数据同步对接，完成与 IAM 平台数据同步联调测试及上线工作。

7.5 数据同步对接接口

7.5.1 IAM 平台主动同步模式

IAM平台主动同步模式数据同步对接接口清单见表1，接口示例见附录A.1。

表1 IAM 平台主动推送模式接口清单

序号	接口名称	接口说明
1	SchemaService	获取第三方目标系统中账号（应用内的user）、机构、角色等对象全部属性信息，包括属性名称、类型、是否必填字段、是否多值。用以建立起IAM平台用户字段和三方目标系统账号字段的映射关系。
2	UserCreateService	应用系统的账号创建
3	UserUpdateService	应用系统的账号修改
4	UserDeleteService	应用系统的账号删除
5	FindAllUserIdsService	查询三方应用系统账号唯一性主键ID列表
6	FindUserByIdService	根据账号ID，查询账号的详细信息
7	OrgCreateService	应用系统的组织机构创建
8	OrgUpdateService	应用系统的组织机构修改
9	OrgDeleteService	应用系统的组织机构删除
10	FindAllOrgIdsService	查询三方应用系统组织机构唯一性主键ID列表
11	FindOrgByIdService	根据组织机构ID，查询组织机构的详细信息
12	FindAllRoleIdsService	查询三方应用系统角色唯一性主键ID列表
13	FindRoleByIdService	根据系统角色ID,查询系统角色的详细信息

7.5.2 应用系统主动同步模式

应用系统主动同步模式数据同步对接接口清单见表2，接口示例见附录A.2。

表2　应用系统主动同步模式接口清单

序号	接口名称	接口说明
1	Login	登录接口
2	Logout	登出接口
3	SyncTask	应用系统从IAM平台获取全量身份数据
4	SyncFinish	应用系统从IAM平台获取全量身份数据完成
5	PullTask	应用系统从IAM平台获取增量身份数据
6	PullFinish	应用系统从IAM平台获取增量身份数据完成
7	PushTask	应用系统推送身份数据到IAM平台
8	PushFinish	应用系统推送身份数据到IAM平台完成

8　应用认证对接要求

8.1　认证对接

IAM 平台与应用系统间通过认证 API 接口进行交互，实现应用系统的统一认证、单点登录及多因素认证的扩展功能。应用系统与 IAM 平台对接后，应满足以下功能要求：

a)　应用系统的统一认证管理，各应用系统统一在 IAM 平台进行认证；
b)　访问已对接的应用系统实现单点登录效果；
c)　提供多因素认证扩展能力。

8.2　认证服务

认证服务为 IAM 平台与应用系统的认证对接提供后台服务，主要提供：单点登录、访问控制、密码策略、会话管理、认证协议、认证策略、扩展认证、融合认证功能。

认证服务通过与应用系统进行认证对接，实现应用系统的统一认证管理。认证服务与应用系统进行认证对接，宜使用标准协议对接与SDK接口对接两种方式：

a)　标准协议对接：支持常用认证协议（如：OAuth、SAML、CAS），应用系统应按 IAM 平台提供的对接规范进行改造或配置；
b)　SDK 接口对接：由应用系统调用 IAM 平台提供的认证接口（支持主流的 WS/REST 外部接口）。

8.3　认证对接流程

IAM 平台与应用系统完成认证集成流程主要分为五步：应用调研、应用注册、集成对接、集成测试及上线。对接流程具体描述如下：

a)　应用调研：调研应用基本情况，确认集成范围与集成方案；
b)　应用注册：应用系统提供注册的基本信息，含应用中文名称、应用英文简称、应用系统账号创建时需要的属性、应用系统账号创建策略等，并在 IAM 平台注册应用系统；
c)　集成对接：应用系统与 IAM 平台进行认证 API 交互；
d)　集成测试：IAM 平台与应用系统对接功能进行联调，确认在功能和业务上满足相关要求；
e)　上线：IAM 平台与应用系统共同完成集成内容的上线。

8.4　认证对接分工

认证集成工作会涉及到 IAM 平台项目组、需求方项目组、应用项目组间的协调配合，各方工作内容描述如下：

a) IAM 平台项目组：进行应用调研，明确应用集成方案及应用集成规范，完成待集成应用系统的注册并提供应用注册后的信息、提供标准协议认证集成规范/提供认证集成外部接口供应用系统调用、完成与应用系统认证集成联调测试及上线工作；
b) 需求方项目组：参与应用调研，确认应用集成范围与集成方案，待 IAM 平台与应用系统完成认证集成联调测试后，测试认证集成效果，确认是否满足业务要求，配合完成应用集成后的上线工作；
c) 应用项目组：参与应用调研，确认应用集成范围与集成方案，提供应用系统注册基本信息，根据 IAM 平台提供的标准协议认证集成规范进行认证改造/调用 IAM 平台发布的认证集成外部接口完成认证集成，完成与 IAM 平台数据同步联调测试及上线工作。

8.5 认证对接接口

8.5.1 标准协议对接模式

标准协议认证对接接口清单见表3（以OAuth协议为例），接口示例见附录A.3。

表3 标准协议认证对接接口清单

序号	接口名称	接口说明
1	authorize	应用系统端授权接口
2	getToken	获取授权码接口
3	refreshToken	更新授权码接口
4	checkTokenValid	校验授权码是否有效接口
5	getUserInfo	获取用户信息接口

8.5.2 认证接口对接模式

认证接口对接模式接口清单见表4，接口示例见附录A.4。

序号	接口名称	接口说明
1	authenticate	认证接口
2	setToken	获取授权码接口
3	refreshToken	设置票据接口
4	isTokenValid	验证票据接口
5	GetUserAttributes	获取用户信息接口
6	logout	登出接口

附 录 A
（资料性）
应用对接接口说明

A.1 数据同步-IAM 平台主动同步模式接口

A.1.1 模式服务接口

模式服务接口说明见表A.1。

表A.1 模式服务接口说明

接口名	SchemaService		
功能说明	获取第三方目标系统中账号（应用内的 user）、机构、角色等对象全部属性信息，包括属性名称、类型、是否必填字段、是否多值。用以建立起 IAM 平台用户字段和三方目标系统账号字段的映射关系。		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用生成的随机 ID，应用系统每次响应返回此 ID，String 类型	是
	IAM 平台 RemotePwd	IAM 平台调用三方应用接口的授权账号，由应用分配给 IAM 平台，String 类型(接口鉴权 key)	是
	IAM 平台 RemoteUser	IAM 平台调用三方应用接口的密码，由应用分配给 IAM 平台，String 类型(接口鉴权 user)	是

请求体报文（JSON 格式）	{
	"IAM 平台 RequestId": "9e928d12ec8a4c1bb75283b8df71308d",
	"IAM 平台 RemotePwd": "password",
	"IAM 平台 RemoteUser": "IAM 平台 admin"
	}		

响应参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用接口发送的请求 ID，字段为 String 类型	是
	account/organization/role	此接口定义的对象类型，可选值为 account（账号）、organization（组织机构）、role（角色）、group（用户组），如果只做大门级账号权限管理，organization 等其它对象可以不用定义，字段为数组类型	是
	name	定义对象的属性字段名称。字段为 String 类型	是
	type	定义对象的属性字段类型，可选值为 String、int、double、float、long、byte、boolean。字段为 String 类型。	是
	Required	定义对象的属性字段在创建时是否为必填字段。可选值 true 或者 false。字段为 boolean 类型。	是
	Multivalued	定义对象的属性字段是否为多值。可选值 true 或者 false。字段为 boolean 类型。	是

表A.1 （续）

返回值(JSON格式)	{
	“IAM平台RequestId”：“9e928d12ec8a4c1bb75283b8df71308d”,
	“account”：[{
	“multivalued”：false,
	“name”：“uid”,
	“required”：false,
	“type”：“String”
	},{
	“multivalued”：false,
	“name”：“8sername”,
	“required”：true,
	“type”：“String”
	}, {
	“multivalued”：false,
	“name”：“orgId”,
	“required”：true,
	“type”：“String”
	}, {
	“multivalued”：true,
	“name”：“roles”,
	“required”：false,
	“type”：“String”
	}, {
	“multivalued”：false,
	“name”：“fullName”,
	“required”：true,
	“type”：“String”
	},{
	“multivalued”：false,
	“name”：“password”,
	“required”：false,
	“type”：“String”
	},{
	“multivalued”：false,
	“name”：“status”,
	“required”：true,
	“type”：“int”
	},……],
	“organization”：[{
	“multivalued”：false,
	“name”：“orgId”,
	“required”：false,
	“type”：“String”
	}, {
	“multivalued”：false,
	“name”：“orgName”,
	“required”：true,
	“type”：“String”
	}, {

表A.1 （续）

返回值(JSON格式)	“multivalued”: false,
	“name”: “parentOrgId”,
	“required”: true,
	“type”: “String”
	},……],
	“role”: [{
	“multivalued”: false,
	“name”: “roleId”,
	“required”: false,
	“type”: “String”
	}, {
	“multivalued”: false,
	“name”: “roleName”,
	“required”: true,
	“type”: “String”
	},……]
	}

A.1.2 账号创建接口

账号创建接口说明见表A.2。

表A.2 账号创建接口说明

接口名	UserCreateService		
功能说明	应用系统的账号创建方法		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用生成的随机ID，应用系统每次响应返回此ID，String类型	是
	IAM平台RemotePwd	IAM平台调用三方应用接口的授权账号，由应用分配给IAM平台，String类型	是
	IAM平台RemoteUser	IAM平台调用三方应用接口的密码，由应用分配给IAM平台，String类型	是
	loginName/ orgId/ fullName	三方应用系统SchemaService接口中定义的账号字段属性	是

表A.2 （续）

<table>
<tr><td>请求体报文（JSON格式）</td><td colspan="3">{
"IAM平台RequestId": "11928d12ec8a4c1bb75283b8df71308d",
"IAM平台RemoteUser": "IAM平台admin",
"IAM平台RemotePwd": "password",
"loginName": "zhangsan",
"orgId": "D01-0110-0110654",
"role": ["11","22"],
"fullName": "张三",
"password": null
"status": 0,…
}</td></tr>
<tr><td rowspan="5">响应参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>IAM平台RequestId</td><td>IAM平台每次调用接口发送的请求ID，字段为String类型</td><td>是</td></tr>
<tr><td>uid</td><td>应用系统账号创建后，形成的全局唯一ID，此ID不能被修改，建议为数据库表主键。此ID返回至IAM平台，此后账号的修改和删除都以此ID为主键。字段为String类型。</td><td>是</td></tr>
<tr><td>resultCode</td><td>接口调用处理的结果码，0为正常处理，其它值由应用系统定义。字段为String类型。</td><td>是</td></tr>
<tr><td>message</td><td>接口调用处理的信息。字段为String类型。</td><td>是</td></tr>
<tr><td>返回值（JSON格式）</td><td colspan="3">{
"IAM平台RequestId": "11928d12ec8a4c1bb75283b8df71308d",
"uid": "89746776",
"resultCode": "0",
"message": "success"
}</td></tr>
</table>

A.1.3 账号更新接口

账号更新接口说明见表A.3。

表A.3 账号更新接口说明

<table>
<tr><th>接口名</th><th colspan="3">UserUpdateService</th></tr>
<tr><td>功能说明</td><td colspan="3">应用系统的账号修改方法</td></tr>
<tr><td>请求类型</td><td colspan="3">POST</td></tr>
<tr><td rowspan="6">请求参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>IAM平台RequestId</td><td>IAM平台每次调用生成的随机ID，应用系统每次响应返回此ID，String类型</td><td>是</td></tr>
<tr><td>IAM平台RemotePwd</td><td>IAM平台调用三方应用接口的授权账号，由应用分配给IAM平台，String类型</td><td>是</td></tr>
<tr><td>IAM平台RemoteUser</td><td>IAM平台调用三方应用接口的密码，由应用分配给IAM平台，String类型</td><td>是</td></tr>
<tr><td>uid</td><td>三方应用系统账号创建时，返回给IAM平台应用系统的账号主键uid。</td><td>是</td></tr>
<tr><td>loginName/
fullName</td><td>需要修改的账号字段属性</td><td>是</td></tr>
</table>

表A.3 （续）

请求体报文(JSON格式)	{
	"IAM平台RequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"IAM平台RemoteUser": "IAM平台admin",
	"IAM平台RemotePwd": "password",
	"uid": "89746776",
	"loginName": "lisi",
	"fullName": "李四"
	}		

响应参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用接口发送的请求ID，字段为String类型	是
	resultCode	接口调用处理的结果码，0为正常处理，其它值由应用系统定义。字段为String类型，必传字段。	是
	message	接口调用处理的信息。字段为String类型	是

返回值(JSON格式)	{
	"IAM平台RequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}		

A.1.4 账号删除接口

账号删除接口说明见表A.4.

表A.4 账号删除接口说明

接口名	UserDeleteService		
功能说明	应用系统的账号删除方法		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用生成的随机ID，应用系统每次响应返回此ID，String类型	是
	IAM平台RemotePwd	IAM平台调用三方应用接口的授权账号，由应用分配给IAM平台，String类型	是
	IAM平台RemoteUser	IAM平台调用三方应用接口的密码，由应用分配给IAM平台，String类型	是
	uid	三方应用系统账号创建时，返回给IAM平台应用系统的账号主键uid。	是

请求体报文（JSON格式）	{
	"IAM平台RequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"IAM平台RemoteUser": "IAM平台admin",
	"IAM平台RemotePwd": "password",
	"uid": "89746776"
	}		

响应参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用接口发送的请求ID，字段为String类型	是
	resultCode	接口调用处理的结果码,0为正常处理,其它值由应用系统定义。字段为String类型。	是
	message	接口调用处理的信息。字段为String类型	是

返回值(JSON格式)	{
	"IAM平台RequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}		

A.1.5 所有账号查询接口

所有账号查询接口说明见表A.5。

表A.5 所有账号查询接口说明

接口名	FindAllUserIdsService		
功能说明	查询三方应用系统账号唯一性主键 ID 列表的接口方法。此 ID 需与 UserCreateService、UserUpdateService、UserDeleteService 接口中的 uid 字段值相同		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用生成的随机 ID，应用系统每次响应返回此 ID，String 类型	是
	IAM 平台 RemoteUser	IAM 平台调用三方应用接口的授权账号，由应用分配给 IAM 平台，String 类型	是
	IAM 平台 RemotePwd	IAM 平台调用三方应用接口的密码，由应用分配给 IAM 平台，String 类型	是
	updateTime	IAM 平台调用三方应用接口的更新时间，由应用分配给 IAM 平台，String 类型（由这个时间字段进行增量回收，应用系统也需要根据时间进行更新时间条件查询）	否
请求体报文（JSON 格式）	{ "IAM 平台 RequestId": "65428d12ec8a4c1bb75283b8df71308d", "IAM 平台 RemotePwd": "password", "IAM 平台 RemoteUser": "IAM 平台 admin", "updateTime":"2020-11-25 14:46:25" }		
响应参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用接口发送的请求 ID，字段为 String 类型	是
	resultCode	接口调用处理的结果码,0 为正常处理,其它值由应用系统定义。字段为 String 类型。	是
	uidList	账号主键 ID 列表，字段为 String 数组类型	是
	message	接口调用处理的信息。字段为 String 类型	是
返回值（JSON 格式）	{ “resultCode”：“0”， “message”：“success”， “uidList”：[“ID00001”，“ID00002”，“ID00003”]， “IAM 平台 RequestId”：“47f591ceca2c410a9fe092af05987f40” }		

A.1.6 单个账号查询接口

单个账号查询接口说明见表A.6。

表A.6 单个账号查询接口说明

接口名	FindUserByIdService		
功能说明	根据 FindAllUserIdsService 接口查询返回的账号 ID，查询账号的详细信息		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用生成的随机 ID，应用系统每次响应返回此 ID，String 类型	是
	IAM 平台 RemotePwd	IAM 平台调用三方应用接口的授权账号，由应用分配给 IAM 平台，String 类型	是
	uid	账号 ID。	是

表A.6 （续）

请求参数	参数名	中文说明	是否必传
	IAM 平台 RemoteUser	IAM 平台调用三方应用接口的密码，由应用分配给 IAM 平台，String 类型	是

请求体报文（JSON 格式）	{
	"IAM 平台 RequestId": "55528d12ec8a4c1bb75283b8df71308d",
	"IAM 平台 RemoteUser": "IAM 平台 admin",
	"IAM 平台 RemotePwd": "password",
	"uid": " D00001"
	}		

响应参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用接口发送的请求 ID，字段为 String 类型	是
	resultCode	接口调用处理的结果码，0 为正常处理，其它值由应用系统定义。字段为 String 类型。	是
	account	应用返回的账号 json 对象。	是
	message	接口调用处理的信息。字段为 String 类型	是

返回值（JSON 格式）	{
	"account": {
	"orgId": "1000-10001-10000011",
	"loginName": "zhangsan",
	"fullName": "zhangsanFull",
	"uid": "D00001",
	"updateTime":"2020-11-25 14:46:25"
	},
	"resultCode": "0",
	"message": "success",
	"IAM 平台 RequestId": "55528d12ec8a4c1bb75283b8df71308d "
	}		

注意事项	如果接口支持增量回收，查询接口有传 updateTime 的话，查询详情接口必须返回更新时间 updateTime。		

A.1.7 机构创建接口

机构创建接口说明见表A.7。

表A.7 机构创建接口说明

接口名	OrgCreateService		
功能说明	应用系统的组织机构创建方法		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用生成的随机 ID，应用系统每次响应返回此 ID，String 类型	是
	IAM 平台 RemotePwd	IAM 平台调用三方应用接口的授权账号，由应用分配给 IAM 平台，String 类型	是
	orgName/parentOrgId	三方应用系统 SchemaService 接口中定义的组织机构字段属性。parentOrgId 上级组织 id 一般必传，是组织机构树建立的依据	是
	IAM 平台 RemoteUser	IAM 平台调用三方应用接口的密码，由应用分配给 IAM 平台，String 类型	是

请求体报文（JSON 格式）	{
	"IAM 平台 RequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"IAM 平台 RemoteUser": "IAM 平台 admin",
	"IAM 平台 RemotePwd": "password",
	"orgName": "集团信息中心",
	"parentOrgId": "000001"
	}		

表A.7 （续）

响应参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用接口发送的请求ID，字段为String类型	是
	resultCode	接口调用处理的结果码，0为正常处理，其它值由应用系统定义。字段为String类型。	是
	orgId	应用系统组织机构创建后，形成的全局唯一ID，此ID不能被修改，建议为数据库表主键。此ID返回至IAM平台，此后组织机构的修改和删除都以此ID为主键。字段为String类型。	是
	message	接口调用处理的信息。字段为String类型	是
返回值(JSON格式)	{ "IAM平台RequestId": "11928d12ec8a4c1bb75283b8df71308d", "orgId": "0000011", "resultCode": "0", "message": "success" }		

A.1.8 机构刷新接口

机构刷新接口说明见表A.8。

表A.8 机构刷新接口说明

接口名	OrgUpdateService		
功能说明	应用系统的组织机构修改方法		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用生成的随机ID，应用系统每次响应返回此ID，String类型	是
	IAM平台RemotePwd	IAM平台调用三方应用接口的授权账号，由应用分配给IAM平台，String类型	是
	orgName / parentOrgId	需要修改的组织机构字段属性	是
	orgId	三方应用系统组织机构创建时，返回给IAM平台应用系统的组织机构主键orgId。	是
	IAM平台RemoteUser	IAM平台调用三方应用接口的密码,由应用分配给IAM平台,String类型	是
请求体报文	{ "IAM平台RequestId": "22928d12ec8a4c1bb75283b8df71308d", "IAM平台RemoteUser": "IAM平台admin", "IAM平台RemotePwd": "password", "orgId": "0000011", "orgName": "集团信息中心", "parentOrgId": "000002" }		
响应参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用接口发送的请求ID，字段为String类型	是
	resultCode	接口调用处理的结果码，0为正常处理，其它值由应用系统定义。字段为String类型。	是
	message	接口调用处理的信息。字段为String类型	是
返回值(JSON格式)	{ "IAM平台RequestId": "22928d12ec8a4c1bb75283b8df71308d", "resultCode": "0", "message": "success" }		

A.1.9 机构删除接口

机构删除接口说明见表A.9。

表A.9 机构删除接口说明

接口名	OrgDeleteService		
功能说明	应用系统的组织机构删除方法		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用生成的随机 ID，应用系统每次响应返回此 ID，String 类型	是
	IAM 平台 RemotePwd	IAM 平台调用三方应用接口的授权账号，由应用分配给 IAM 平台，String 类型	是
	orgId	三方应用系统组织机构创建时，返回给 IAM 平台应用系统的组织机构主键 orgId。	是
	IAM 平台 RemoteUser	IAM 平台调用三方应用接口的密码，由应用分配给 IAM 平台，String 类型	是

请求体报文（JSON 格式）	{
	"IAM 平台 RequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"IAM 平台 RemoteUser": "IAM 平台 admin",
	"IAM 平台 RemotePwd": "password",
	"orgId ": "000011"
	}		

响应参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用接口发送的请求 ID，字段为 String 类型	是
	resultCode	接口调用处理的结果码，0 为正常处理，其它值由应用系统定义。字段为 String 类型。	是
	message	接口调用处理的信息。字段为 String 类型	是

返回值（JSON 格式）	{
	"IAM 平台 RequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}		

A.1.10 所有机构查询接口(机构查找)

所有机构查询接口说明见表A.10。

表A.10 所有机构查询接口说明

接口名	FindAllOrgIdsService		
功能说明	查询三方应用系统组织机构唯一性主键 ID 列表的接口方法。此 ID 需与 OrgCreateService、OrgUpdateService、OrgDeleteService 接口中的 orgID 字段值相同		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM 平台每次调用生成的随机 ID，应用系统每次响应返回此 ID，String 类型	是
	IAM平台RemotePwd	IAM 平台调用三方应用接口的授权账号，由应用分配给 IAM 平台，String 类型	是
	IAM 平台 RemoteUser	IAM 平台调用三方应用接口的密码,由应用分配给 IAM 平台,String 类型	是
	updateTime	IAM 平台调用三方应用接口的更新时间，由应用分配给 IAM 平台，String 类型（由这个时间字段进行增量回收，应用系统也需要根据时间进行更新时间条件查询）	否

表A.10 （续）

请求体报文(JSON格式)	{
	"IAM平台RequestId": "65428d12ec8a4c1bb75283b8df71308d",
	"IAM平台RemotePwd": "password",
	"IAM平台RemoteUser": "IAM平台admin",
	"updateTime":"2020-11-25 14:46:25"
	}		

响应参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用接口发送的请求ID，字段为String类型	是
	resultCode	接口调用处理的结果码，0为正常处理，其它值由应用系统定义。字段为String类型。	是
	orgIdList	组织机构主键ID列表，字段为String数组类型。	是
	message	接口调用处理的信息。字段为String类型	是

返回值(JSON格式)	{
	“resultCode”：“0”，
	“message”：“success”，
	“orgIdList”：[“0000011”，“0000012”，“0000013”]，
	“IAM平台RequestId”：“47f591ceca2c410a9fe092af05987f40”
	}		

A.1.11 单个机构详情查询接口(单个机构详情查询)

单个机构详情查询接口说明见表A.11。

表A.11 单个机构详情查询接口说明

接口名	FindOrgByIdService		
功能说明	根据FindAllOrgIdsService接口查询返回的组织机构ID，查询组织机构的详细信息		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用生成的随机ID，应用系统每次响应返回此ID，String类型	是
	IAM平台RemotePwd	IAM平台调用三方应用接口的授权账号，由应用分配给IAM平台，String类型	是
	orgId	组织机构ID。	是
	IAM平台RemoteUser	IAM平台调用三方应用接口的密码，由应用分配给IAM平台，String类型	是

请求体报文(JSON格式)	{
	"IAM平台RequestId": "55528d12ec8a4c1bb75283b8df71308d",
	"IAM平台RemoteUser": "IAM平台admin",
	"IAM平台RemotePwd": "password",
	"orgId": " 000012",
	}		

响应参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用接口发送的请求ID，字段为String类型	是
	resultCode	接口调用处理的结果码，0为正常处理，其它值由应用系统定义。字段为String类型。	是
	organization	应用返回的机构对象。	是
	message	接口调用处理的信息。字段为String类型	是

表A.11 （续）

返回值(JSON格式)	{
	"organization": {
	"orgName": "信息中心应用处",
	"parOrgId": "000001",
	"orgId": "000012"
	"updateTime":"2020-11-25 14:46:25"
	},
	"resultCode": "0",
	"message": "success",
	"IAM平台RequestId": "55528d12ec8a4c1bb75283b8df71308d "
	}

注意事项	如果接口支持增量回收，查询接口有传 updateTime 的话，查询详情接口必须返回更新时间updateTime。

A.1.12 角色查询接口

角色查询接口说明见表A.12。

表A.12 角色查询接口说明

接口名	FindAllRoleIdsService		
功能说明	查询三方应用系统角色唯一性主键ID列表的接口方法		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用生成的随机ID，应用系统每次响应返回此ID，String类型	是
	IAM平台RemotePwd	IAM平台调用三方应用接口的授权账号，由应用分配给IAM平台，String类型	是
	IAM平台RemoteUser	IAM平台调用三方应用接口的密码，由应用分配给IAM平台，String类型	是
	updateTime	IAM平台调用三方应用接口的更新时间，由应用分配给IAM平台，String类型（由这个时间字段进行增量回收，应用系统也需要根据时间进行更新时间条件查询）	否

请求体报文(JSON格式)	{
	"IAM平台RequestId": "65428d12ec8a4c1bb75283b8df71308d",
	"IAM平台RemotePwd": "password",
	"IAM平台RemoteUser": "IAM平台admin",
	"updateTime":"2020-11-25 14:46:25"
	}		

响应参数	参数名	中文说明	是否必传
	IAM平台RequestId	IAM平台每次调用接口发送的请求ID，字段为String类型	是
	resultCode	接口调用处理的结果码,0为正常处理,其它值由应用系统定义。字段为String类型。	是
	roleIdList	角色主键ID列表，字段为String数组类型，必传字段	是
	message	接口调用处理的信息。字段为String类型	是

返回值(JSON格式)	{
	“resultCode”：“0”，
	“message”：“success”，
	“roleIdList”：[“0000011”，“0000012”，“0000013”]，
	“IAM平台RequestId”：“47f591ceca2c410a9fe092af05987f40”
	}		

A.1.13 角色详情查询接口

角色详情查询接口说明见表A.13。

表A.13 角色详情查询接口说明

接口名	FindRoleByIdService		
功能说明	查询三方应用系统角色唯一性主键 ID 列表的接口方法		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用生成的随机 ID，应用系统每次响应返回此 ID，String 类型	是
	IAM 平台 RemotePwd	IAM 平台调用三方应用接口的授权账号，由应用分配给 IAM 平台，String 类型	是
	roleId	角色 ID。必传字段	是
	IAM 平台 RemoteUser	IAM 平台调用三方应用接口的密码，由应用分配给 IAM 平台，String 类型	是

请求体报文(JSON 格式)	{
	"IAM 平台 RequestId": "55528d12ec8a4c1bb75283b8df71308d",
	"IAM 平台 RemoteUser": "IAM 平台 admin",
	"IAM 平台 RemotePwd": "password",
	"roleId": " 000012"
	}		

响应参数	参数名	中文说明	是否必传
	IAM 平台 RequestId	IAM 平台每次调用接口发送的请求 ID，字段为 String 类型	是
	resultCode	接口调用处理的结果码，0 为正常处理，其它值由应用系统定义。字段为 String 类型。	是
	role	应用返回的角色对象。	是
	message	接口调用处理的信息。字段为 String 类型	是

返回值(JSON 格式)	{
	"role": {
	"roleId": "000012",
	"roleName": "审批员",
	"updateTime":"2020-11-25 14:46:25"
	},
	"resultCode": "0",
	"message": "success",
	"IAM 平台 RequestId": "55528d12ec8a4c1bb75283b8df71308d "
	}		

注意事项	如果接口支持增量回收，查询接口有传 updateTime 的话，查询详情接口必须返回更新时间 updateTime。		

A.2 数据同步-应用系统主动同步模式接口

A.2.1 登录接口

登录接口说明见表A.14。

表A.14 登录接口说明

接口名	LOGIN		
功能说明	LOGIN 是第三方应用调用 IAM 平台身份同步 API 的登录接口		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	systemCode	系统代码，由 IAM 平台提供	是
	integrationKey	集成密钥，集成客户端会自动使用 MD5 加密，由 IAM 平台提供	是
	force	强制登录	是
	timestamp	时间戳，当前客户端系统时间截，集成客户端会自动产生	是

表A.14 （续）

<table>
<tr><td>请求体报文（JSON格式）</td><td colspan="3">{
"systemCode" : "AD",
"integrationKey" : "P@ssW0rd",
"force" : false,
"timestamp" : 1458793365386
}</td></tr>
<tr><td rowspan="14">响应参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>tokenId</td><td>令牌 ID，登录后，每次发送请求，必须附带 tokenId</td><td></td></tr>
<tr><td>systemId</td><td>系统 ID</td><td></td></tr>
<tr><td>systemCode</td><td>系统代码</td><td></td></tr>
<tr><td>systenName</td><td>系统名称</td><td></td></tr>
<tr><td>schemas</td><td>对象 Schema，List<ApiObjectSchema></td><td></td></tr>
<tr><td>enableSync</td><td>是否启用同步</td><td></td></tr>
<tr><td>enablePull</td><td>是否启用下拉</td><td></td></tr>
<tr><td>enablePush</td><td>是否启用上推</td><td></td></tr>
<tr><td>debug</td><td>调试开关</td><td></td></tr>
<tr><td>timestamp</td><td>时间戳</td><td></td></tr>
<tr><td>success</td><td>是否成功</td><td></td></tr>
<tr><td>message</td><td>出错消息</td><td></td></tr>
<tr><td>exception</td><td>异常信息</td><td></td></tr>
<tr><td>返回值（JSON格式）</td><td colspan="3">{
"tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874",
"systemId" : "01E095B613BA46739E814EB7263ED4F1",
"systemCode" : "AD",
"systemName" : "活动目录",
"schemas" : [{
"objectType" : "TARGET_ACCOUNT",
"objectId" : "47D1133D78684657AA2C680B09BD9B49",
"objectCode" : "TESTDB_ACC",
"objectName" : "TESTDB 账户",
"objectAttributes" : [{
"type" : "STRING",
"provisionMethod" : "AUTO",
"reconcileMethod" : "AUTO",
"code" : "_user",
"name" : "用户",
"isRequired" : true,
"isUniqued" : false,
"isMultiValue" : false,
"isEncrypted" : false
}, {
"type" : "STRING",
"provisionMethod" : "AUTO",
"reconcileMethod" : "AUTO",
"code" : "_organization",
"name" : "所属机构",
"isRequired" : false,
"isUniqued" : false,
"isMultiValue" : false,
"isEncrypted" : false
}, {
"type" : "STRING",
"provisionMethod" : "AUTO",</td></tr>
</table>

表A.14 （续）

返回值(JSON格式)	"reconcileMethod" : "AUTO", "code" : "username", "name" : "账户名", "length" : 64, "isRequired" : true, "isUniqued" : false, "isMultiValue" : false, "isEncrypted" : false }, { "type" : "STRING", "provisionMethod" : "AUTO", "reconcileMethod" : "AUTO", "code" : "password", "name" : "密码", "length" : 64, "isRequired" : false, "isUniqued" : false, "isMultiValue" : false, "isEncrypted" : true }, { "type" : "STRING", "provisionMethod" : "AUTO", "reconcileMethod" : "AUTO", "code" : "fullname", "name" : "姓名", "length" : 64, "isRequired" : true, "isUniqued" : false, "isMultiValue" : false, "isEncrypted" : false }, { "type" : "BOOLEAN", "provisionMethod" : "AUTO", "reconcileMethod" : "AUTO", "code" : "isDisabled", "name" : "禁用", "length" : 1, "isRequired" : false, "isUniqued" : false, "isMultiValue" : false, "isEncrypted" : false }, { "type" : "BOOLEAN", "provisionMethod" : "AUTO", "reconcileMethod" : "AUTO", "code" : "isLocked", "name" : "锁定", "length" : 1, "isRequired" : false, "isUniqued" : false,

表A.14 （续）

返回值(JSON格式)	"isMultiValue" : false,
	"isEncrypted" : false
	}, {
	"type" : "TIMESTAMP",
	"provisionMethod" : "AUTO",
	"reconcileMethod" : "AUTO",
	"code" : "createAt",
	"name" : "创建日期",
	"isRequired" : false,
	"isUniqued" : false,
	"isMultiValue" : false,
	"isEncrypted" : false
	}, {
	"type" : "TIMESTAMP",
	"provisionMethod" : "AUTO",
	"reconcileMethod" : "AUTO",
	"code" : "updateAt",
	"name" : "更新日期",
	"isRequired" : false,
	"isUniqued" : false,
	"isMultiValue" : false,
	"isEncrypted" : false
	}],
	"debug" : false,
	"timestamp" : 1458793365386,
	"success" : true
	}

A.2.2 注销接口

注销接口说明见表A.15。

表A.15 注销接口说明

接口名	logout		
功能说明	LOGIN是第三方应用调用IAM平台身份同步API的登录接口		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	tokenId	令牌ID	是
	timestamp	时间戳，当前客户端系统时间截，集成客户端会自动产生	是

请求体报文(JSON格式)	{
	"tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874",
	"timestamp" : 1458793365386
	}		

响应参数	参数名	中文说明	是否必传
	timestamp	时间戳	
	success	是否成功	
	message	出错消息	
	exception	异常信息	

返回值(JSON格式)	{
	"timestamp" : 1458793365386,
	"success" : true
	}		

A.2.3 同步任务接口

同步任务接口说明见表A.16。

表A.16 同步任务接口说明

接口名	syncTask		
功能说明	syncTask 是第三方应用从 IAM 平台进行全量数据同步接口		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	tokenId	令牌 ID	是
	timestamp	时间戳	是
请求体报文(JSON 格式)	{ "tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874", "timestamp" : 1458793365386 }		
响应参数	参数名	中文说明	是否必传
	objectType	对象类型	
	objectCode	对象代码	
	id	对象 ID	
	data	对象数据,Map<String, Object>	
	guid	GUID	
	timestamp	时间戳	
	success	是否成功	
	message	出错消息	
	exception	异常信息	
返回值(JSON 格式)	{ "objectType" : "TARGET_ACCOUNT", "objectCode" : "AD_ACCOUNT", "id" : "47D1133D78684657AA2C680B09BD9B49", "data" : { "_user" : "test02", "_organization" : "集团总部/集团董事会", "username" : "测试账户 02", "password" : "password", "fullname" : "Test02", "isDisabled" : false, "isLocked" : false, "createAt" : "2016-03-16 16:38:55.000", "updateAt" : "2016-03-24 13:33:29.000" }, "guid" : "112", "timestamp" : 1458793365386, "success" : true }		

A.2.4 同步完成接口

同步完成接口说明见表A.17。

表A.17 同步完成接口说明

接口名	syncFinish
功能说明	syncFinish 是第三方应用从 IAM 平台进行全量数据同步完成接口
请求类型	POST

表A.17 （续）

<table>
<tr><td rowspan="10">请求参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>tokenId</td><td>令牌 ID</td><td>是</td></tr>
<tr><td>objectType</td><td>对象类型</td><td>是</td></tr>
<tr><td>objectCode</td><td>对象代码</td><td>是</td></tr>
<tr><td>id</td><td>对象 ID</td><td>是</td></tr>
<tr><td>success</td><td>是否成功</td><td>是</td></tr>
<tr><td>data</td><td>对象数据,当 success=true 时必须 Map<String, Object></td><td></td></tr>
<tr><td>guid</td><td>GUID,当 success=true 时必须</td><td></td></tr>
<tr><td>message</td><td>出错原因,当 success=false 时必须</td><td></td></tr>
<tr><td>timestamp</td><td>时间戳</td><td>是</td></tr>
<tr><td>请求体报文(JSON 格式)</td><td colspan="3"><pre>{
  "tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874",
  "objectType" : "TARGET_ACCOUNT",
  "objectCode" : "AD_ACCOUNT",
  "id" : "47D1133D78684657AA2C680B09BD9B49",
  "success" : true
  "data" : {
    "_user" : "test02",
    "_organization" : "集团总部/集团董事会",
    "username" : "测试账户 02",
    "password" : "password",
    "fullname" : "Test02",
    "isDisabled" : false,
    "isLocked" : false,
    "createAt" : "2016-03-16 16:38:55.000",
    "updateAt" : "2016-03-24 13:33:29.000"
  },
  "guid" : "111",
  "timestamp" : 1458793365386
}</pre></td></tr>
<tr><td rowspan="5">响应参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>timestamp</td><td>时间戳</td><td></td></tr>
<tr><td>success</td><td>是否成功</td><td></td></tr>
<tr><td>message</td><td>出错消息</td><td></td></tr>
<tr><td>exception</td><td>异常信息</td><td></td></tr>
<tr><td>返回值(JSON 格式)</td><td colspan="3"><pre>{
  "timestamp" : 1458793365386,
  "success" : true
}</pre></td></tr>
</table>

A.2.5 下拉任务接口

下拉任务接口说明见表A.18。

表A.18 下拉任务接口说明

<table>
<tr><td>接口名</td><td colspan="3">pullTask</td></tr>
<tr><td>功能说明</td><td colspan="3">pullTask 是第三方应用从 IAM 平台进行增量数据同步接口</td></tr>
<tr><td>请求类型</td><td colspan="3">POST</td></tr>
<tr><td rowspan="3">请求参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>tokenId</td><td>令牌 ID</td><td>是</td></tr>
<tr><td>timestamp</td><td>时间戳，当前客户端系统时间截，集成客户端会自动产生</td><td>是</td></tr>
</table>

表A.18 （续）

<table>
<tr><td>请求体报文(JSON格式)</td><td colspan="3">{
"tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874",
"timestamp" : 1458793365386
}</td></tr>
<tr><td rowspan="12">响应参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>taskId</td><td>任务 ID</td><td></td></tr>
<tr><td>objectType</td><td>对象类型</td><td></td></tr>
<tr><td>objectCode</td><td>对象代码</td><td></td></tr>
<tr><td>effectOn</td><td>作用点</td><td></td></tr>
<tr><td>data</td><td>对象数据，Map<String, Object></td><td></td></tr>
<tr><td>guid</td><td>GUID</td><td></td></tr>
<tr><td>id</td><td>对象 ID</td><td></td></tr>
<tr><td>timestamp</td><td>时间戳</td><td></td></tr>
<tr><td>success</td><td>是否成功</td><td></td></tr>
<tr><td>message</td><td>出错消息</td><td></td></tr>
<tr><td>exception</td><td>异常信息</td><td></td></tr>
<tr><td>返回值(JSON格式)</td><td colspan="3">{
"taskId" : "BCCC21EAFAEC40D4AE899D1A0B861B43",
"objectType" : "TARGET_ACCOUNT",
"objectCode" : "TESTDB_ACC",
"effectOn" : "UPDATED",
"data" : {
"_user" : "test02",
"_organization" : "213",
"username" : "测试账户 02",
"password" : "password",
"fullname" : "Test02",
"isDisabled" : false,
"isLocked" : false,
"createAt" : "2016-03-16 16:38:55.000",
"updateAt" : "2016-03-24 20:07:22.000"
},
"guid" : "112",
"id" : "47D1133D78684657AA2C680B09BD9B49",
"timestamp" : 1458793365386,
"success" : true
}</td></tr>
</table>

A.2.6 下拉完成接口

下拉完成接口说明见表A.19。

表A.19 下拉完成接口说明

<table>
<tr><th>接口名</th><th colspan="3">PullFinish</th></tr>
<tr><td>功能说明</td><td colspan="3">PullFinish 是第三方应用从 IAM 平台进行增量数据同步接口</td></tr>
<tr><td>请求类型</td><td colspan="3">POST</td></tr>
<tr><td rowspan="6">请求参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>tokenId</td><td>令牌 ID</td><td>是</td></tr>
<tr><td>taskId</td><td>任务 ID</td><td>是</td></tr>
<tr><td>success</td><td>是否成功</td><td>是</td></tr>
<tr><td>data</td><td>对象数据,当 success=true 时必须 Map<String, Object></td><td></td></tr>
<tr><td>guid</td><td>GUID</td><td></td></tr>
</table>

表A.19 （续）

<table>
<tr><td rowspan="2">请求参数</td><td>message</td><td>出错原因</td><td></td></tr>
<tr><td>timestamp</td><td>时间戳</td><td>是</td></tr>
<tr><td>请求体报文 (JSON格式)</td><td colspan="3"><pre>{
  "tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874",
  "taskId" : "47D1133D78684657AA2C680B09BD9B49",
  "success" : true
  "data" : {
    "_user" : "test02",
    "_organization" : "213",
    "username" : "测试账户 02",
    "password" : "password",
    "fullname" : "Test02",
    "isDisabled" : false,
    "isLocked" : false,
    "createAt" : "2016-03-16 16:38:55.000",
    "updateAt" : "2016-03-24 20:07:22.000"
  },
  "guid" : "111",
  "timestamp" : 1458793365386
}</pre></td></tr>
<tr><td rowspan="5">响应参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>timestamp</td><td>时间戳</td><td></td></tr>
<tr><td>success</td><td>是否成功</td><td></td></tr>
<tr><td>Message</td><td>出错消息</td><td></td></tr>
<tr><td>Exception</td><td>异常信息</td><td></td></tr>
<tr><td>返回值(JSON格式)</td><td colspan="3"><pre>{
  "timestamp" : 1458793365386,
  "success" : true
}</pre></td></tr>
</table>

A.2.7 上推任务接口

上推任务接口说明见表A.20。

表A.20 上推任务接口说明

<table>
<tr><th>接口名</th><th colspan="3">pushTask</th></tr>
<tr><td>功能说明</td><td colspan="3">pushTask 是第三方应用将变更数据同步到 IAM 平台的同步接口</td></tr>
<tr><td>请求类型</td><td colspan="3">POST</td></tr>
<tr><td rowspan="8">请求参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>tokenId</td><td>令牌 ID</td><td>是</td></tr>
<tr><td>objectType</td><td>对象类型</td><td>是</td></tr>
<tr><td>objectCode</td><td>对象代码</td><td>是</td></tr>
<tr><td>data</td><td>对象数据，Map<String, Object></td><td>是</td></tr>
<tr><td>guid</td><td>GUID</td><td></td></tr>
<tr><td>timestamp</td><td>时间戳</td><td>是</td></tr>
</table>

表A.20 （续）

<table>
<tr><td>请求体报文 (JSON格式)</td><td colspan="3"><pre>{
  "tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874",
  "objectType" : "TARGET_ACCOUNT",
  "objectCode" : "TESTDB_ACC",
  "effectOn" : "UPDATED",
  "data" : {
    "_user" : "test02",
    "_organization" : "213",
    "username" : "测试账户02",
    "password" : "password",
    "fullname" : "Test02",
    "isDisabled" : false,
    "isLocked" : false,
    "createAt" : "2016-03-16 16:38:55.000",
    "updateAt" : "2016-03-24 20:07:22.000"
  },
  "timestamp" : 1458793365386,
  "success" : true
}</pre></td></tr>
<tr><td rowspan="10">响应参数</td><td>参数名</td><td>中文说明</td><td>是否必传</td></tr>
<tr><td>objectType</td><td>对象类型</td><td>是</td></tr>
<tr><td>objectCode</td><td>对象代码</td><td>是</td></tr>
<tr><td>data</td><td>对象数据，Map<String, Object></td><td>是</td></tr>
<tr><td>guid</td><td>GUID</td><td></td></tr>
<tr><td>id</td><td>对象 ID</td><td>是</td></tr>
<tr><td>timestamp</td><td>时间戳</td><td>是</td></tr>
<tr><td>success</td><td>是否成功</td><td>是</td></tr>
<tr><td>message</td><td>出错消息</td><td></td></tr>
<tr><td>exception</td><td>异常信息</td><td></td></tr>
<tr><td>返回值(JSON格式)</td><td colspan="3"><pre>{
  "objectType" : "TARGET_ACCOUNT",
  "objectCode" : "TESTDB_ACC",
  "data" : {
    "_user" : "test02",
    "_organization" : "213",
    "username" : "测试账户02",
    "password" : "password",
    "fullname" : "Test02",
    "isDisabled" : false,
    "isLocked" : false,
    "createAt" : "2016-03-16 16:38:55.000",
    "updateAt" : "2016-03-24 20:07:22.000"
  },
  "guid" : "112",
  "id" : "47D1133D78684657AA2C680B09BD9B49",
  "timestamp" : 1458793365386,
  "success" : true
}</pre></td></tr>
</table>

A.2.8 上推完成接口

上推完成接口说明见表A.21。

表A.21 上推完成接口说明

接口名	pushFinish		
功能说明	pushFinish 是第三方应用将变更数据同步到 IAM 平台的同步完成接口		
请求类型	POST		
请求参数	参数名	中文说明	是否必传
	tokenId	令牌 ID	是
	objectType	对象类型	是
	objectCode	对象代码	是
	timestamp	时间戳，当前客户端系统时间截，集成客户端会自动产生	是
请求体报文（JSON 格式）	{ "tokenId" : "8e586926-c308-4496-9398-bad7f8ff7874", "objectType" : "TARGET_ACCOUNT", "objectCode" : "TESTDB_ACC", "timestamp" : 1458793365386 }		
响应参数	参数名	中文说明	是否必传
	objectType	对象类型	是
	objectCode	对象代码	是
	timestamp	时间戳	是
	success	是否成功	是
	message	出错消息	
	exception	异常信息	
返回值（JSON 格式）	{ "objectType" : "TARGET_ACCOUNT", "objectCode" : "TESTDB_ACC", "timestamp" : 1458793365386, "success" : true }		

A.3 认证对接-标准协议对接模式接口

A.3.1 授权接口

授权接口说明见表A.22。

表A.22 授权接口说明

接口名	authorize		
功能说明	获取授权码接口		
请求类型	GET		
参数	参数名	中文说明	描述
	client_id	应用标识	客户端应用注册 ID(IAM 平台提供)
	redirect_uri	跳转地址	跳转地址(uri 编码)
	response_type	响应类型	code
	state	任意值	用于保持请求和回调的状态，在回调时，会在 Query Parameter 中回传该参数。开发者可以用这个参数验证请求有效性，也可以记录用户请求授权页前的位置。这个参数可用于防止跨站请求伪造（CSRF）攻击
返回值	参数正确登录成功时，会跳转到回调地址，携带参数 code 和 state。		

表A.22 （续）

描述	此接口是浏览器 redirect 跳转方式调用。 如果用户已完成过登录，访问此地址则会直接跳转到指定的回调地址，带上 code。如果请求参数中传入了 state，这里会带上原始的 state 值。 如果用户未登录，访问此地址会跳转至登录页面，显示应用配置的认证方式，用户完成登录后跳转到指定的回调地址，带上 code。如果请求参数中传入了 state，这里会带上原始的 state 值。

A.3.2 获取接口

获取接口说明见表A.22。

表A.23 获取接口说明

接口名	getToken		
功能说明	获取 access_token 接口		
请求类型	POST		
参数	参数名	中文说明	描述
	client_id	应用标识	客户端应用注册 ID(IAM 平台提供)
	client_secret	密钥	客户端应用注册密钥(IAM 平台提供)
	code	授权码	调用 authorize 接口获得的授权码 code
	grant_type	认证方式	请求类型，默认 authorization_code

返回值	类型：JSON
	正确返回时：
	{
	"access_token": "0255c4e849d00d360249b7cf0db7beb1",
	"refresh_token": "0fd421e3e40693536fef7565ffc919f1",
	"uid": "20201125144720612-EEF2-5A66B6EAB",
	"expires_in": 60
	}		

描述	OAuth 获取授权 Token 接口可以获得 access_token、expires_in、refresh_token、uid。 access_token 用于获取用户信息，expires_in 是 access_token 有效时长，时长在 console 应用注册时配置。 refresh_token 可在 access_token 到期后进行刷新续期，uid 为用户 id。		

A.3.3 刷新接口

刷新接口说明见表A.24。

表A.24 刷新接口说明

接口名	refreshToken		
功能说明	刷新 access_token 接口		
请求类型	POST		
参数	参数名	中文说明	描述
	client_id	应用标识	客户端应用注册 ID(IAM 平台提供)
	client_secret	密钥	客户端应用注册密钥(IAM 平台提供)
	refresh_token		刷新 token 授权码
	grant_type	认证方式	请求类型，默认 refresh_token

表A.24 （续）

返回值	类型：JSON
	正确返回时：
	{
	"access_token": "07111c4e2d536759326f281a8f363937",
	"refresh_token": "e8e2bef0da609fd13b086415e77e3638",
	"uid": "20171123092851812-3272-F82D3EAC0",
	"expires_in": 43200
	}

描述	刷新 Token 接口可以对授权 access_token 有效期做续期操作

A.3.4 验证接口

验证接口说明见表A.25。

表A.25 验证接口说明

接口名	checkTokenValid		
功能说明	验证 access_token 接口，检查 token 有效性		
请求类型	GET		
参数	参数名	中文说明	描述
	access_token	token 授权码	token 授权码

返回值	类型：JSON
	正确返回时：
	{
	"result":"true"
	}		

描述	result 为 true 表示有效		

A.3.5 获取认证用户接口

获取认证用户接口说明见表A.26。

表A.26 获取认证用户接口说明

接口名	getUserInfo		
URL Path	获取用户信息接口，验证参数有效性,根据应用配置的属性权限列表，查询用户信息返回		
请求类型	GET		
请求示例	https://{host}:{port}/idp/oauth2/getUserInfo?access_token=46e4d79fc6384105e157465032c9684e&client_id=20170830061623854-E5A8-B2FABDC35		
参数	参数名	中文说明	描述
	access_token		token 授权码
	client_id	应用标识	客户端应用注册 ID(IAM 平台提供)

返回值	类型：JSON
	正确返回时：
	{
	"spRoleList": [
	"zhaoyun"
	],
	"uid": "20201125144720612-EEF2-5A66B6EAB",
	"mail": "zhaoyun@qq.com",
	"displayName": "赵云",
	"loginName": "zhaoyun",
	"mobile": null,
	"employeeNumber": null
	}		

表A.26 （续）

描述	loginName 对应登录的用户名 spRoleList 对应集成的应用系统账号的账号名(应用账号与用户名不一致或多账号时使用,数组格式)

A.4 认证对接-认证接口对接模式接口

A.4.1 认证接口

认证接口说明见表A.27。

表A.27 认证接口说明

接口名	authenticate		
功能说明	调用认证接口,验证 appId 是否有效，用户名/密码是否有效		
请求类型	GET、POST		
参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(IAM 平台提供)
	userName	用户名	用户登录名
	password	密码	当采用用户名+密码认证时，传入密码 当采用用户名+短信认证时，此参数被忽略 当采用用户名+OTP 认证时，此参数被忽略 当采用用户名+密码+OTP 认证时，传入密码
	checkcode	短信验证码	当采用用户名+密码/OTP 认证时，此参数被忽略 当采用用户名+短信认证时，传入短信验证码。短信验证码需要先通过“发送短信验证码”接口发到用户手机上。
	remoteIp	客户端 IP	必传
	j_otpcode	OTP 动态码	当采用用户名+密码/短信认证时，此参数被忽略 当采用用户名+OTP 认证时，传入 OTP 动态码。 当采用用户名+密码+OTP 认证时，传入 OTP 动态码
	authnMethod	认证方式	当采用用户名+密码认证时，传入 UsernamePassword 当采用用户名+密码+OTP 双因素认证时，传入 UsernamePassword 当采用用户名+短信验证码认证时，传入 UsernameSM 当采用用户名+OTP 认证时，传入 UsernameOTP

返回值	用户密码认证通过时：
	{
	"data": {
	"tokenId":
	"MTI3LjAuMC4x|NGY3ZGJkNzkzYmQwMmE5ZTAwZGQ3YmNlYTM3YTI3M2JhYzc1NjkxOThmMWMwMDE0OGQ3NmQzNmUxMmU2MDcyZQ==|/1xHjeNfqenI6T9khG5RUntJcnU="
	}
	}		

A.4.2 验证票据接口

验证票据接口说明见表A.28。

表A.28 验证票据接口说明

接口名	isTokenValid		
功能说明	验证票据接口，验证 appId 是否有效 ,验证 tokenId 是否有效		
请求类型	POST、GET		
参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(IAM 平台提供)
	tokenId	用户票据	
	remoteIp	客户端 IP	

表A.28 （续）

返回值	类型：JSON 正确返回时： {"data":{"isValid":true}}

A.4.3 获取用户信息接口

获取用户信息接口说明见表A.29。

表A.29 获取用户信息接口说明

接口名	GetUserAttributes		
功能说明	获取用户信息接口		
请求类型	POST、GET		
参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(IAM 平台提供)
	tokenId	用户票据	
	remoteIp	客户端 IP	
	attributeNames	属性名	逗号分割字符串：“spOrgCodePath,sn,givenName,uid” 该参数没有时使用 IDP 默认的用户属性

返回值	类型：JSON
	正确返回时：
	{
	"data": {
	"tokenId":
	"MTI3LjAuMC4x|OWMyNzZkZmI3OGRjYjM5NDZkMjY0YmMyMWFiNGE2MDBiMTE3OTAwZmUwMzkwMzU1YjQ1NWNmN2RlMTc1NDBlMg==|pbE+SW/eiXlpzVG4V8QbA57v7TM=",
	"attributes": {
	"spRoleList": [
	"zhaoyun"
	],
	"uid": "20201125144720612-EEF2-5A66B6EAB",
	"mail": "zhaoyun@qq.com",
	"displayName": "赵云",
	"loginName": "zhaoyun",
	"secAccValid": 1,
	"mobile": "15411112222",
	"employeeNumber": null
	}
	}
	}		

A.4.4 获取票据接口

获取票据接口说明见表A.30。

表A.30

接口名	getToken		
功能说明	获取用户票据接口		
请求类型	POST、GET		
参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(IAM 平台提供)
	jsonpCallback	回调函数	Jsonp 回调函数，测试时可不填忽略不计
	remoteIp	客户端 IP	

表A.30 （续）

返回值	tokenId: 用户票据
返回 URL	有 cookie 时: {"data":{"isValid":true,"tokenid":"MTI3LjAuMC4x|MDE4ZTI1ODM3ZjRjNmQxNzk3NzExNzA4MGVmMjIzZDgzZTU3NzU3NjAxMDEwMGU1NTM1ZTljYWUxNjE0OGQyNw==|mnY4Qafcdz9hc2gdGv2DSq1tYEo="}} 没有 cookie 时: {} appUrl 参数错误或异常时不跳转且页面显示： ”invalid_remoteIp” 客户端 IP 和 cookie 认证的 IP 不匹配 ”invalid_appId_error” appId 不存在或不匹配

A.4.5 设置票据接口

设置票据接口说明见表A.31。

表A.31 设置票据接口说明

接口名	setToken		
功能说明	设置票据，写浏览器 SSO Cookie		
请求类型	GET		
参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(IAM 平台提供)
	tokenId	用户票据	
	jsonpCallback	回掉函数	Jsonp 回调函数
	remoteIp	客户端 IP	
返回值	无		
返回 URL	appUrl 参数错误或异常时不跳转且页面显示”invalid_appId_error”、”wrong_tokenId”等错误信息		

A.4.6 登出接口

登出接口说明见表A.32。

表A.32 登出接口说明

接口名	logout
功能说明	登出接口
请求类型	https://{host}:{port}/apphub/logout
注意事项	需要 IAM 平台在 apphub 配置白名单，不拦截 此接口需要清除当前浏览器存在的用户会话信息，因此需要前端使用此接口跳转，例如 jsp 直接跳转或 ajax 调用等，后台 httpclient 方式会存在问题