一、R1 云认证鉴权平台概述

R1 云身份认证及应用鉴权平台(下文简称 R1 云认证鉴权平台)，是构建云平台的重要支持能力，为集约化管理和集成的云应用提供统一身份、统一认证、SSO、应用鉴权的平台云服务及相关配套管理工具。提供的服务和管理工具包括：

1、 提供统一用户通行证和身份信息管理，为云应用建立全局的、统一的用户身份库。

2、 提供统一身份认证服务，包括用户名密码、PKI 等多重认证机制。

3、 开放的接入机制，遵循 OAuth2.0 协议，云应用只需要遵循 OAuth2.0 协议就可以获取 R1 云认证平台提供的单点登录(SSO)的服务和应用鉴权服务。

4、 提供在统一的应用权限控制服务，并提供相应的应用统一授权管理功能。

二、基于平台建设统一的认证鉴权平台

基于 R1 云认证鉴权平台建设统一的认证鉴权平台，从身份安全的角度，可以带来如下好处：

1、避免了各个应用系统都开发各自的身份认证系统将造成资源的浪费，消耗开发成本，以及因此带来的身体信息泄露的风险。

2、实现用户信息的集中存储和管理，用户信息规范命名、统一存储，用户 ID 全局唯一。从而节省整个云平台用户管理的工作成本。用户身份信息的统一管理，方便形成一致性的标准以支撑绩效核算和企业决策。

3、避免用户需要记忆多个帐户和口令，同时也避免由于用户口令遗忘而导致的支持费用不断上涨；

4、实现统一认证和授权，方便快捷用户身份安全策略，以提高系统的安全级别。

5、为统一分析用户的应用行为提供了功能。

基于上述益处，在基于 R1 云认证鉴权平台建设统一的认证鉴权平台时，原则上推荐：

1、由专业的角色，例如集成商或运营商，统筹地设计统一认证身份管理和认证平台的建设方案（下文统称“建设方案”），内容包括：目标用户范围、管理用户信息的范围、管理的策略、认证的技术方式、单点登录集成应用范围等。

2、遵从建设方案，将用户帐号统一注册或导入到 R1 云认证鉴权平台。

3、为负责各应用系统改造的开发商提供帐号接入和单点登录接入的规范，只要遵循在 Oauth2.0 协议的应用均可以快捷地实现单点登录接入。

4、各开发商遵循“帐号接入和单点登录接入的规范”完成云应用的接入。

三、帐号的统一管理

帐号的统一管理是云应用单点登录的基础，因此，要实现云应用的单点登录，首先需要实现帐号的统一管理或帐号的映射。

1、由专业的角色，例如集成商或运营商，负责帐号的统一注册或导入。

1)、可以根据平台提供的 Excel 模板，进行帐号的收集，最后完成 Excel 的导入。

2)、也可以选择一个相对标准的帐号管理系统，例如 AD 等导成 Excel，实现帐号的导入。

2、由于云应用的开发者自己决定自身系统用户如何与 R1 云认证鉴权平台的帐号的统一管理或帐号映射。

1)、基于 R1 APaaS 开发的云应用，只要将 R1 云认证鉴权平台导出的 Excel 文件，对帐号进行梳理，筛选之后直接可以导入到 R1 APaaS，完成帐号的统一。

2)、非 R1 APaaS 开发的云应用或已有的应用系统，需要根据自己业务系统的特点，决定自己系统如何与 R1 云认证鉴权平台的帐号应该如何映射，例如：

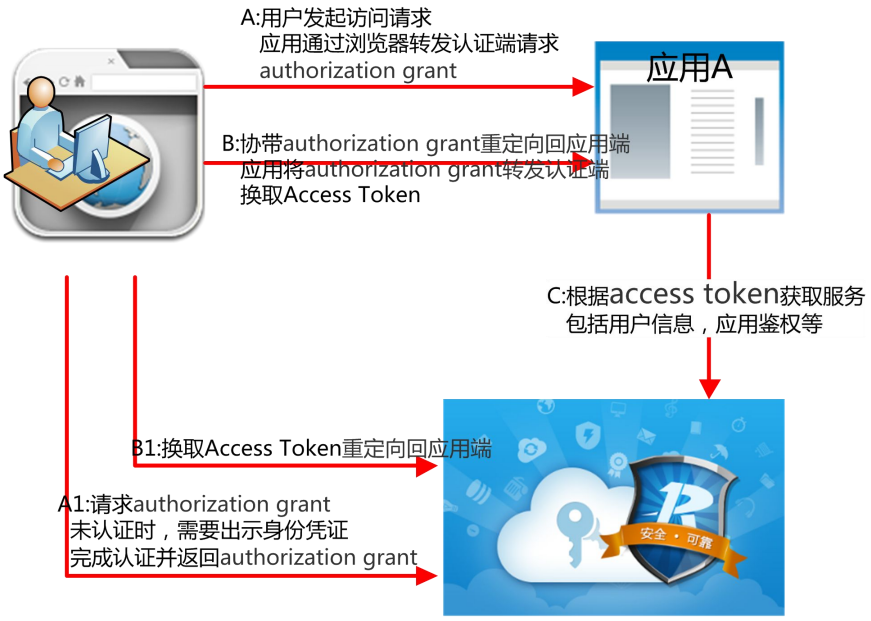
a) 根据用户帐号实现映射
b) 根据用户 Email 实现映射
c) 根据用户编识码(例如员工编码)实现映射
d) 根据用户身份证等信息实现映射。

四、云应用的单点登录接入

R1 云认证鉴权平台是基于 Oauth2.0 协议。关于 OAuth2.0 协议规范，请参考这里。

为了获取R1云认证鉴权平台提供的各项服务，各云应用需要在R1云认证平台注册应用，这时**会为每个应用提供一个专属的 App ID 和 App Secret**。D 跟 Secret 的使用方式跟其他一些协议中的公钥私钥的方案相类似，为你发出的每个请求添加签名，以此来 R1 云认证鉴权平台表明自己的合法身份。

基于 R1 APaaS 开发的云应用，本身已经内置了与 R1 云认证鉴权的单点登录整合。



(A)用户向应用发起访问请求，应用需要向 R1 云认证鉴权请求 authorization grant

由于用户没有认证，应用需要将请求通过浏览器向 R1 云认证鉴权发起认证请求，从而获取授权认可（authorization grant）.

R1 云认证鉴权获取到请求时（A1），需要判断当前用户是否已经登录，如果未登录，要求用户出示身份凭证（例如用户名密码）。完成认证后将生成的授权认可（authorization grant）通过应用传递的 redirect_uri 重定向到应用端。

(B)、应用根据 authorization grant 获取 access token

当 R1 云认证鉴权平台完成认证之后，会根据认证结果，携带着 authorization grant 回到应用传递的 redirect_uri 指向的地址。

这时，应用需要将该 authorization grant 重新通过浏览器转向 R1 云认证鉴权平台换取 access token。

同样，当 R1 云认证鉴权平台获取得到 access token，同样将根据应用传递的 redirect_uri 重定向到应用端。

(C)、应用根据 access token 直接请求 R1 云认证鉴权平台提供的服务

这个过程可以直接通过 restful API，根据 access token 获取应用所需要的服务，包括单点登录过程中所需要的用户身份信息，或应用鉴权信息。

应用可以访问的服务列表，请参考 1.5 已提供的服务列表。

4.1 获取授权许可

这个过程即上述过程所述的第一步，在这个步骤当中，这个授权许可，将以 authorization_code 来表示。

当用户向应用发起访问请求时，应用需要判断用户 Session 是否存在，如果不存在，老百姓通过在浏览器中访问下面的地址，进行用户身份的认证请求。，并获得授权码（www.r1as.com 为认证中心的真实域名）

```
https://www.r1as.com/oauth2/authorize
```

该过程需要携带的参数:

参数名称	参数说明
client_id	必填，应用的唯一标识，即平台中注册应用时指定的 AppId
client_secret	必填，应用的凭证，对应于注册后生成的 secret
redirect_uri	必填，用户授权完成后的回调地址，应用需要通过此回调地址获得用户的授权结果。此地址必须与在应用注册时填写的回调地址一致。
response_type	必填，传递的值只能是 code 或者 token ，如果在平台中应用设置为不允许隐式授权，则只能使用 code
scope	可选值，申请权限的范围。如果不填，则使用缺省的 scope。如果申请多个 scope，使用逗号分隔。

state	可选参数，用来维护请求和回调状态的附加字符串，在授权完成回调时会附加此参数，应用可以根据此字符串来判断上下文关系。

例如：

```
https://www.r1as.com/oauth2/authorize?

client_id=APPID&

redirect_uri=https://www.example.com/back&

response_type=code
```

返回结果：

当身份认证失败或用户对当前应用没有授权访问时，浏览器会重定向到 redirect_uri，并附加错误信息

```
1.      https://www.example.com/back?error=access_denied&errorCode=407&errorDescri
   ption=用户没有权限访问
```

当身份认证成功，并且用户有权限访问这个应用时，浏览器会重定向到 redirect_uri，并附加 autorization_code

```
2.      https://www.example.com/back?code=1644fb4c-af54-4149-a33a-9f538788e5af
```

4.2 换取访问令牌

4.2.1 访问令牌

应用拿到授权码之后，同样需要经浏览器，通过如下地址获取访问令牌，注意：请求必须为 POST（www.r1as.com 为认证中心的真实域名）

```
https://www.r1as.com/oauth2/access_token
```

访问令牌请求参数列表:

参数名称	参数说明
client_id	必填，应用的唯一标识，对应于在平台中注册是的 AppId
client_secret	必填，应用的凭证，对应于注册后生成的 secret
redirect_uri	必填，用户授权完成后的回调地址，应用需要通过此回调地址获得用户的授权结果。此地址必须与在应用注册时填写的回调地址一致

grant_type	必填，此值可以为 authorization_code(根据授权码换取访问令牌) 或者 refresh_token(根据刷新码换取访问令牌)
code	必选参数，上一步中获得的 authorization_code

例如：

```
https://www.r1as.com/oauth2/access_token?

client_id=APPID&

client_secret=1644fb4c-af54-4149-a33a-9f538788e5af&

redirect_uri=https://www.example.com/back&

grant_type=authorization_code&

code=0f826145-090d-4825-86d0-5d42e6241ec4
```

返回结果：

```
{

"access_token":"BFR26145-090d-4825-86d0-5d42e62411FS",

"expires_in":3920,

"refresh_token":"g644fb4c-af54-4149-a33a-9f538788e5ab",

"token_type":"bearer"

}
```

4.2.2 令牌的有效期

access_token 是有一定的有效时间的，当失效之后，需要重新请求。在授权获取 access_token 时会一并返回其有效期，也就是返回值中的 expires_in 参数。

在 access_token 使用过程中，如果服务器返回 416 错误：“expired_token”，此时，说明 access_token 已经过期，除了通过再次引导用户进行授权来获取 access_token 外，还可以通过 refresh_token 的方式来换取新的 access_token 和 refresh_token。

通过 refresh_token 换取 access_token 的处理过程如下：

```
https://www.r1as.com/oauth2/access_token
```

参数名称	**参数说明**

client_id	必选参数，应用的唯一标识，对应于在平台中注册是的 AppId
client_secret	必选参数，应用的凭证，对应于注册后生成的 secret
redirect_uri	必选参数，用户授权完成后的回调地址，应用需要通过此回调地址获得用户的授权结果。此地址必须与在应用注册时填写的回调地址一致
grant_type	必选参数，值为 refresh_token
refresh_token	必选参数，刷新令牌

注意：此请求必须是 HTTP POST 方式，refresh_token 只有在 access_token 过期时才能使用，并且只能使用一次。当换取到的 access_token 再次过期时，使用新的 refresh_token 来换取 access_token

例如：

```
https://www.r1as.com/oauth2/access_token?

client_id=APPID&

client_secret=1644fb4c-af54-4149-a33a-9f538788e5af&

redirect_uri=https://www.example.com/back&

grant_type=refresh_token&

refresh_token=0f826145-090d-4825-86d0-5d42e6241ec4
```

返回结果：

```
{

"access_token":"gth4fb4c-af54-4149-a33a-9f538788e5af",

"expires_in":3920,

"refresh_token":"0f826145-3142-4825-86d0-5d42e6241ec4",

"token_type":"bearer"

}
```

4.3 使用访问令牌调用 API

R1 云认证鉴权所提供的服务均需要应用根据 access_token 来获取的。传递 access_token 的方式有：

1. 直接使用参数传递参数名为 access_token，例如：`https://www.r1as.com/api/user?access_token=1644fb4c-af54-4149-a33a-9f538788e5af`
2. 在 header 里传递 形式为在 header 里添加 Authorization:**OAuth2** 空格 the_token，例如：`Authorization=OAuth 1644fb4c-af54-4149-a33a-9f538788e5af`
3. 在 header 里传递 形式为在 header 里添加 Authorization:**bearer** 空格 the_token，例如：`Authorization=bearer 1644fb4c-af54-4149-a33a-9f538788e5af`

4.4 服务调用时的错误码

在获取授权码、请求令牌时，R1 云认证鉴权平台会对请求的请求头部、请求参数进行检验，若请求不合法或验证未通过，授权服务器会返回相应的错误信息，包含以下几个参数：

1. error：错误码
2. errorCode：错误的内部编号
3. errorDescription：错误的描述信息

错误码 error	错误编号 errorCode	错误的描述信息 errorDescription
unsupported_response_type	400	不支持的 ResponseType
invalid_request	401	请求不合法,缺少必要的参数
unknow_client	402	未知的客户端
invalid_redirect_uri	403	重定向地址不合法
redirect_uri_mismatch	404	重定向地址不匹配
scope_not_valid	405	SCOPE 超出范围
implicit_grant_not_permitted	406	不允许隐式授权
redirect_rui_fragment_componet	407	重定向地址不能包含片段
access_denied	407	用户或管理员禁止访问
invalid_grant	409	提供的 Access Grant 是无效的、过期的、已撤销的

unsupported_grant_type	410	不支持的 GrantType
client_unavailable	411	客户端不可用，还未颁发 secret 或被管理员禁用
invalid_client	412	客户端验证失败，client_id 或者 client_secret 不匹配
authorizationcode_reused	413	授权码不能重复使用
invalid_token	414	访问令牌或刷新码无效
invalid_request_method	415	不支持当前请求方法
expired_token	416	令牌已过期
disabled_token	417	令牌已禁用
disabled_app	418	客户端应用已停用

五、已提供的服务列表

R1 云认证鉴权平台提供的服务列表包括如下文所示，在具体调用时有两种方式：

1. 直接通过 OAuth2 协议调用,获取到访问令牌后请参考使用访问令牌调用 API
2. 使用客户端调用，客户端封装了 OAuth2 协议的过程，使用更加简单，请参考使用客户端调用 API

5.1.获取用户信息

调用示例（直接调用接口,需要先获取到访问令牌）

```
调用方式：https://www.r1as.com/api/user
```

返回结果示例：

```
{
"personUuid" : "4089e314403d26ae01403d26aee90000",
```

```
"userId" : "tester",

"fullName" : "tester",

"email" : "tester@tester.com",

"accountType" : "1",

"accountStat" : "2",

"certificateId" : "",

"loginWay" : "",

"cardType" : "0",

"idNum" : "",

"personCode" : "",

"orgName" : "",

"gender" : "男",

"orderNo" : "1",

"telNo" : "",

"otherInfo" : "",

"createTime" : "2013-08-02 11:51:20",

"createUser" : "",

"updateTime" : "2013-08-20 11:35:35",

"updateUser" : "",

"isAdministrator" : "false"

}
```


5.2.获取应用详细信息

调用示例一（直接调用接口, 需要先获取到访问令牌）

```
调用方式：https://www.r1as.com/api/app?secret=b0bff92c-e3e3-4ead-9f57-d85af21577ee
```

返回结果示例：


```
{

         "id" : "297eff0240766269014076626905000 0",

         "creationDate" : "2013-08-13 14:34:55",

         "appID" : "testapp",
```

```
        "memo" : "1",
        "expireDuration" : "604800",
        "appName" : "测试应用",
        "allowedImplicitGrant" : "false",
        "allowedClientCredentials" : "false",
        "secret" : "b0bff92c-e3e3-4ead-9f57-d85af21577ee",
        "skipConsent" : "true",
        "includePrincipal" : "false",
        "iconURL" : "",
        "useRefreshTokens" : "false",
        "resourceserverId" : "",
        "status" : "1",
        "orderNO" : "100",
        "clientScope" : "",
        "secretTime" : "2013-08-20 17:20:41",
        "redirectUris" : "",
        "developerId" : "000000000000000001",
        "developerName" : "中软国际-部门一"
}
```

5.3.创建用户

```
https://www.r1as.com/api/createUser?userId=test        //userId 登录帐号（必填）
                &fullName=测试                          //fullName 全名 （必填）
                &email=test@163.com                     //email 邮箱 （必填）
                &cardType=身份证                        // cardType 证件类型（选填）
                &idNum=222                              //idNum  证件号码（选填)
                &personCode=00003                       //personCode 应用名称 （选填）
                &orgName=中软                           //orgName 用户单位(选填)
                &gender=男                              //gender 性别 （选填）
                &orderNo=001                            //orderNo 排序后 （选填）
```

```
                &telNo=13233913419                          //telNo 联系电话 （选填）
                &otherInfo=备注                             //otherInfo 备注 （选填）
```

返回结果(JSON)：

```
创建用户成功：{
  "result" : "success",
  "personUuid" : "4089e35e427866c00142788d63850005"
}
创建用户失败：{
  "result" : "failure",
  "error" : "失败原因"
}
```

5.4.更新用户信息

```
https://www.r1as.com/api/updateUser?personUuid=4089e35e427866c00142788d63850005    /
/personUuid 用户 uuid（必填）
                 userId=test                               //userId 登录帐号（必填）
                &fullName=测试                             //fullName 全名 （必填）
                &email=test@163.com                        //email 邮箱 （必填）
                &cardType=身份证                           // cardType 证件类型（选填）
                &idNum=222                                 //idNum  证件号码（选填)
                &personCode=00003                          //personCode 应用名称 （选填）
                &orgName=中软                              //orgName 用户单位(选填)
                &gender=男                                 //gender 性别 （选填）
                &orderNo=001                               //orderNo 排序后 （选填）
                &telNo=13233913419                         //telNo 联系电话 （选填）
                &otherInfo=备注                            //otherInfo 备注 （选填）
```

返回结果(JSON)：

```
更新成功：{"result" : "success"}
更新失败：{"result" : "failure", "error" : "失败原因"}
```

5.5.删除用户

```
https://www.r1as.com/api/deleteUser?personUuid=4089e35e427866c00142788d63850005    /
/personUuid 用户 uuid（必填）
```

返回结果(JSON)：

```
删除成功：{"result" : "success"}

删除失败：{"result" : "failure", "error" : "失败原因"}
```