[SRIAM-GYSJSMS]

尚融身份识别与访问管理：概要设计说明书

[SRIAM- GYSJSMS] - v20170809
尚融身份识别与访问管理：概要设计说明书

发布日期：2017/08/09
发布范围：研发部 IAM 项目组

版本修订记录

日期	版本	作者	描述
2016/12/26	2.0	胡锦亚	初稿。[2.0.0_20161226] 确定组织架构接口。[2.0.1_20170511] 完善整体架构。[2.0.2_20170605] 增加产品许可证管理。[2.0.3_20170720] 规范化 SSO 接口。[2.0.4_20170809]

目 录

1 需求分析

1.1 功能需求

1.1.1 用户管理

分域的树形组织架构,顶级目录代表域,每个域拥有自己的认证方式、用户组织、以及单点登录应用列表。支持运营和集团分公司的独立管理机制。

用户接口：支持用户自我信息查询、编辑接口。

组织接口：提供组织架构信息获取接口。

1.1.2 认证管理

系统用户身份可采用数据库、AD、LDAP、动态口令、数字证书、二维码，短信等多种认证方式，并可以继续扩展，对不同级别的用户可以扩展其他的认证方式。

提供可配置的认证接口，对单点登录模块提供的认证信息进行认证，成功返回用户 ID 号，失败返回错误原因。

1.1.3 单点登录

参照 CAS 接口标准，提供统一登录、认证、退出功能。

登录接口：能够接受多种认证信息，包括用户名、密码、验证码、短信等信息。将信息提交给认证管理模块进行认证，成功返回 TGC（Ticket Granted Cookie）,服务端保存对应的 TGT（Ticket Granting Ticket）的，失败返回错误信息。

验证接口：用于用户应用系统服务端对 ST（Service Ticket ）进行验证是否合法。

退出接口：返回已登录系统的登出接口，由客户端执行登录接口调用完成统一退出。

1.1.4 授权管理

基于用户组织架构、角色、访问控制策略的权限管理，提供默认系统

策略，用户可以自定义策略。

访问策略基于类型（禁止或允许）、资源（URL 资源）、方法（获取、增加、删除、修改等）、条件（资源条件限制，IP 限制等）。所有需要统一授权的资源必须支持 OAUTH 2.0 规范和上述访问策略。

1.2 其它需求

（1）规范性

尽可能遵循 OPENID、OAUTH2.0、SAML 等业界标准。

（2）数据安全性

存储、传输，密码及密匙安全性。

用户中心所有接口采用 HTTPS。

（3）可扩展性

功能模块化，界面、功能变动时底层功能模块尽可能保证可以重用。

（4）系统高可用性

支持集群部署，通过负载均衡接入。

2 整体设计

2.1 方案分析

2.1.1 用户管理

用户中心提供以域为顶级目录的树形组织架构，支持数据库、LDAP 导入用户,允许开放用户注册功能,可通过配置注册后是否需要管理员审核。

2.1.2 认证管理

认证中心仅提供身份认证功能，兼容多种身份认证方式，单点登录模块检测到用户未登录时,重定向到认证接口,若需多种认证方式采用循环，注意重定向时必须加上原来 URL 参数，否则认证成功后无法跳回原来的页面。

认证方式：密码认证，U-KEY 数字证书，短信动态码，二维码扫描，指纹，OTP 口令，人脸识别，虹膜。

2.1.3 单点登录

单点登录采用 CAS 的接口规范，增加日志记录。

常用的 CAS 只有三个接口：登录，验证，退出，其实不太复杂，但是 CAS 为了兼容各种标准，提供很多接口化的东西，架构变得较为复杂。但有些基本的功能确还不支持，比如验证码功能，所以考虑不直接使用 CAS，参照 CAS 的原理实现以上三个接口即可。

2.1.4 授权管理

基于用户组织架构、角色、访问控制策略的权限管理。采用 OAUTH 2.0 统一授权框架，用户身份认证功能由单点登录模块提供，ACCESS_TOKEN 可兼容 JWT。

应用系统在接入用户中心时可以选择使用统一授权或者自己的权限管理系统。

2.2 总体架构

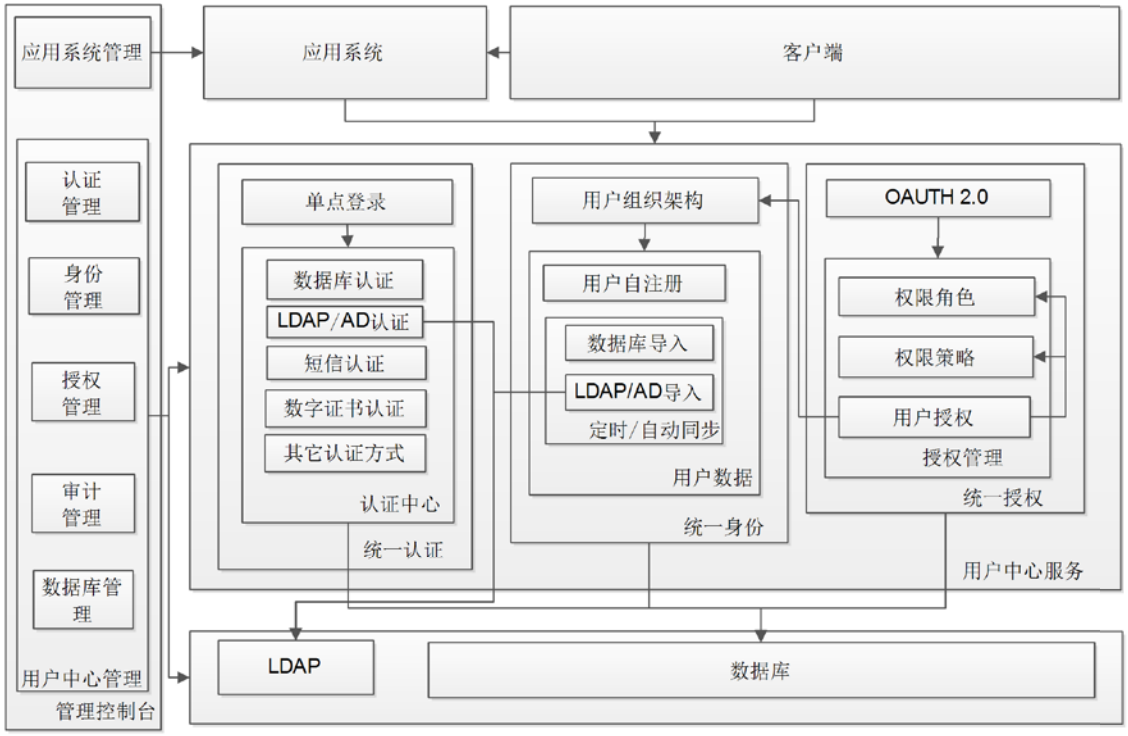

图 2- 总体架构

2.3 工作流程

2.3.1 二维码认证

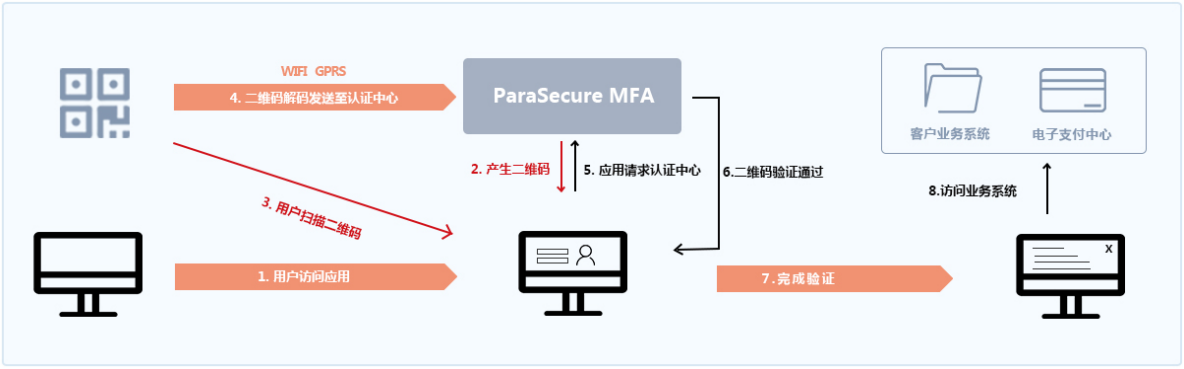

图 2- 二维码验证流程图

2.3.2 单点登录

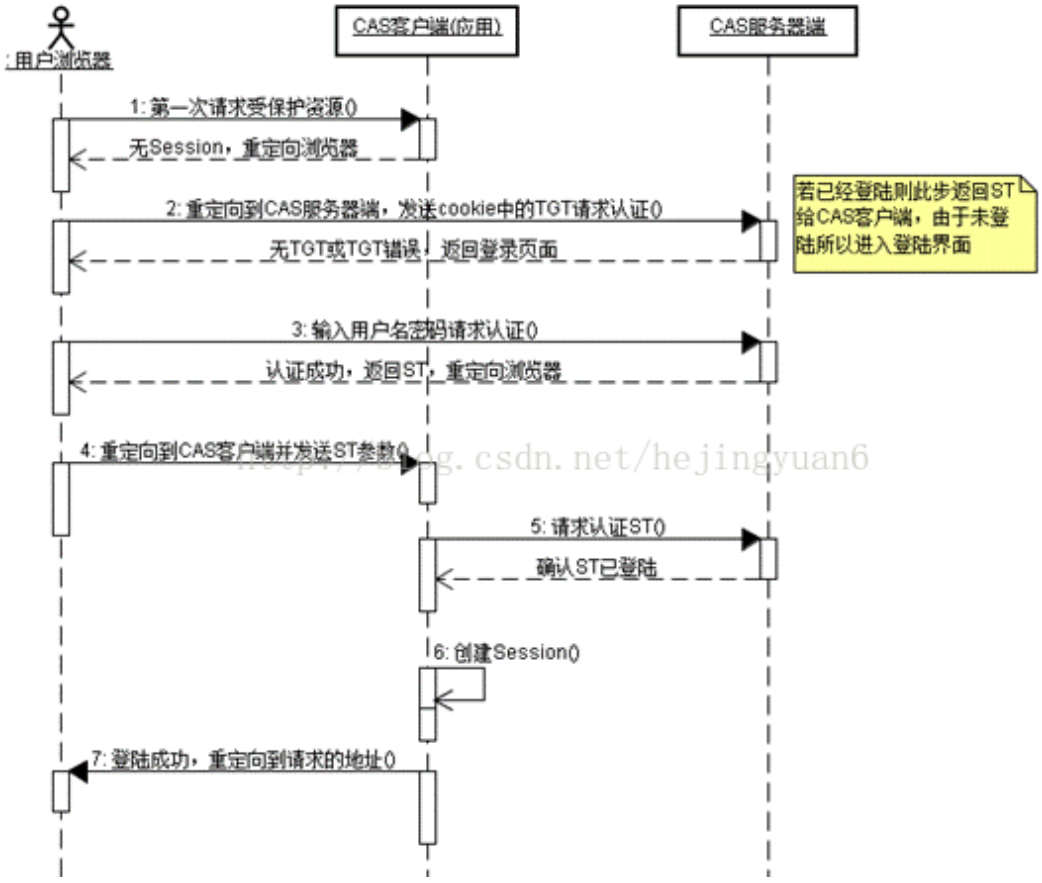

图 2- 单点登录流程图

2.3.3 单点退出

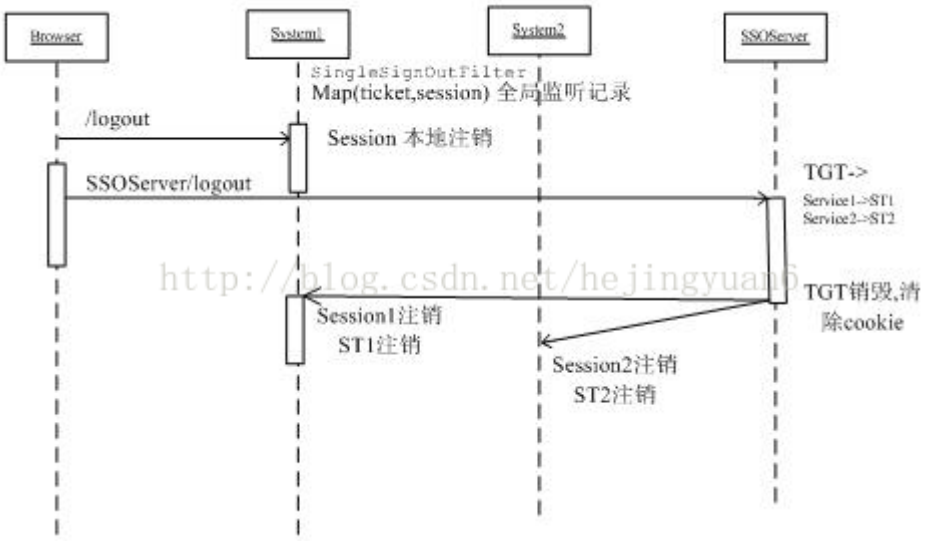

图 2- 单点退出流程图

2.3.4 统一授权

（1)服务提供方,用户使用服务提供方来存储受保护的资源,如照片，视频，联系人列表。

（2）用户，存放在服务提供方的受保护的资源的拥有者。

（3）客户端，要访问服务提供方资源的第三方应用，通常是网站。在认证过程之前，客户端要向服务提供者申请客户端标识。

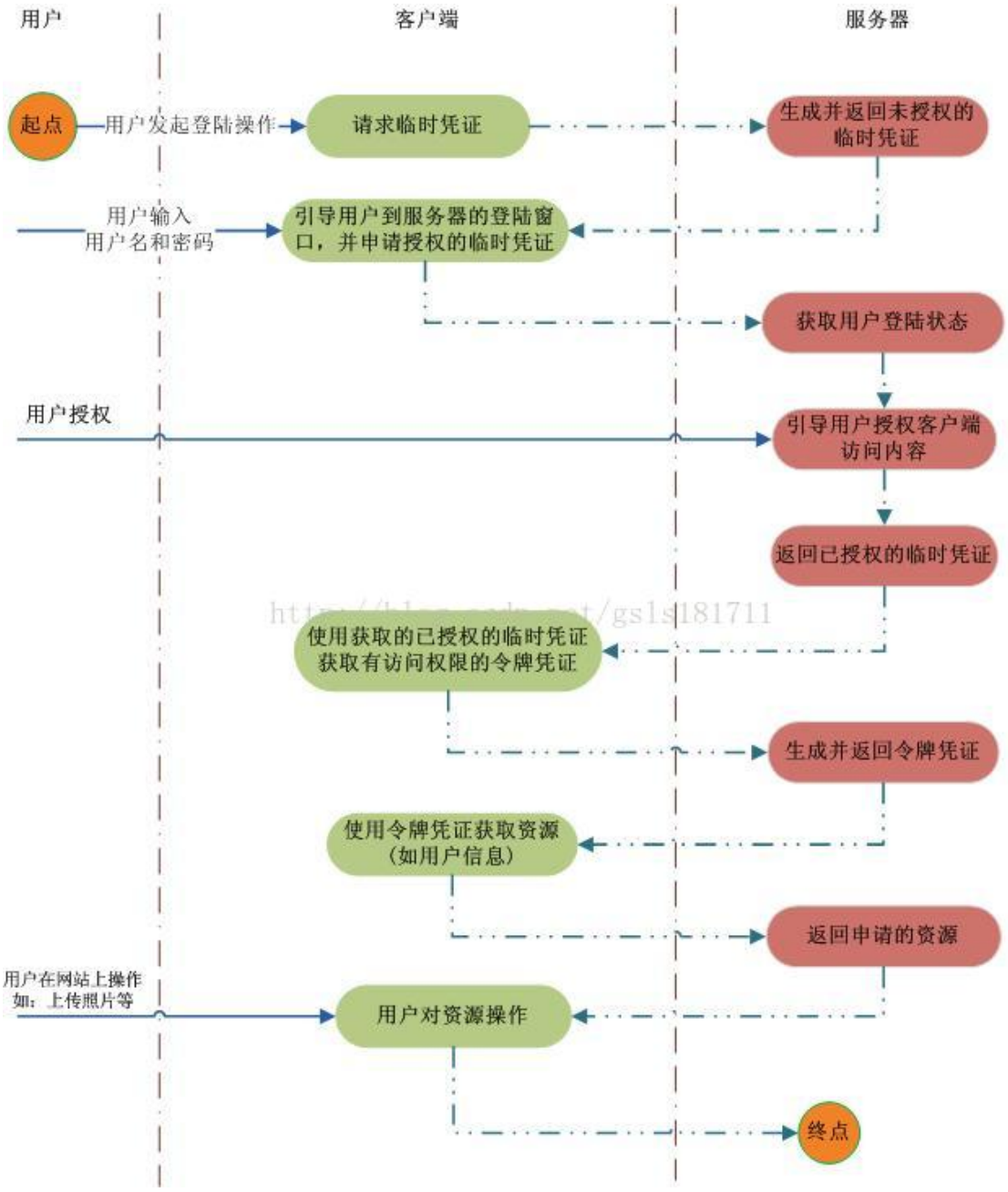

图 2- 统一授权流程图

用户访问客户端的网站，想操作用户存放在服务提供方的资源。

客户端向服务提供方请求一个临时令牌。

服务提供方验证客户端的身份后，授予一个临时令牌。

客户端获得临时令牌后，将用户引导至服务提供方的授权页面请求用户授权。在这个过程中将临时令牌和客户端的回调连接发送给服务提供方。

用户在服务提供方的网页上输入用户名和密码，然后授权该客户端访问所请求的资源。

授权成功后，服务提供方引导用户返回客户端的网页，并返回已授权的临时凭证。

客户端根据已授权的临时令牌从服务提供方那里获取访问令牌。

服务提供方根据临时令牌和用户的授权情况授予客户端访问令牌。

客户端使用获取的访问令牌访问该用户存放在服务提供方上的受保护的资源。（客户端只能访问给予它授权的用户的资源信息）

3 接口设计

3.1 接口概览

3.1.1 接口列表

表 2-1 IAM 接口列表

资源	操作	描述
domain	get	获取域信息
	list	获取域列表
oauth2	authorize	获取统一授权授权码
	introspect	验证是否具备访问资源的权限
	token	获取或者刷新统一授权授令牌
org	get	获取组织详细信息
	list	获取组织列表
product	get	获取产品详细信息
	list	获取产品列表
sso	login	验证单点登录密码
	logout	退出单点登录
	service_validate	用于业务系统向 SSO 验证 session ticket
user	get	获取用户详细信息

3.1.2 接口返回错误码

表 2-2 IAM 接口返回错误码

响应码	错误码	描述
400(BAD_REQUEST)	40010	LT 无效

	40011	TGC 不存在
	40012	TGC 已过期
	40013	用户名或者密码错误
	40014	用户不存在
	40015	退出错误
	40016	服务错误
	40017	服务认证错误
	40018	服务格式错误
401(UNAUTHORIZED)	40101	
403(FORBIDDEN)	40301	
404(NOT_FOUND)	40401	
500(INTERNAL_ERROR)	50001	

3.2 单点登录

3.2.1 获取登录 LT

请求(GET)：

http://<HOST>:<PORT>/sunruniam/sso/login?service=<SERVICE>

参数说明：

service:服务名，用于业务系统的唯一识别标识。

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
    "lt":"<LOGIN_TCIKET>",
}
```

3.2.2 登录验证

请求(POST)：

http://<HOST>:<PORT>/sunruniam/sso/login?

service=<SERVICE>&lt=<LOGIN_TICKET>&login_type=1&
username=<USERNAME>&password=<PASSWORD>

参数说明：

service:服务名，用于业务系统的唯一识别标识。

lt:防止重放攻击。

login_type:登录方式。1 表示用户名、密码登录，2,4,8...二进制的每一位代表一种验证方式，便于多种验证方式的组合。

username:用户名

password:密码

成功返回：

HTTP/1.1 302 Moved Temporarily

Location: <SERVICE>?st=<SERVICE_TICKET>

Set-Cookie:tgc=<GRANTED_TICKET>

3.2.2 获取 ST

请求(POST)：

http://<HOST>:<PORT>/sunruniam/sso/login?service=<SERVICE>&tgc=<GRANTED_TICKET>

参数说明：

service:服务名，用于业务系统的唯一识别标识。

tgc:若为 C/S 应用，可以通过参数传递给认证服务端；B/S 应用直接以 COOKIE 的方式传递参数给认证服务端。

成功返回：

HTTP/1.1 302 Moved Temporarily

Location: <SERVICE>?st=<SERVICE_TICKET>

3.2.3 验证 ST

请求(GET)：

http://<HOST>:<PORT>/sunruniam/sso/service_validate?st=<SESSION_TICKET>&service_logout=<SERVICE_LOGOUT>&session_name=<SESSION_NAME>&session_id=<SESSION_ID>

参数说明：

st:服务登录会话标识。

service_logout:可选参数，服务退出回调地址。若未指定表明统一退出时业务系统不需要执行退出操作。

session_name：可选参数，服务会话名称，根据服务环境确定， 如PHPSESSIONID,JSESSIONID。若未指定由 SSO 服务器生成。

session_id：可选参数，服务器会话标识，可以由服务指定。若未指定由 SSO 服务器生成。

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
    "user_id":"<USER_ID>",
    "session_name":"<SESSION_NAME>",
    "session_id":"<SESSION_ID>"
}
```

3.2.4 退出登录

请求(POST)：

http://<HOST>:<PORT>/sunruniam/sso/logout?tgc=<GRANTED_TICKET>&service=<SERVICE>

参数说明：

tgc:若为 C/S 应用，可以通过参数传递给认证服务端；B/S 应用直接以 COOKIE 的方式传递参数给认证服务端。

service: 服务地址，可选参数，用于退出成功后跳转地址。

成功返回：

（1）若服务地址为空，退出成功后返回 200.

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:0

{ "error":0, "message":"Successed." }
```

（2）若服务地址不为空，退出成功后 302 跳转到指定的服务地址。

```
HTTP/1.1 302 Moved Temporarily
Location: <SERVICE>
```

3.3 统一授权

3.3.1 获取授权码

请求(GET)：

http://<HOST>:<PORT>/sunruniam/oauth2/token

参数说明：

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
    "access_token":"<ACCESS_TOKEN>",
    "expires_in": 7200
}
```

3.3.2 获取令牌

请求(GET)：

http://<HOST>:<PORT>/sunruniam/oauth2?action=token&grant_type=
client_credential&access_key=<ACCESS_KEY>&access_secret=<ACCESS_SECRET>

参数说明：

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
    "access_token":"<ACCESS_TOKEN>",
    "expires_in": 7200
}
```

3.4 用户管理

3.4.1 获取域列表

请求(GET)：

http://<HOST>:<PORT>/sunruniam/domian/list?access_token=<ACCESS_TOKEN>

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
     "domains":[
         {
             "id":1,
             "name":"domian1",
          }
     ]
}
```

3.4.2 获取域详细信息

请求(GET)：

http://<HOST>:<PORT>/sunruniam/domain/get?access_token=<ACCESS_TOKEN>&domain_id=<DOMAIN_ID>

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
     "name":"domain1
      ...
}
```

3.4.3 获取组织列表

请求(GET)：

http://<HOST>:<PORT>/sunruniam/org/list?access_token=<ACCESS_TOKEN>&domain_id=<DOMAIN_ID>&org_id=<ORG_ID>&type=<TYPE>&depth=<DEPTH>

参数说明：

domain_id:表示域 id。

org_id:表组织 id；若 org_id 为 0 或者不带 org_id 参数，表示一级组织。

type：取值为 0、1、2；0 表示只返回用户，1 表示只返回组织，2 表示返回所有用户和组织。

depth: 要求查询的层次，最少一层，0 代表全部子对象。

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
     "orgs":[
        {
             "id":1,
             "name":"org1
             "type":"org",
             "children":[
                 ...
             ]
        },
        {
             "id":2,
             "name":"user1",
             "type":"user"
        }
     ]
}
```

3.4.4 获取组织详细信息

请求(GET)：

http://<HOST>:<PORT>/sunruniam/org/get?access_token=<ACCESS_TOKEN>&org_id=<ID>

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
     "name":"organization1",
      ...
}
```

3.4.5 获取用户详细信息

请求(GET)：

http://<HOST>:<PORT>/sunruniam/user/get?access_token=<ACCESS_TOKEN>&user_id=<USER_ID>

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
     "name":"user1",
     "sex":,"男",
     "email":"xxx@163.com",
      ...
}
```

3.5 其它接口

3.5.1 获取产品列表

请求(GET)：

http://<HOST>:<PORT>/sunruniam/product/list?access_token=<ACCESS_TOKEN>

参数说明：

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx

{
    products:[
        {
            "name":"",
            "admin_addr":"",
            "service_addr":""
        }
    ]
}
```

3.5.2 获取产品详细信息

请求(GET)：

http://<HOST>:<PORT>/sunruniam/product/list?access_token=<ACCESS_TOKEN>

参数说明：

成功返回：

```
HTTP/1.1 200 ok
Content-Type:application/json
Content-Length:xxx
```

4 核心服务设计

5 管理平台设计

5.1 功能架构

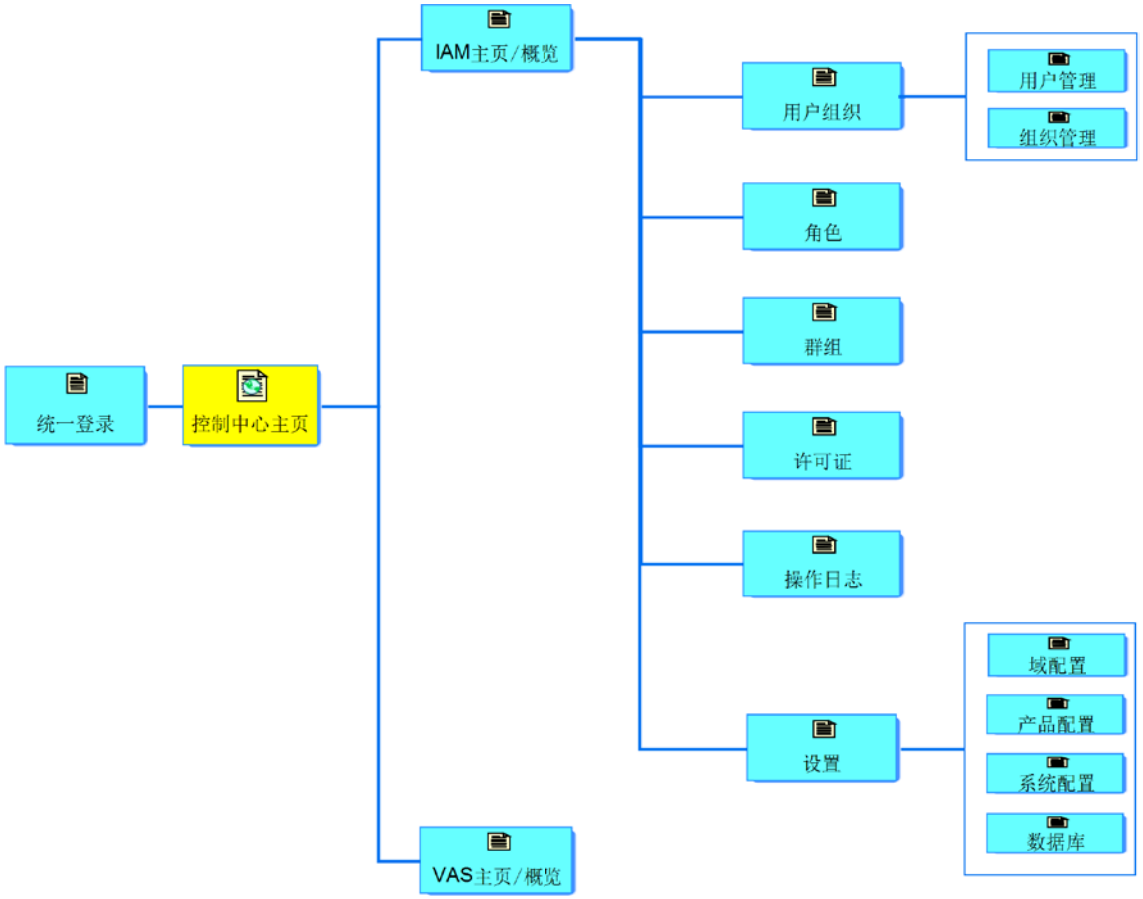

图 5-1 管理平台功能架构

控制中心登录、导航使用流程：

（1）浏览器访问 IAM 或者应用系统，系统检测到未登录跳转至控制中心登录页面，附带重定向页面地址。

（2）输入用户名和密码，提交给用户中心后台服务验证，验证成功返回附加验证方式。

（3）客户端完成附加验证，登录成功，并跳转至用户初始化访问页面。

IAM 管理系统使用流程：

（1）配置数据库，备份数据，还原数据。

（2）系统全局配置，系统 logo,系统名等。

（3）产品配置，产品类型、名称（英文，唯一）、备注、管理平台地址、服务入口地址。

（4）新建域。

域名：域名、描述信息。

安全认证：AD 域/本地数据库、附加验证方式（短信、二维码、UKEY）。

个性化设置：会话超时、文件上传限制、用户密码错误锁定、客户端安全信息绑定。

（5）选择要管理的域，用户组织、用户的导入或新建。

（6）选择要管理的域，群组、权限角色新建与授权。

（7)选择要管理的域,导入许可证文件,查看授权情况和已授权数目。

（8）选择要管理的域，操作日志查看。

5.2 控制中心原型设计

5.2.1 统一登陆

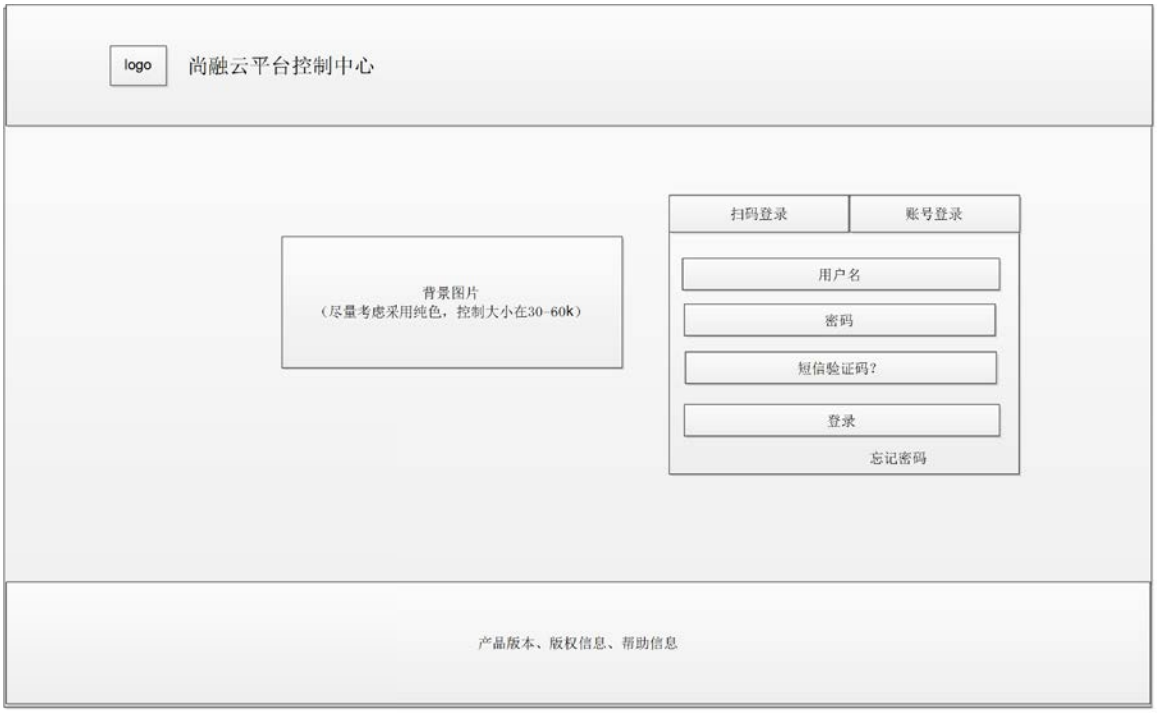

图 5-2 登录页面原型

注：（1）“顶端 logo”、“尚融云平台控制中心”、“背景图片”可通过后台系统配置。

（2）登录框需要考虑账号密码输入、证书认证、短信认证、二维码认证。具体允许认证方式通过后台配置，前段需要根据后台配置信息生成不同的配置框，稍微有点麻烦，细节待后续细化考虑，暂时可完成密码登陆验证即可。

5.2.1 控制中心主页

图 5-3 控制中心主页面原型

注：（1）“顶端 logo”、“尚融云平台控制中心”与登录页相同，图片和字体大小根据实际页面调整。

（2）“产品中心下拉菜单”、“桌面”显示所有应用系统的导航，通过后台配置，所有的应用系统实现单点登录。

5.3 用户中心原型设计

图 5-2 用户中心列表显示原型

注：（1）“顶端 logo”、“尚融云平台控制中心”与登录页相同，图片和字体大小根据实际页面调整。

（2）每个页面的导航按“控制中心>用户中心>页面 1”格式显示。

5.3.1 概览

显示条目如下：（按域分别显示）
用户数/在线用户数：N1/N2
群组数：N2
产品数目：N3

5.3.2 用户组织

1、用户管理
是否区分域：是
选项卡：无
功能：同步|添加用户
搜索选项：用户名
树形组织架构（编辑、删除）

列表显示字段：编号、用户名、操作（启用|禁用、编辑、删除）
批量操作功能：删除、启用|禁用
（1）同步、添加用户
当域配置选择 AD\LDAP 导入用户时，用户只允许同步，不允许添加，反之，允许添加。
（2）启用|禁用
（3）编辑
2、组织管理
是否区分域：是
选项卡：无
功能：同步|添加组织
搜索选项：组织名
树形组织架构（编辑、删除）
列表显示字段：编号、组织名、操作（启用|禁用、编辑、删除）
批量操作功能：删除
（1）同步|添加组织当域配置选择 AD\LDAP 导入用户时，用户只允许同步，不允许添加，反之，允许添加。
（2）编辑

5.3.2 角色

是否区分域：是
选项卡：无
功能：添加
搜索选项：名称、标签
列表显示字段：编号、角色名称、备注、操作（策略、授权、删除）
批量操作功能：无

5.3.4 群组

是否区分域：是
选项卡：无
功能：新建、刷新
搜索选项：组名
列表显示字段：编号、组名、操作（编辑）
批量操作功能：无

5.3.5 许可证

是否区分域：否
选项卡：无
功能：导入，刷新
搜索选项：产品
列表显示字段：编号、产品、公司、版本、许可模式、过期

5.3.5 操作日志

是否区分域：是
选项卡：无
功能：刷新。
搜索选项：名称
列表显示字段：编号、级别、时间、详情、来源、操作（删除）
批量操作功能：删除

5.3.6 配置

1、域配置
是否区分域：否
选项卡：无
功能：新建
搜索选项：域名
列表显示字段：编号、域名、描述、操作（编辑、删除）
批量操作功能：无
（1）新建域（Wizard）
域名：域名、描述信息。
安全认证：AD域/本地数据库、附加验证方式（短信、二维码、UKEY）。
个性化设置：会话超时、文件上传限制、用户密码错误锁定、客户端安全信息绑定。
3、产品配置
是否区分域：否
选项卡：无
功能：添加（Wizard）。
搜索选项：名称
列表显示字段：编号、名称、描述、URL、操作（编辑、删除）
（1）添加

基本配置：产品名称（英文，唯一）、备注、访问密匙(用于应用系统向控制中心获取消息)

服务器配置：URL、Token（用于控制中心向应用服务器获取消息）。

3、系统配置

是否区分域：否

选项卡：无

配置项：。

4、数据库

是否区分域：否

选项卡：设置、备份、还原

6 数据库设计

6.1 数据表

6.1.1 权限组 auth_group

```
DROP TABLE IF EXISTS `auth_group`;
CREATE TABLE `auth_group` (
  `id` mediumint(8) unsigned NOT NULL AUTO_INCREMENT,
  `title` char(100) NOT NULL DEFAULT '',
  `status` tinyint(1) NOT NULL DEFAULT '1',
  `rules` char(80) NOT NULL DEFAULT '',
  `remark` varchar(150) DEFAULT NULL COMMENT '备注信息',
  `label` varchar(150) DEFAULT NULL COMMENT '标签:用户自定义
',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM AUTO_INCREMENT=139 DEFAULT CHARSET=utf8;
```

6.1.2 权限组与用户关联 auth_group_access

```
DROP TABLE IF EXISTS `auth_group_access`;
CREATE TABLE `auth_group_access` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `group_id` int(8) NOT NULL,
  `uid` int(10) NOT NULL,
  PRIMARY KEY (`id`),
```

```
  UNIQUE KEY `uid_group_id` (`uid`,`group_id`),
  KEY `uid` (`uid`),
  KEY `group_id` (`group_id`)
) ENGINE=MyISAM AUTO_INCREMENT=882 DEFAULT CHARSET=utf8;
```

6.1.3 权限组与组织关联 auth_group_org_access

```
DROP TABLE IF EXISTS `auth_group_org_access`;
CREATE TABLE `auth_group_org_access` (
  `id` int(10) NOT NULL AUTO_INCREMENT,
  `uid` int(10) DEFAULT NULL COMMENT '用户 id',
  `gid` int(10) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM AUTO_INCREMENT=850 DEFAULT CHARSET=utf8;
```

6.1.4 权限 auth_rule

```
DROP TABLE IF EXISTS `auth_rule`;
CREATE TABLE `auth_rule` (
  `id` mediumint(8) unsigned NOT NULL AUTO_INCREMENT,
  `name` char(80) NOT NULL DEFAULT '',
  `title` char(20) NOT NULL DEFAULT '',
  `type` tinyint(1) NOT NULL DEFAULT '1',
  `status` tinyint(1) NOT NULL DEFAULT '1',
  `condition` char(100) NOT NULL DEFAULT '' COMMENT '权限类别:1:
基础权限 2:管理权限 3:其它权限',
  PRIMARY KEY (`id`),
  UNIQUE KEY `name` (`name`)
) ENGINE=MyISAM AUTO_INCREMENT=39 DEFAULT CHARSET=utf8;
```

6.1.5 配置 conf

```
DROP TABLE IF EXISTS `conf`;
CREATE TABLE `conf` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.6 域 domain

```
DROP TABLE IF EXISTS `domain`;
CREATE TABLE `domain` (
  `id` int(11) NOT NULL AUTO_INCREMENT COMMENT '编号',
  `name` varchar(30) DEFAULT NULL COMMENT '域名',
  `remark` varchar(255) DEFAULT NULL COMMENT '备注',
  `sso_password` int(11) DEFAULT NULL COMMENT '认证方式',
  `sso_binding_code` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.7 群组 group

```
DROP TABLE IF EXISTS `group`;
CREATE TABLE `group` (
  `id` int(11) NOT NULL AUTO_INCREMENT COMMENT '编号',
  `domain_id` int(11) DEFAULT NULL COMMENT '域关联 ID',
  `name` varchar(30) DEFAULT NULL COMMENT '群组名',
  `remark` varchar(255) DEFAULT NULL COMMENT '备注',
  `label` varchar(30) DEFAULT NULL COMMENT '标签',
  `orgs` varchar(255) DEFAULT NULL COMMENT '组织关联 ID 集合',
  `users` varchar(255) DEFAULT NULL COMMENT '用户关联 ID 集合
',
  `create_time` datetime DEFAULT NULL COMMENT '群创建时间',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.8 日志 log

```
DROP TABLE IF EXISTS `log`;
CREATE TABLE `log` (
  `id` int(11) NOT NULL AUTO_INCREMENT COMMENT '编号',
  `domain_id` int(11) DEFAULT NULL COMMENT '域关联 ID',
  `time` datetime DEFAULT NULL COMMENT '时间',
  `user_name` varchar(30) DEFAULT NULL COMMENT '户名用',
  `user_real_name` varchar(30) DEFAULT NULL COMMENT '用户真实
名',
```

```
  `host` varchar(30) DEFAULT NULL COMMENT '机主名',
  `level` int(11) DEFAULT NULL COMMENT '日志级别 0-7, 0-紧急 emerg,1-alert,2-crit,3-错误 err,4-警告 warning,5-notice,6-信息 info,7-调试 debug',
  `moudle` varchar(255) DEFAULT NULL COMMENT '操作模块',
  `method` varchar(30) DEFAULT NULL COMMENT '操作方法',
  `object_id` int(11) DEFAULT NULL COMMENT '操作对象唯一标识',
  `message` varchar(512) DEFAULT NULL COMMENT '消息文本',
  `client_version` varchar(60) DEFAULT NULL COMMENT '客户端版本',
  `client_os` varchar(60) DEFAULT NULL COMMENT '客户端系统及版本信息',
  `client_ip` varchar(40) DEFAULT NULL COMMENT '客户端 IP 地址',
  `client_longitude` double DEFAULT NULL COMMENT '客户端位置经度',
  `client_latitude` double DEFAULT NULL COMMENT '客户端位置纬度',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.9 许可证 license

```
DROP TABLE IF EXISTS `license`;
CREATE TABLE `license` (
  `id` int(11) NOT NULL COMMENT '编号',
  `domain_id` int(11) DEFAULT NULL COMMENT '域编号',
  `license_file_id` int(11) DEFAULT NULL COMMENT '权授文件关联编号',
  `product_type` varchar(20) DEFAULT NULL COMMENT '产品名称',
  `company` varchar(100) DEFAULT NULL COMMENT '授权单位',
  `edition` int(11) DEFAULT NULL COMMENT '版本，基础版，高级版，企业版',
  `mode` int(11) DEFAULT NULL COMMENT '授权模式',
  `number` int(11) DEFAULT NULL COMMENT '权授数量',
  `expiration_time` datetime DEFAULT NULL COMMENT '过期时间',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.10 许可证文件 license_file

```
DROP TABLE IF EXISTS `license_file`;
CREATE TABLE `license_file` (
  `id` int(11) NOT NULL DEFAULT '0',
  `domain_id` int(11) DEFAULT NULL COMMENT '域编号',
  `host` varchar(255) DEFAULT NULL,
  `name` varchar(255) DEFAULT NULL,
  `add_user` varchar(30) DEFAULT NULL COMMENT '注册人',
  `add_time` datetime DEFAULT NULL COMMENT '注册时间',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.11 组织 org

```
DROP TABLE IF EXISTS `org`;
CREATE TABLE `org` (
  `id` int(11) NOT NULL AUTO_INCREMENT COMMENT '编号',
  `domain_id` int(11) DEFAULT NULL COMMENT '组织关联 ID',
  `name` varchar(30) DEFAULT NULL COMMENT '组织名',
  `remark` varchar(255) DEFAULT NULL COMMENT '备注',
  `parent_id` int(11) DEFAULT NULL COMMENT '父级组织 ID',
  `depth` int(11) DEFAULT NULL COMMENT '树形组织深度',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.12 产品 product

```
DROP TABLE IF EXISTS `product`;
CREATE TABLE `product` (
  `id` int(11) NOT NULL AUTO_INCREMENT COMMENT '编号',
  `name` varchar(30) DEFAULT NULL COMMENT '产品名称',
  `remark` varchar(255) DEFAULT NULL COMMENT '备注',
  `admin_addr` varchar(255) DEFAULT NULL COMMENT '产品管理平台地址',
  `service_addr` varchar(255) DEFAULT NULL COMMENT '服务入口地址',
  PRIMARY KEY (`id`)
```

```
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

6.1.13 用户 user

```
DROP TABLE IF EXISTS `user`;
CREATE TABLE `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT COMMENT '编号',
  `org_id` int(11) DEFAULT NULL COMMENT '组织关联 ID',
  `domain_id` int(11) DEFAULT NULL COMMENT '域关联 ID',
  `name` varchar(30) DEFAULT NULL COMMENT '用户名',
  `real_name` varchar(30) DEFAULT NULL COMMENT '真实姓名',
  `remark` varchar(255) DEFAULT NULL COMMENT '备注',
  `head` varchar(255) DEFAULT NULL COMMENT '头像',
  `sex` int(11) DEFAULT NULL COMMENT '性别,1-男, 2-女',
  `birthday` date DEFAULT NULL COMMENT '生日',
  `id_type` int(11) DEFAULT NULL COMMENT '证件类型',
  `id_number` varchar(60) DEFAULT NULL COMMENT '证件号码',
  `mobile` varchar(16) DEFAULT NULL COMMENT '移动电话号码',
  `telephone` varchar(16) DEFAULT NULL COMMENT '固定电话号码
',
  `qq` varchar(16) DEFAULT NULL COMMENT 'QQ 号码',
  `email` varchar(60) DEFAULT NULL COMMENT '邮箱地址',
  `address` varchar(255) DEFAULT NULL COMMENT '地址',
  `add_time` datetime DEFAULT NULL COMMENT '添加时间',
  `update_time` datetime DEFAULT NULL COMMENT '最后编辑时间',
  `password` varchar(128) DEFAULT NULL COMMENT '用户密码',
  `binding_code` varchar(100) DEFAULT NULL COMMENT '机器码',
  `access_key` varchar(255) DEFAULT NULL,
  `access_secret` varchar(255) DEFAULT NULL COMMENT '访问',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

7 版本 2 与版本 1 区别及兼容

评审记录

版本：2.0.3
评审地点：老饶办公室
评审时间：2017/06/12 10:00-11:00
参与评审人员：钟伟彬、胡锦亚
记录人：胡锦亚

序号	评审人	意见	结论
1	钟伟彬	注册功能统一移到 IAM 完成，由 IAM 控制允许使用用户。	一致同意