华为数字平台 OneAccess 集成接口规范

文档版本 01

发布日期 2020-02-27

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 文档介绍

1.1 文档目的

本文档旨在为企业应用系统集成华为 OneAccess，提供详细的集成流程、方案和接口描述，为系统集成人员提供技术指导。

1.2 读者对象

本文档的阅读对象为应用集成方项目经理、开发人员、测试人员。

1.3 集成说明

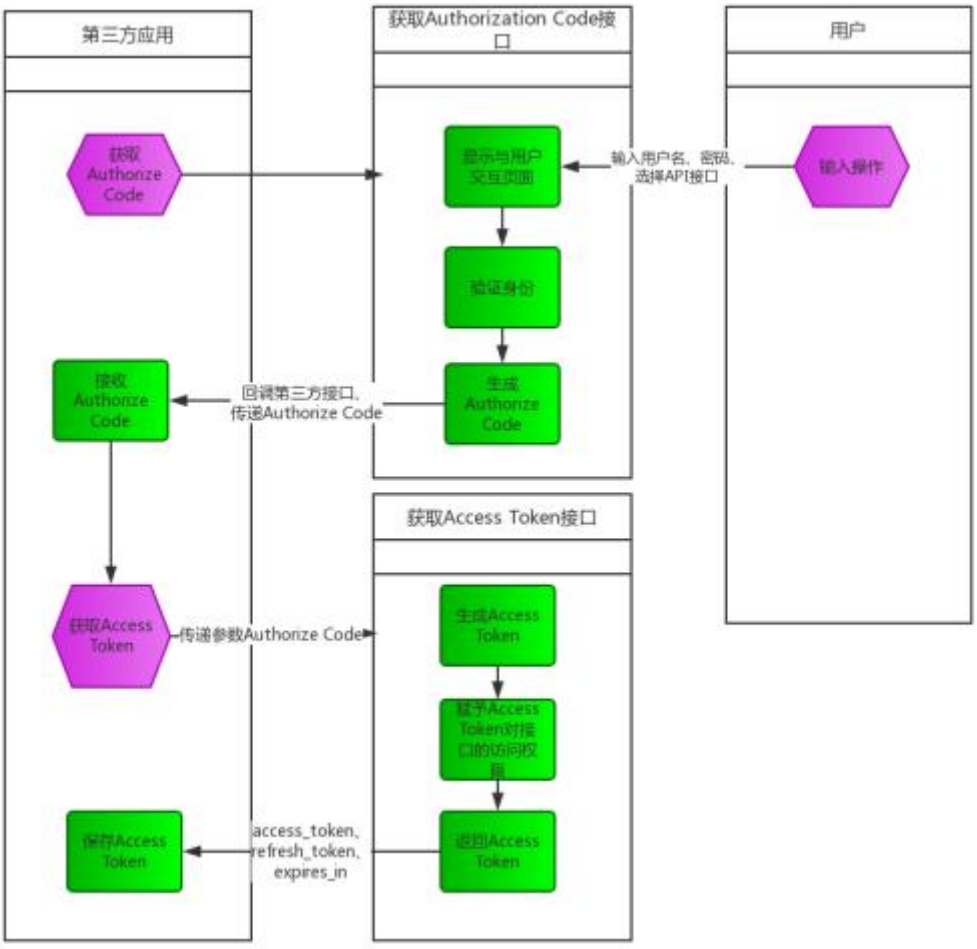
应用系统集成 OneAccess 共分为两部分：身份认证以及数据同步集成，其中身份认证集成支持 OAuth、SAML、CAS 三种标准协议以及 Restful 接口协议，应用系统可根据实际情况选择其中一种协议，应用数据同步采用 Restful 接口协议，具体可参考第 5 章节。

2 OAuth 协议集成指引

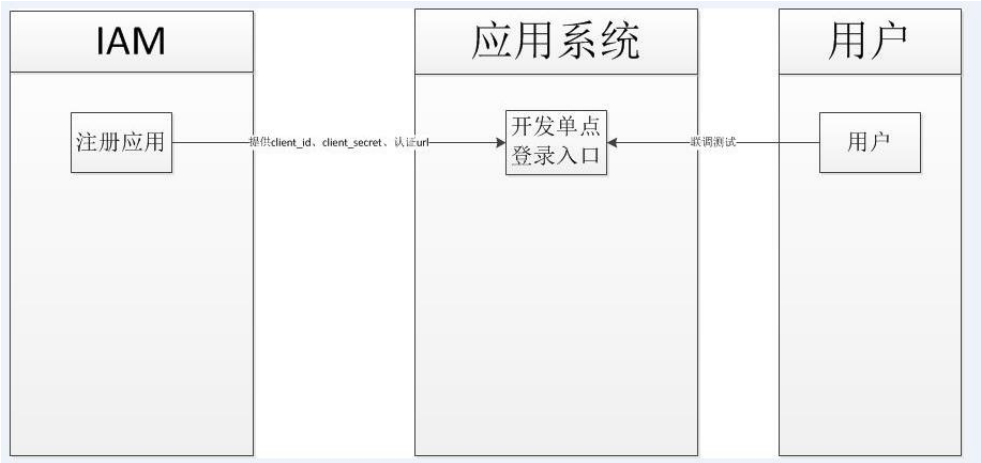
2.1 OAuth 介绍

OAuth 是一个关于授权的开放的网络协议，在第三方应用与服务提供商之间设置一个授权层。第三方应用不能直接登录服务提供商，只能登录授权层，以此将用户与客户端区分开来。第三方应用登录授权层所用的令牌，与用户的密码不同。用户可以在登录授权的时候，指定授权层令牌的权限范围和有效期。第三方应用登录授权层以后，服务提供商根据令牌的权限范围和有效期，向第三方应用开放用户资源。

2.2 OAuth 认证流程



2.3 OAuth 集成流程



2.4 OAuth 接口规范

2.4.1 授权接口

接口名	authorize		
URL Path	https://{host}:{port}/idp/oauth2/authorize		
请求类型	GET		
请求示例	https://{host}:{port}/idp/oauth2/authorize?redirect_uri=http://{host}:{port}/apphub/oauth/callback&state=xxxx&client_id=xxxxx&response_type=code		
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(OneAccess 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
处理逻辑	判断参数 验证 client_id 是否有效 校验 redirect_uri，BAM-CONSOLE 中可填写多 URL（以”;”分隔），判断参数中的 URL 是否以 BAM-CONSOLE 中填写的 URL 开头（此功能可选择是否启用） 显示认证授权页面。 验证身份后页面跳转至 redirect_uri 并附有参数授权码		
返回值	参数正确登录成功时，会跳转到回调地址： 以上文中的回调地址为例，完成后会跳转至 http://{host}:{port}/apphub/oauth/callback?code=ae1838f40638e218bc90a92df3091793&state=xxxxx，携带参数 code 和 state。		
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。		

2.4.2 获取 Token

接口名	getToken		
URL Path	https://{host}:{port}/idp/oauth2/getToken		
请求类型	POST		
请求参数示例	https://{host}:{port}/idp/oauth2/getToken?client_id=xxxxxx&grant_type=authorization_code&code=xxxxxx&client_secret=xxxxxx		
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(OneAccess 提供)
	client_secret	密钥	客户端应用注册密钥(OneAccess 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
处理逻辑	验证参数有效性 验证授权码有效性及范围 根据以上判断、验证及认证结果返回 JSON 数据		

返回值	类型：JSON
	正确返回时：
	{
	"access_token":"skiew234i3i4o6uy77b4k3b3v2j1vv53j",
	"expires_in":"1500",
	"refresh_token":"iewoer233422i34o2i34uio55iojhg6g",
	"uid":"admin"
	}		

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。		

2.4.3 刷新 Token

接口名	refreshToken
URL Path	https://{host}:{port}/idp/oauth2/refreshToken
请求类型	POST
请求参数示例	https://{host}:{port}/idp/oauth2/refreshToken?client_id=xxxxxxx&grant_type=refresh_token&client_secret=xxxxxxx&refresh_token=xxxxxxxxxx

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(OneAccess 提供)
	client_secret	密钥	客户端应用注册密钥(OneAccess 提供)
	refresh_token		刷新 token 授权码
	grant_type	认证方式	请求类型，默认 refresh_token
处理逻辑	验证参数有效性 刷新续期业务逻辑操作 根据以上判断、验证及认证结果返回 JSON 数据		

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		

2.4.4 验证 token

接口名	checkTokenValid		
URL Path	http://{host}:{port}/idp/oauth2/ checkTokenValid		
请求类型	POST		
请求示例	https://{host}:{port}/oauth2/checkTokenValid?access_token=46e4d79fc6384105e157465032c9684e		
参数	参数名	中文说明	描述
	access_token		token 授权码
处理逻辑	判断参数 检查 token 有效性 根据以上判断、验证及认证结果返回 JSON 数据		

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

描述	

2.4.5 获取认证用户

接口名	getUserInfo		
URL Path	http://{host}:{port}/idp/oauth2/getUserInfo		
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(OneAccess 提供)
处理逻辑	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 根据以上判断、验证及认证结果返回 JSON 数据		

返回值	类型：JSON
	正确返回时：
	{
	"uid":"20190104143740849-DF0C-690E07E54",
	"spRoleList":[],
	"loginName":"user1"
	}		

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

2.4.6 登出接口

接口名	GLO		
请求类型	POST		
请求示例	https://{host}:{port}/idp/profile/OAUTH2/Redirect/GLO?redirctToUrl=https://{host}:{port}&redirectToLogin=true&entityId=20170830061623854-E5A8-B2FABDC35		
参数	参数名	中文说明	描述
	redirctToUrl	回跳 url	应用的登录地址 注:url 必须为一个完整有效的地址
	redirectToLogin	true	是否直接跳转至应用 redirctToUrl，true 为跳转至 redirctToUrl，false 为停留在 idp 退出展示页面
	entityId	应用 ID	
处理逻辑	判断参数 根据以上判断、验证及认证结果返回 JSON 数据		
返回值			
注意事项	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		

2.5 OAuth 错误码参考

序号	错误代码	错误说明
1	1001	缺少参数 client_id
2	1009	缺少参数 code
3	1010	缺少参数 grant_type
4	1008	缺少参数 client_secret
5	1005	参数 code 非法
6	1024	refresh_token 值不能为空
7	1025	参数 refresh_token 不正确或者过期

序号	错误代码	错误说明
8	2001	缺少参数 access_token
9	2002	参数 access_token 不正确或者过期

3 SAML 协议集成指引

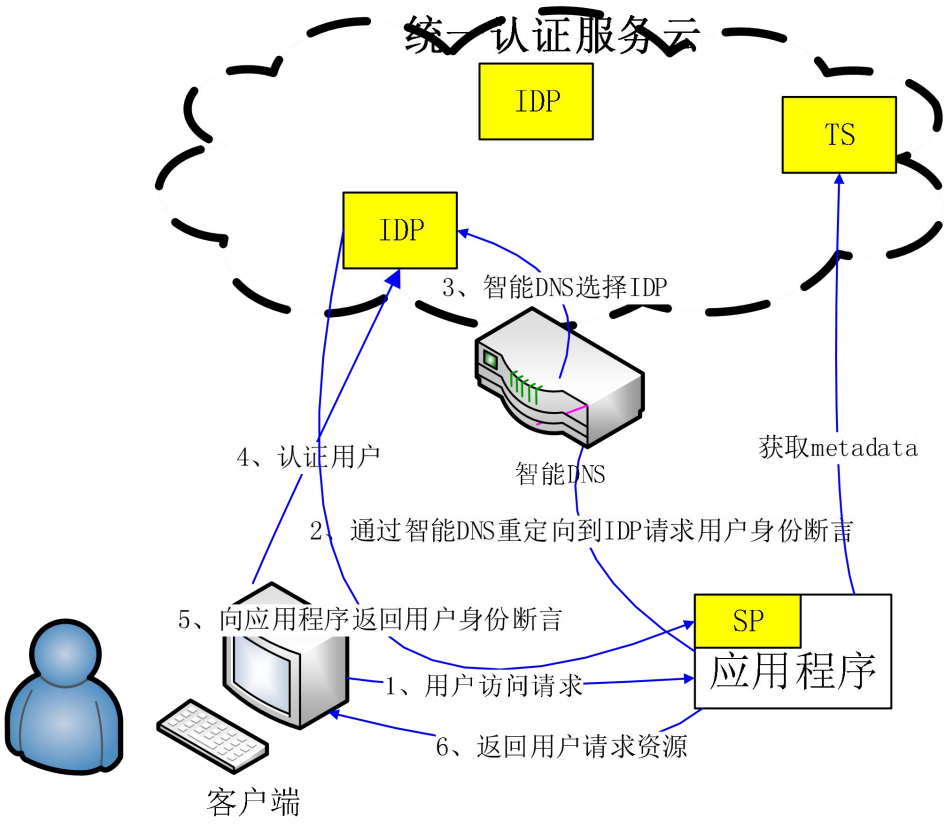
3.1 SAML 介绍

SAML 即安全声明标记语言，英文全称是 Security Assertion Markup Language。它是一个基于 XML 的标准，用于在不同的安全域(security domain)之间交换认证和授权数据。

断言， SAML 中的”A”，是整个 SAML 协议中出现的最多的字眼，我们可以将断言看作是一种判断，并且我们相信这种判断，因此，做出断言的一方必须被信赖。校验来自断言方的断言必须通过一些手段，比如数字签名，以确保断言的确实来自断言方。

3.2 SAML 认证流程

在使用 SAML 用户认证过程中，统一认证服务各组件 IDP、SP、TS 完成用户身份认证业务流程如下图如示：

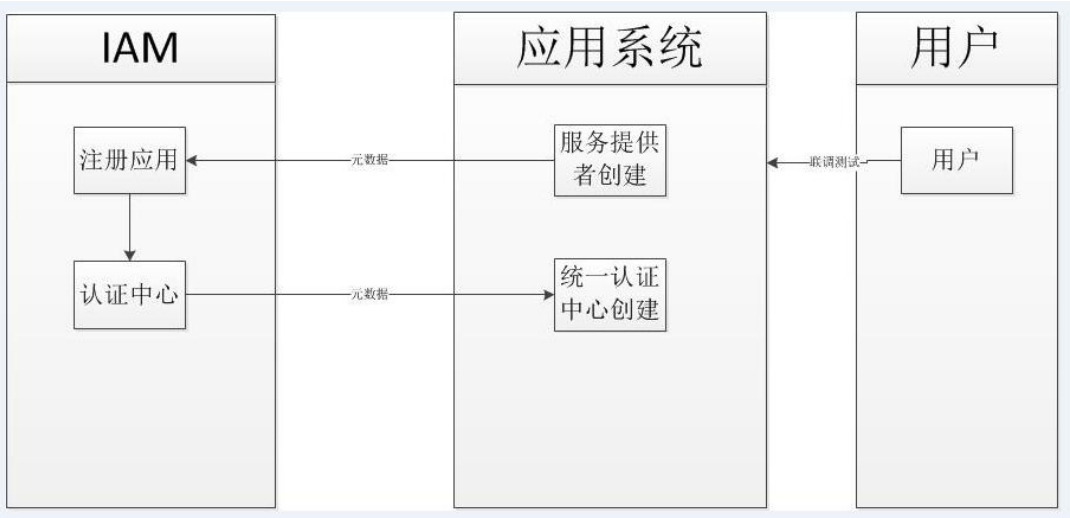


认证流程图

用户认证过程如下：

1. 用户访问应用服务程序，请求应用资源。应用服务器检查用户是否经过身份认证，如会话中没有用户认证结果信息，将控制权交给 SP 组件。
2. SP 生成身份认证请求信息（包含应用程序、签名要求、加密要求等信息），重定向到 IDP 对应域名通过 DNS 解析分发。
3. 智能 DNS 通过 IP 地址与认证中心的映射关系选择一个对应的可用的认证中心服务地址访问。
4. IDP 根据配置的认证方式供用户选择认证。
5. IDP 签发身份断言，签名，加密，重定向回应用程序。
6. SP 验证断言，解析出用户身份。返回用户请求的资源。

3.3 SAML 集成流程

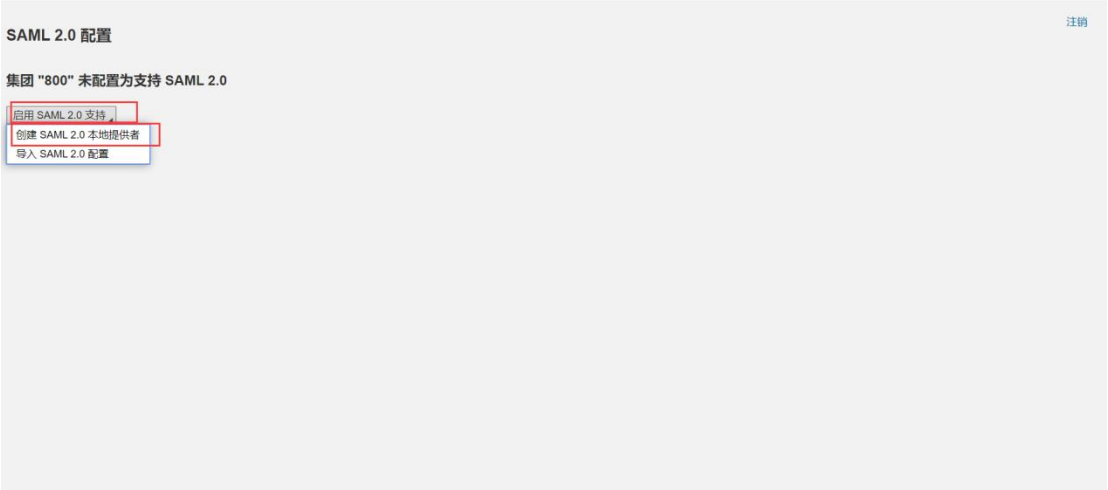


3.4 标准 SAML 集成示例

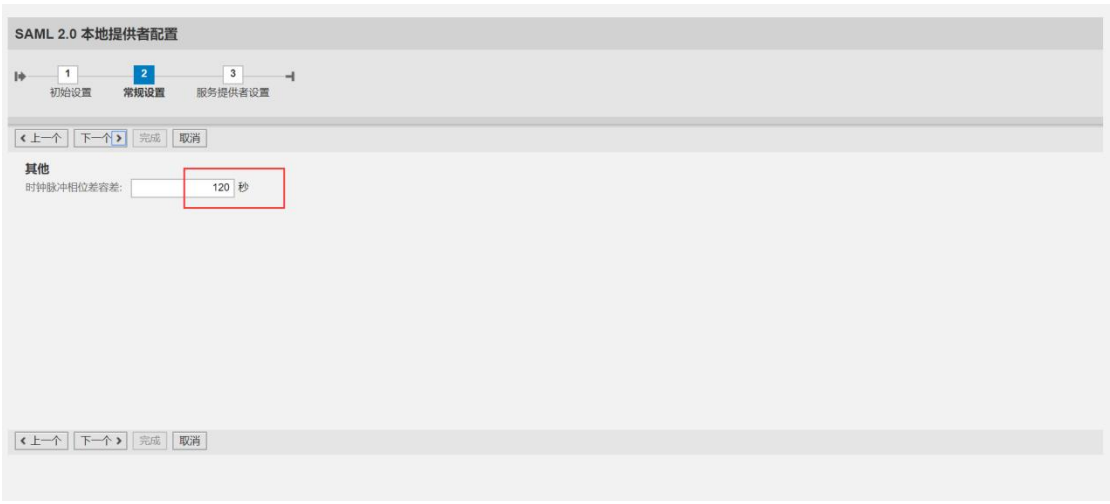
3.4.1 服务提供者创建

1、进入 SAP 的配置页面

2、选择启用 SAML2.0 支持

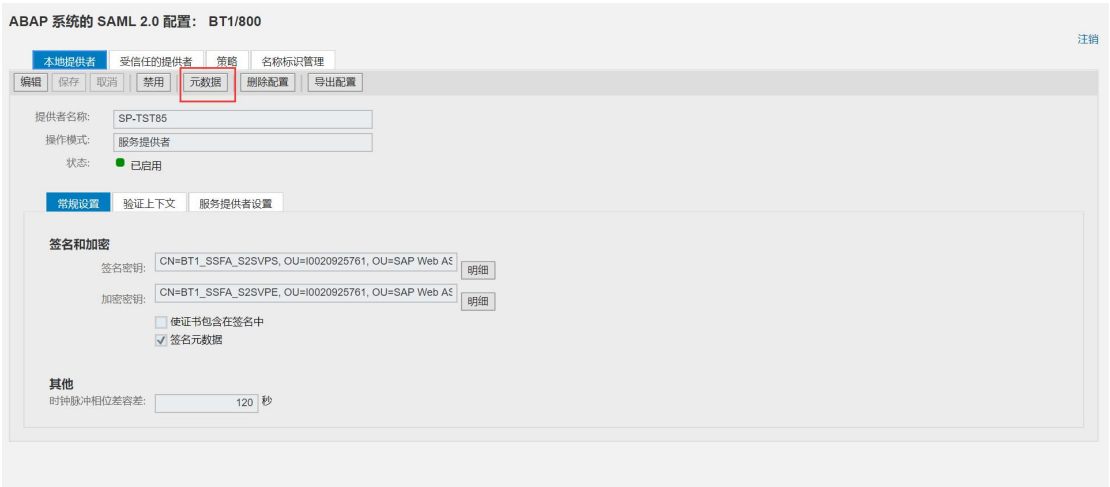


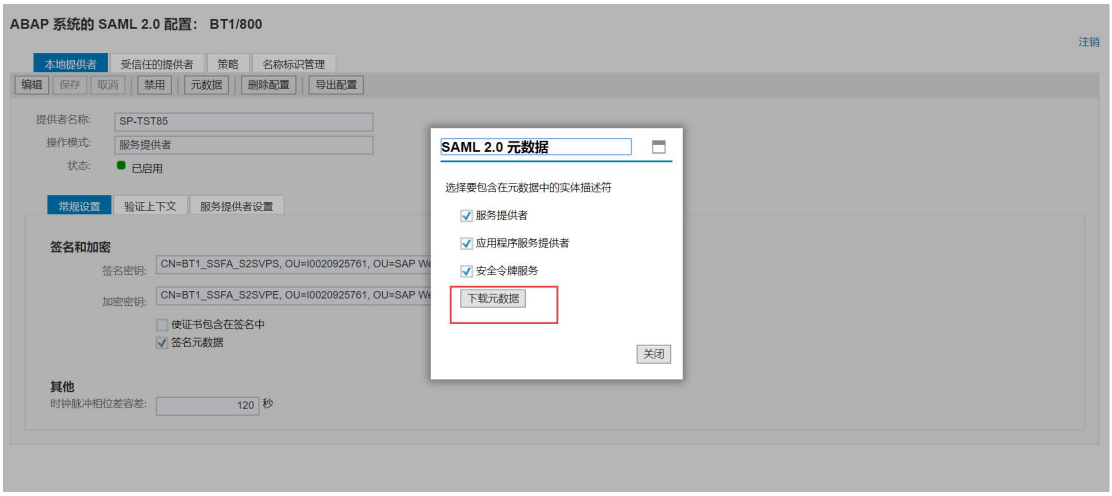
3、创建一个服务提供者



这样就完成了本地服务者的创建工作（即 SP 应用服务提供者）

为统一认证中心提供元数据文件



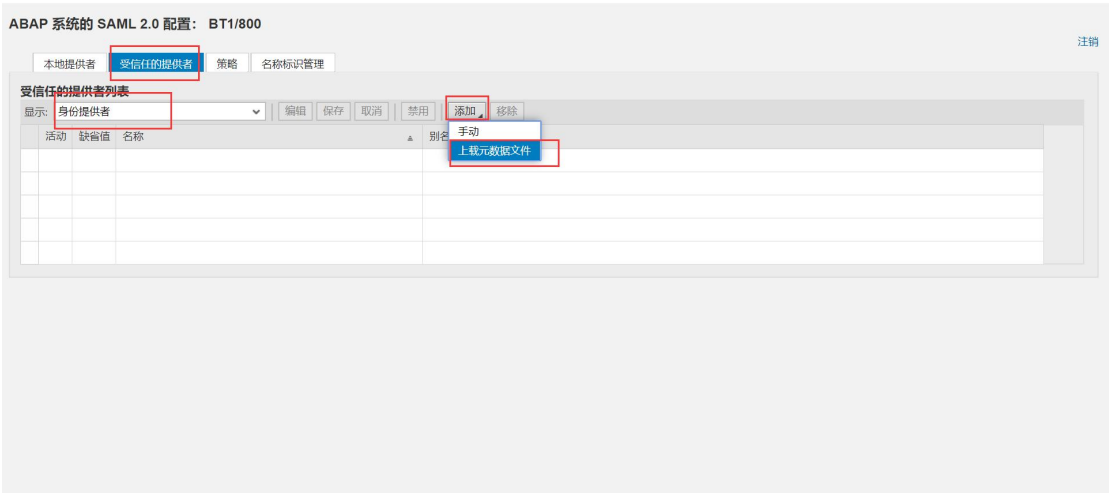


下载出一个应用服务提供者的 metadata.xml 文件

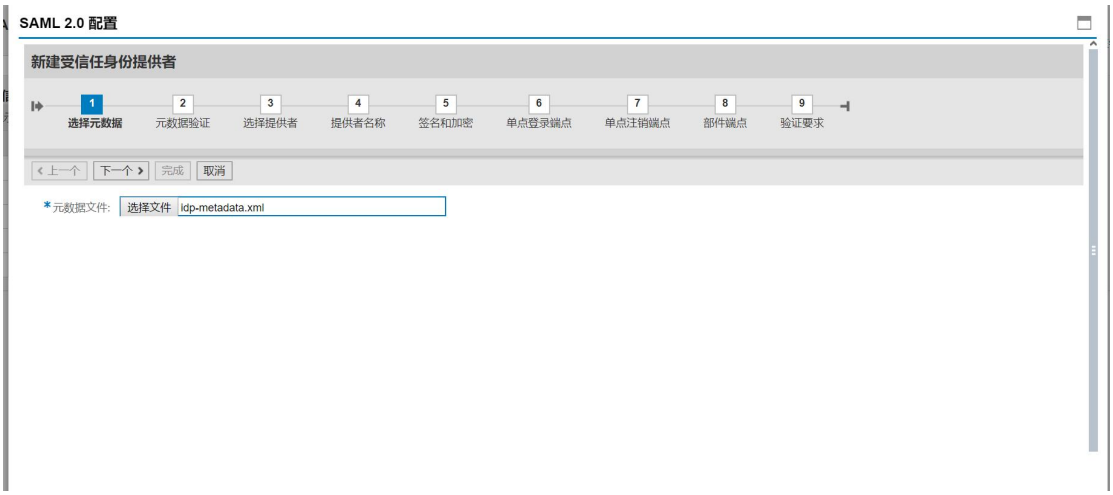
3.4.2 统一认证中心创建

1、统一认证中心服务为 SAP 提供一个元数据文件（即 idp-metadata.xml 文件）

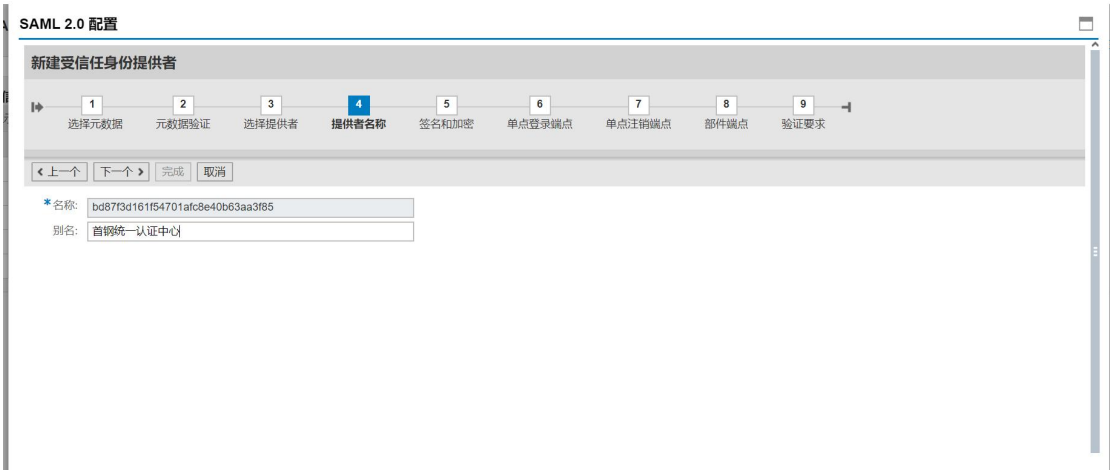
2、开始建立一个身份提供者（SAML 协议的统一认证中心）



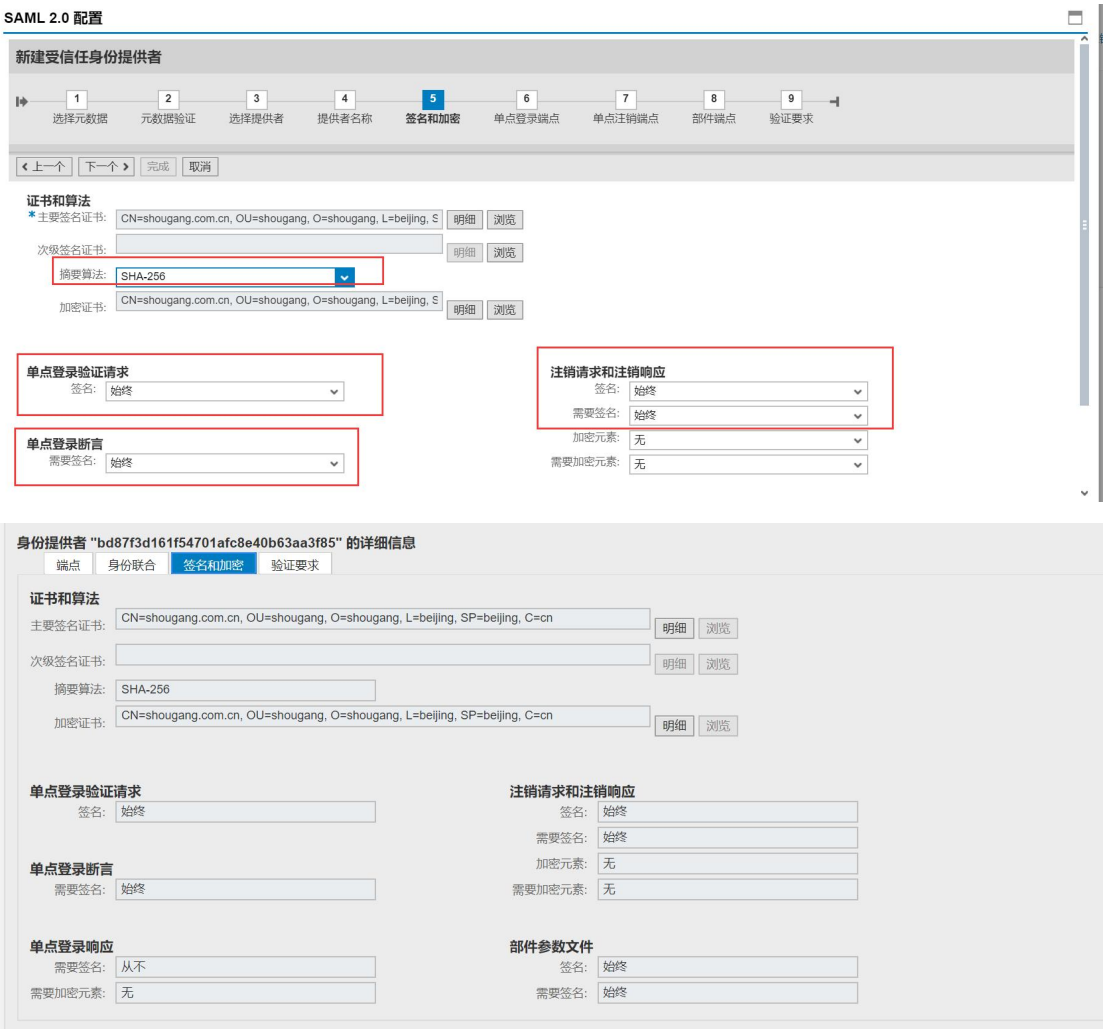
3、导入统一身份服务提供的元数据文件



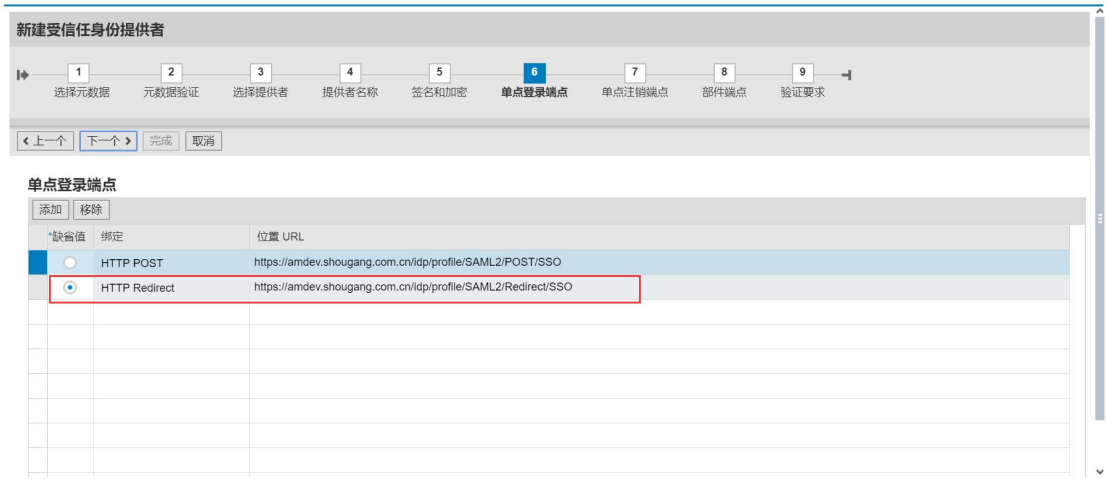
4、填写身份服务提供者的别名



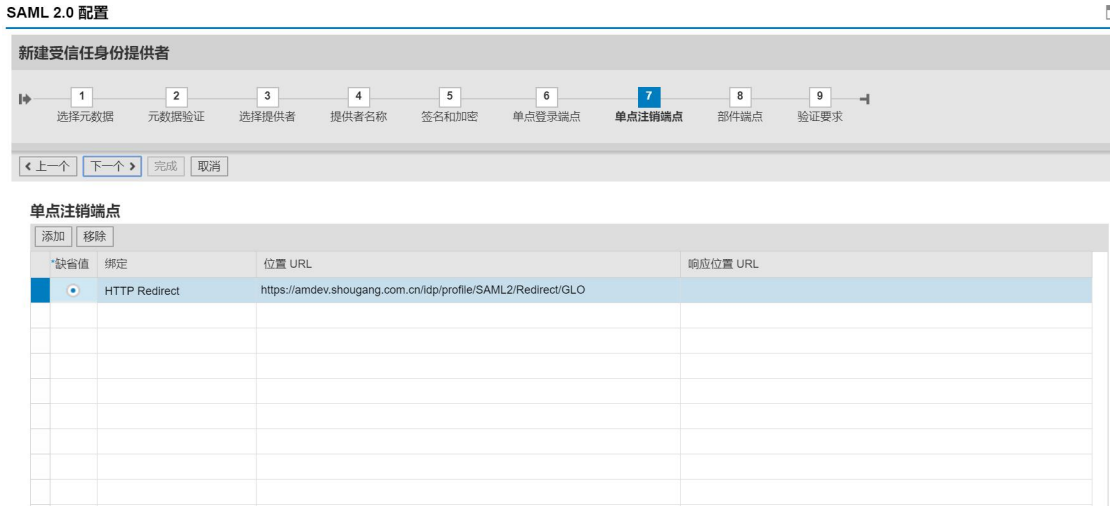
5、签名摘要算法选择 SHA-256，以及各个步骤中是否需要进行签名验签的选项按照下图选择。



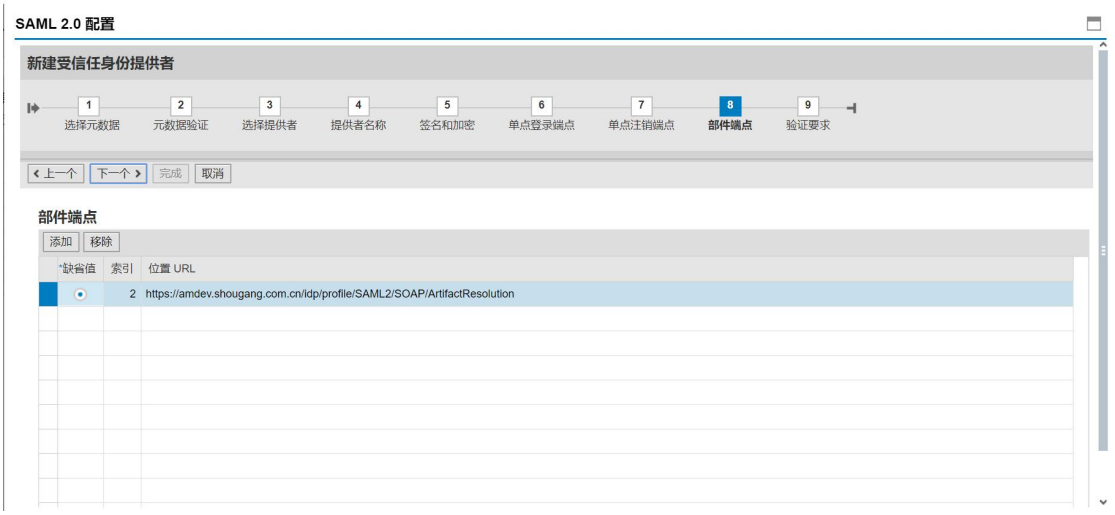
6、单点登录的端点默认为 HTTP Redirect 选项。



7、单点登录注销端点默认选择

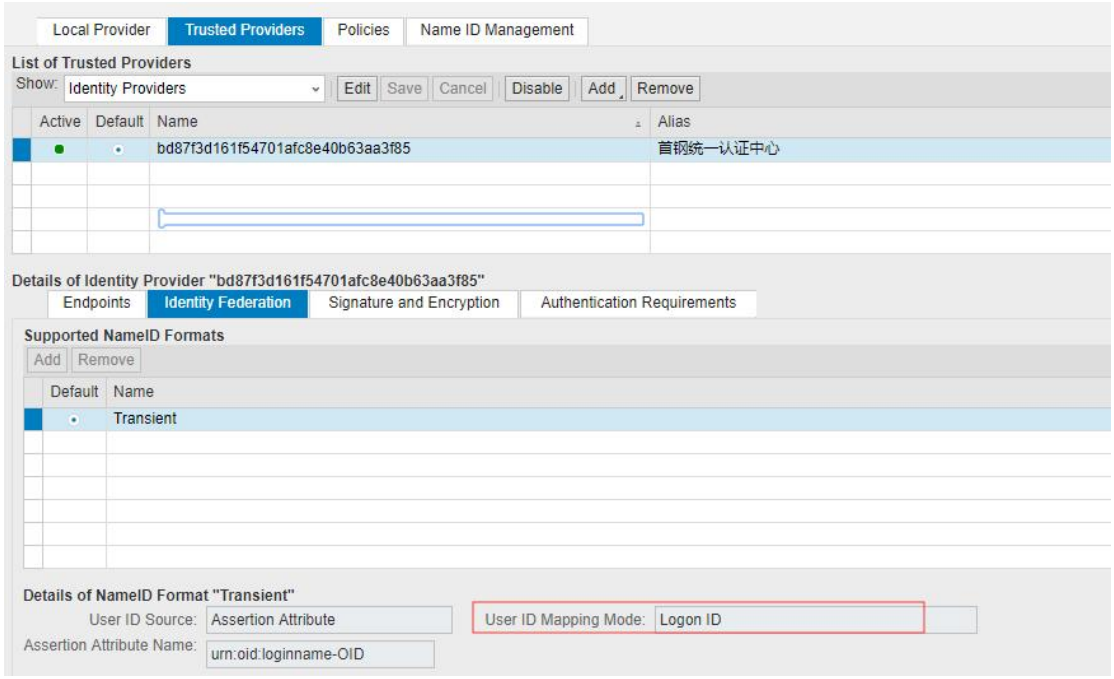


8、部件端点默认选择



9、验证要求默认选择

10、编辑【受信任的提供者】-【身份联合】-【名称表示格式得详细信息”Transient”】

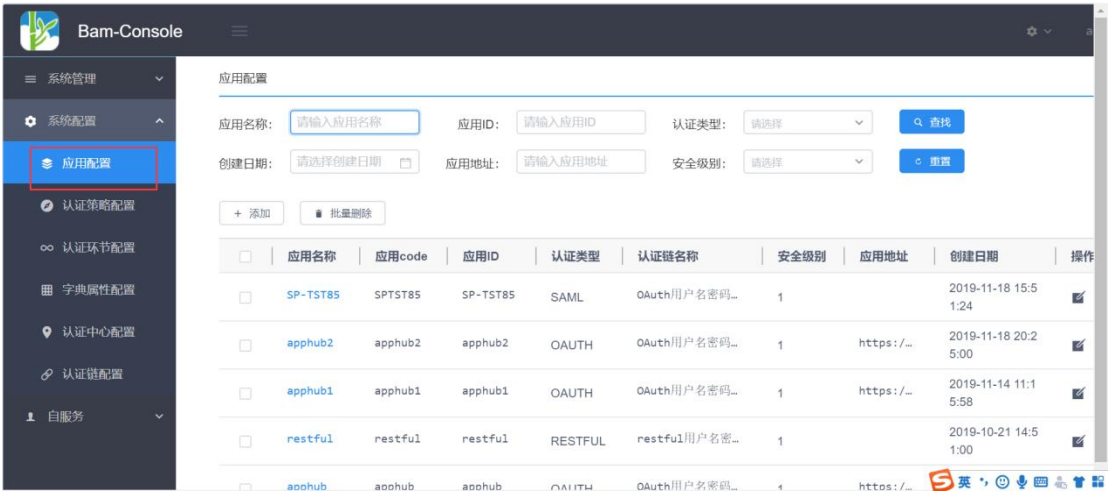


这里表示的含义是统一认证中心返回的报文中”urn:oid:loginname-OID”这个属性映射到 SAP 用户库的 Logon Logon ID 字段。

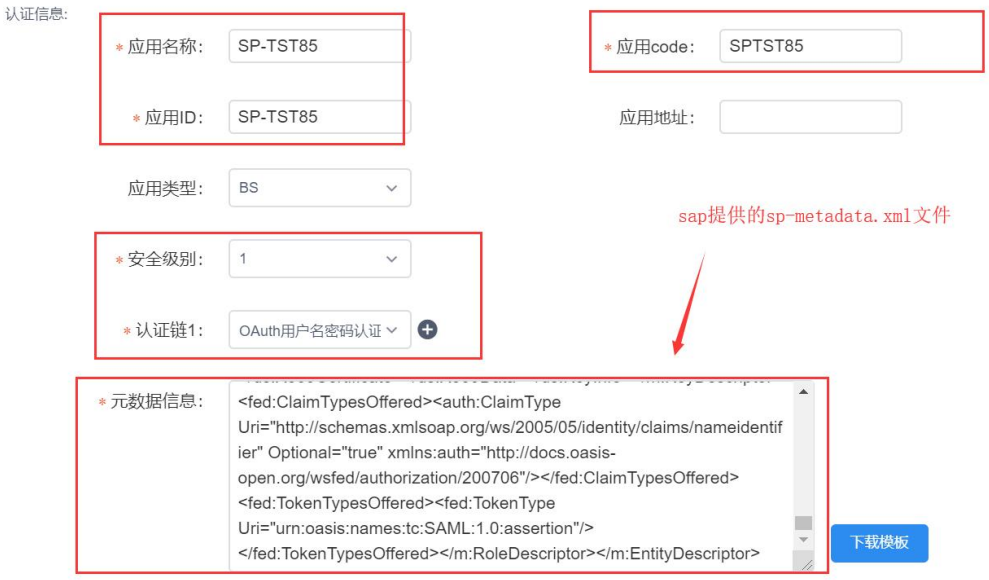
11、最后启用身份提供者服务

3.4.3 统一认证中心注册 SAP 应用

1、【系统配置】-【应用配置】



新增一个应用系统



将 SAP 提供的 sp-metadata.xml 文件的内容放入元数据信息中。

3.5 标准 SAML 集成错误码

序号	错误代码	错误说明
1	error.message.saml.request.unlikelihood	SAML 认证请求应用不可信，请联系管理员。
2	error.message.saml.request.marshall	无法组装认证请求上下文，请联系管理员。

序号	错误代码	错误说明
3	error.message.saml.request.invalid	无效的 SAML 认证请求消息，请联系管理员
4	error.message.saml.request.decode	SAML 认证请求消息解码验证错误，请联系管理员。
5	error.message.saml.request.security	SAML 认证请求消息不符合安全策略要求，请联系管理员。
6	error.message.saml.request.forward	SAML 认证请求消息转发错误，请联系管理员。
7	error.message.saml.request.version.low	SAML 请求版本过低，请联系管理员。
8	error.message.saml.request.version.high	SAML 请求版本太高，请联系管理员。
9	error.message.saml.request.authen.failure	SAML 请求认证失败，请联系管理员。
10	error.message.saml.request.sp.invalid	SAML 认证请求 SP 无效，请联系管理员。
11	error.message.saml.request.sp.metadata	查找元数据错误，请联系管理员。
12	error.message.saml.reponse.sp.metadata	无法确定应该签署断言的应用 metadata 完整性，请联系管理员。
13	error.message.saml.reponse.no.sig.credenttial	无断言签名证书配置，请联系管理员。
14	error.message.saml.reponse.sig	断言签名错误，请联系管理员。
15	error.message.saml.reponse.sig.marshall	无法组装断言签名，请联系管理员。
16	error.message.saml.reponse.sig.unable	无法签名断言，请联系管理员。
17	error.message.saml.reponse.no.peer.endpoint	没有 SP 认证请求端点。无法发送响应，请联系管理员。

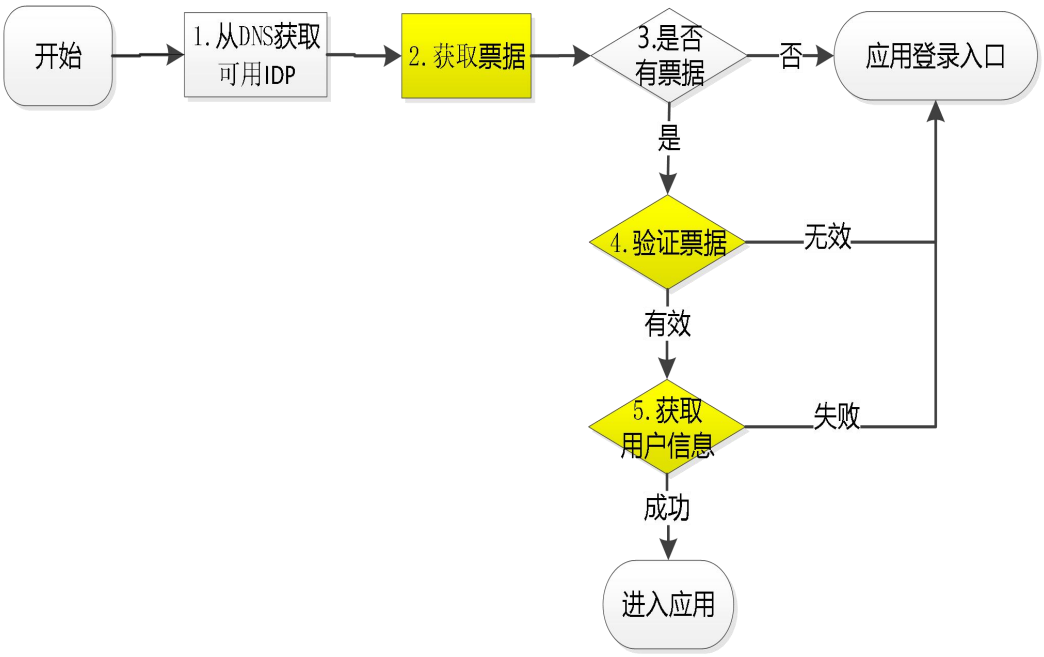
序号	错误代码	错误说明
18	error.message.saml.reponse.no.msg.encoder	没有配置消息输出编码器，请联系管理员。
19	error.message.saml.reponse.isno.assertions.encrypt	无法确认断言是否需要加密，请联系管理员。
20	error.message.saml.reponse.no.construct.encoder	无法构建消息加密处理器，请联系管理员。
21	error.message.saml.reponse.assertions.encrypt.unable	无法加密断言，请联系管理员。
22	error.message.saml.reponse.encrypt.unable	无法加密报文，请联系管理员。

4 Restful 认证集成指引

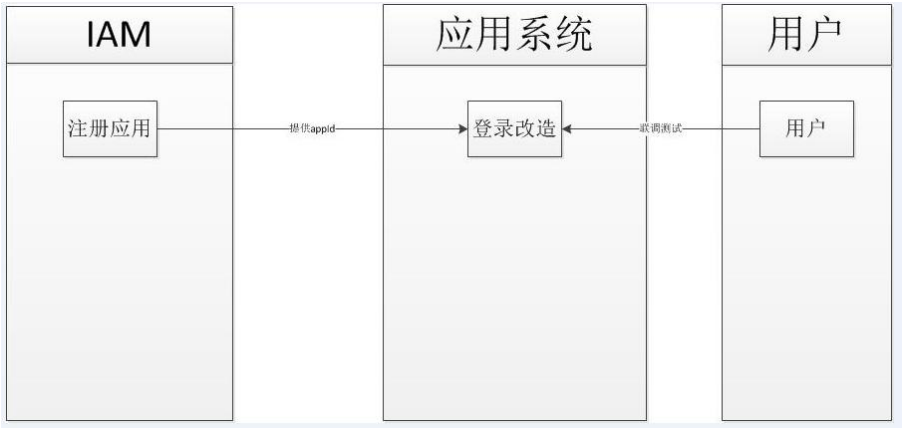
4.1 Restful 介绍

统一认证服务的 REST 提供了认证接口、验证 Token 有效性接口和获取用户信息接口；同时为了实现 SSO，提供了 2 个认证辅助接口，用于认证中心的票据获取和设置。应用可以根据这 5 个接口，编写应用的访问控制逻辑，实现 SSO 和访问控制。由于 HTTP URL 自身限制，无论 REST 接口还是认证辅助接口，传入的参数值如果包含例如”%”、”&”、” ”、”=”等特殊字符或中文时，需要先作 urlEncode 编码。推荐所有参数值先都作 urlEncode 编码再调用接口传入。

4.2 Restful 认证流程



4.3 Restful 集成流程



4.4 Restful 接口规范

4.4.1 认证接口

接口名	authenticate
URL Path	https://{host}:{port}/ idp/restful/IDPAuthenticate
请求类型	GET、POST

<table>
<tr><td>请求示例</td><td colspan="3">https://{host}:{port}/idp/restful/IDPAuthenticate?appId=xxx&userName=xxx&password=xxx&authnMethod=xxx&remoteIp=</td></tr>
<tr><td rowspan="8">参数</td><td>参数名</td><td>中文说明</td><td>描述</td></tr>
<tr><td>appId</td><td>应用标识</td><td>客户端应用注册 ID(OneAccess 提供)</td></tr>
<tr><td>userName</td><td>用户名</td><td>用户登录名</td></tr>
<tr><td>password</td><td>密码</td><td>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</td></tr>
<tr><td>checkcode</td><td>短信验证码</td><td>当采用用户名+密码认证时，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。</td></tr>
<tr><td>remoteIp</td><td>客户端 IP</td><td></td></tr>
<tr><td>authnMethod</td><td>认证方式</td><td>当采用用户名+密码认证时，传入 UsernamePassword 或不传
当采用用户名+短信验证码认证时，传入 UsernameSM</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>处理逻辑</td><td colspan="3">判断参数
验证 appId 是否有效
调用 IDP 认证接口
根据以上判断、验证及认证结果返回 JSON 数据</td></tr>
<tr><td>返回值</td><td colspan="3">用户密码认证通过时：
[
{
"data": {
"tokenId": "MTkyLjE2OC4xMjguMQ==|NzI4Nzg5OWNiNDM0ZWRjMTMwMWM0Y2NjNDIzNzk3NjQ4MzRkNmVhODk4Y2MxMWZiMTY3MjZhOTM2ZmFmZGVhNA==|Qgai5XhdPTYWf9GbWfynyIySczY="
},
"message": null
}
]</td></tr>
</table>

4.4.2 验证票据接口

接口名	isTokenValid		
URL Path	https://{host}:{port}/ idp/restful/isIDPTokenValid		
请求类型	POST、GET		
请求参数示例	https://{host}:{port}/ idp/restful/isIDPTokenValid?appId=xxx&tokenId=xxx&remoteIp		
参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(OneAccess 提供)
	tokenId	用户票据	
	remoteIp	客户端 IP	
处理逻辑	判断参数 验证 appId 是否有效 验证 tokenId 是否有效 根据以上判断、验证结果返回 JSON 数据		

返回值	类型：JSON
	正确返回时：
	[
	{
	"data": {
	"isValid": true
	},
	"message": null
	}
	]		

4.4.3 获取用户信息接口

接口名	GetUserAttributes
URL Path	https://{host}:{port}/idp/ idp/restful/getIDPUserAttributes
请求类型	POST、GET
请求参数示例	https://{host}:{port}/ idp/restful/getIDPUserAttributes?appId=xxx&tokenId=xxx&remoteIp=&attributeNames=xxxx

参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(OneAccess 提供)
	tokenId	用户票据	
	remoteIp	客户端 IP	必填
	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
处理逻辑	判断参数 验证 appId 是否有效 验证 tokenId 是否有效 获取用户信息 根据以上判断及结果返回 JSON 数据		

返回值	类型：JSON
	正确返回时：
	[
	{
	"data": {
	"tokenId": "MTkyLjE2OC4xMjguMQ==|ODZlNTY2MzY5MWU4ZTkxYmZmNzEwMjVlNmFhNDdiMWMzYzZkMmQ3MjVmMTY3NzA5YTQxNDY0Y2ZhMjNhODgwZQ==|1m0nP3K952xf2r+xkj8bXpvXdw8=",
	"attributes": {
	"uid": [
	"dingkx"
	],
	"sn": [
	"丁"
	],
	"givenName": [
	"新星"
	],
	"spOrgCodePath": [
	"/10010000/10010001/30200000/30200018/30204583/"
	]
	}
	},
	"message": null
	}
	]

4.4.4 获取票据接口

接口名	getToken
URL Path	https://{host}:{port}/ idp/restful/getIDPToken

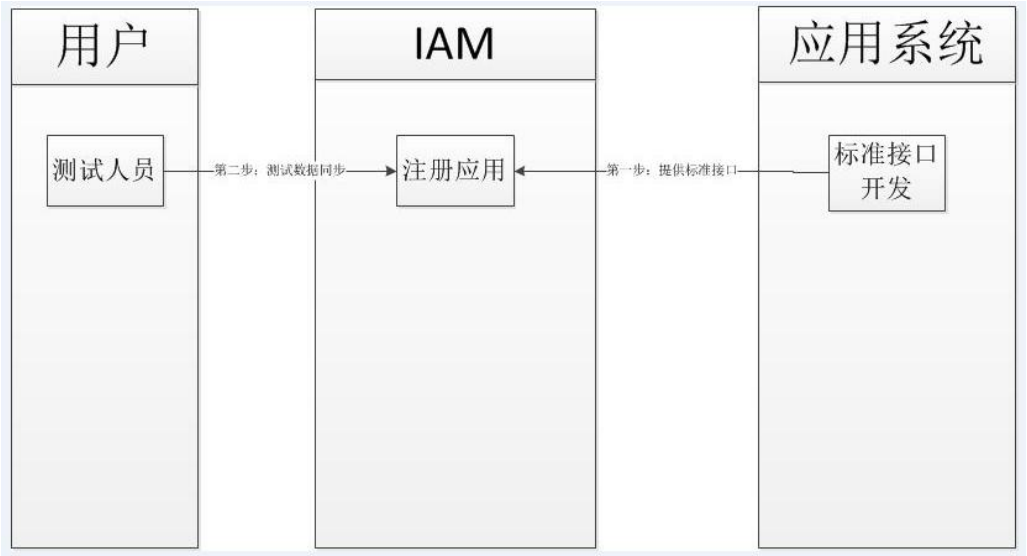
<table>
<tr><td>请求类型</td><td colspan="3">POST、GET</td></tr>
<tr><td>请求参数示例</td><td colspan="3">https://{host}:{port}/ idp/restful/getIDPToken?appId=xxx&
jsonpCallback=&remoteIp=</td></tr>
<tr><td rowspan="5">参数</td><td>参数名</td><td>中文说明</td><td>描述</td></tr>
<tr><td>appId</td><td>应用标识</td><td>客户端应用注册 ID(OneAccess 提供)</td></tr>
<tr><td>jsonpCallback</td><td>回调函数</td><td>Jsonp 回调函数</td></tr>
<tr><td>remoteIp</td><td>客户端 IP</td><td></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>处理逻辑</td><td colspan="3">判断参数
验证 appId
获取浏览器中的 SSO Cookie
验证 token
根据 SSO Cookie 存在情况跳转到 app 并附加参数</td></tr>
<tr><td>返回值</td><td colspan="3">tokenId:
用户票据</td></tr>
<tr><td>返回 URL</td><td colspan="3">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_appId_error”等错误信息</td></tr>
</table>

5 数据同步集成规范

5.1 数据同步介绍

华为数字平台 OneAccess 平台与下游集成应用系统，数据交互分为”供应/回收”两个部分，数据供应是通过内置 connector 连接器请求下游集成应用系统的 API 接口服务，请求调用接口定义的接口方法，数据回收是通过内置 connector 连接器请求下游集成应用系统的 API 接口服务，将应用系统中的账号和组织机构回收到 OneAccess，实现 OneAccess 用户和原有应用系统账号身份的绑定。

5.2 数据同步集成流程



5.3 数据同步接口规范

5.3.1 数据加解密方式

功能说明	为了报证在公有云环境下数据同步的安全性，对传送数据加入加解密校验，即每一个接口 oneAccess 调用时都会对请求参数进行加密,系统方对密文解密处理后响应的报文需加密后通过接口返回给 oneAccess	
调用参数	参数名	中文说明

	STR	数据密文
	KEY	OneAccess 提供的密钥
	TYPE	OneAccess 提供的加密类型默认为 AES
示例	**加密示例** **密文：xxx(str)** 密钥:123456 类型:AES	`BamboocloudFacade.encrypt(xxx, "123456", "AES");`
	解密示例 **密文：xxx(str)** 密钥:123456 类型:AES	`BamboocloudFacade.decrypt(xxx, "123456", "AES");`

5.3.2 SchemaService 接口

接口名	SchemaService	
功能说明	SchemaService 的功能是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 OneAccess 平台用户字段和三方目标系统账号字段的映射关系。	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
	iamRemoteUser	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型

	account/organization/role/userpost	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）、userpost（兼岗）、post（岗位）、bank（银行卡），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
	name	定义对象的属性字段名称。字段为 String 类型
	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。
	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。
	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。

返回值	{
	"aimRequestId": "9e928d12ec8a4c1bb75283b8df71308d",
	"account": [{
	"multivalued": false,
	"name": "uid",
	"required": false,
	"type": "String"
	},{
	"multivalued": false,
	"name": "userName",
	"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"
	}, {
	"multivalued": false,
	"name": "parentOrgId",
	"required": true,
	"type": "String"
	},……] }

5.3.3 UserCreateService 接口(账号创建)

接口名	UserCreateService	
功能说明	UserCreateService 接口是应用系统的账号创建方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
	loginName/ orgId/ fullName	三方应用系统 SchemaService 接口中定义的账号字段属性
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型

	uid	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 OneAccess 系统，此后账号的修改和删除都以此 ID 为主键。字段为 String 类型，必传字段
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功:
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"uid": "89746776",
	"resultCode": "0",
	"message": "success"
	}
	失败:
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"uid": "89746776",
	"resultCode": "1",
	"message": "xxxxxxxxxx"
	}	

5.3.4 UserUpdateService 接口(账号更新)

接口名	UserUpdateService	
功能说明	UserUpdateService 接口是应用系统的账号修改方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型

	uid	三方应用系统账号创建时，返回给 OneAccess 应用系统的账号主键 uid。必传字段
	loginName/ fullName	需要修改的账号字段属性
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功:
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}	

5.3.5 UserDeleteService 接口(账号删除)

接口名	UserDeleteService	
功能说明	UserDeleteService 接口是应用系统的账号删除方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
	uid	三方应用系统账号创建时，返回给 OneAccess 应用系统的账号主键 uid。必传字段

响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}	

5.3.6 FindAllUserIdsService 接口(账号查找)

接口名	FindAllUserIdsService	
功能说明	FindAllUserIdsService 是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	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	uidList	账号主键 ID 列表，字段为 String 数组类型，必传字段

	message	接口调用处理的信息。字段为 String 类型

返回值	{
	"resultCode": "0",
	"message": "success",
	"uidList": ["ID00001", "ID00002", "ID00003"],
	"aimRequestId": "47f591ceca2c410a9fe092af05987f40"
	}	

5.3.7 FindUserByIdService 接口(查询单个账号详情)

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	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	uid	账号 ID。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	account	应用返回的账号 json 对象。必传字段
	message	接口调用处理的信息。字段为 String 类型

返回值	{
	"account": {
	"orgId": "1000-10001-10000011",
	"loginName": "zhangsan",
	"fullName": "zhangsanFull",
	"uid": "D00001"
	},
	"resultCode": "0",
	"message": "success",
	"aimRequestId": "55528d12ec8a4c1bb75283b8df71308d "
	}

5.3.8 OrgCreateService 接口(机构创建，可选)

接口名	OrgCreateService	
功能说明	OrgCreateService 接口是应用系统的组织机构创建方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	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
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	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 OneAccess 系统，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，必传字段。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"orgId": "0000011",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"orgId": "",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}

5.3.9 OrgUpdateService 接口(机构刷新，可选)

接口名	OrgUpdateService	
功能说明	OrgUpdateService 接口是应用系统的组织机构修改方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	orgName / parentOrgId	需要修改的组织机构字段属性
	orgId	三方应用系统组织机构创建时，返回给 OneAccess 应用系统的组织机构主键 orgId。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功:
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败:
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxxxx"
	}

5.3.10 OrgDeleteService 接口(机构删除，可选)

接口名	OrgDeleteService	
功能说明	OrgDeleteService 接口是应用系统的组织机构删除方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	orgId	三方应用系统组织机构创建时，返回给 OneAccess 应用系统的组织机构主键 orgId。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功:
	{
	"aimRequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}

5.3.11 UserPostCreateService 接口(兼岗创建，可选)

接口名	UserPostCreateService	
功能说明	UserPostCreateService 接口是应用系统的兼岗创建方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	emplid/position_nbr	三方应用系统 SchemaService 接口中定义的用户兼岗
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	userPostId	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 OneAccess 系统，此后用户岗位的修改和删除都以此 ID 为主键。字段为 String 类型，必传字段。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"userPostId": "0000011",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"userPostId": "0000011",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}

5.3.12 UserPostUpdateService 接口(兼岗刷新，可选)

接口名	UserPostUpdateService	
功能说明	UserPostUpdateService 接口是应用系统的兼岗修改方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	emplid/position_nbr	需要修改的兼岗字段属性
	userPostId	三方应用系统用户兼岗创建时，返回给 OneAccess 应用系统的组织机构主键 userPostId。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。

	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxx"
	}	

5.3.13 UserPostDeleteService 接口(兼岗删除，可选)

接口名	UserPostDeleteService	
功能说明	UserPostDeleteService 接口是应用系统的兼岗删除方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	userPostId	三方应用系统用户兼岗创建时，返回给 OneAccess 应用系统的用户兼岗主键 userPostId。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败:
	{
	"aimRequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}

5.3.14 PostCreateService 接口(创建，可选)

接口名	PostCreateService	
功能说明	PostCreateService 接口是岗位创建方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	emplid/position_nbr	三方应用系统 SchemaService 接口中定义的用户银行卡属性
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	postId	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 OneAccess 系统，此后用户岗位的修改和删除都以此 ID 为主键。字段为 String 类型，必传字段。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"postId": "0000011",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "11928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}

5.3.15 PostUpdateService 接口(更新，可选)

接口名	PostUpdateService	
功能说明	PostUpdateService 接口是岗位修改方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	emplid/position_nbr	三方应用系统 SchemaService 接口中定义的用户银行卡属性
	postId	三方应用系统用户银行卡创建时，返回给 OneAccess 应用系统的银行卡主键 bankId。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败：
	{
	"aimRequestId": "22928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxx"
	}

5.3.16 PostDeleteService 接口(删除，可选)

接口名	PostDeleteService	
功能说明	PostDeleteService 接口是应用系统的组织机构删除方法	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	postId	三方应用系统用户银行卡创建时，返回给 OneAccess 应用系统的银行卡主键 bankId。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	message	接口调用处理的信息。字段为 String 类型

返回值	成功：
	{
	"aimRequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "0",
	"message": "success"
	}
	失败:
	{
	"aimRequestId": "33928d12ec8a4c1bb75283b8df71308d",
	"resultCode": "1",
	"message": "xxxxxxxx"
	}

5.3.17 FindAllOrgIdsService 接口(机构查找，可选)

接口名	FindAllOrgIdsService	
功能说明	FindAllOrgIdsService 是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	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	orgIdList	组织机构主键 ID 列表，字段为 String 数组类型，必传字段
	message	接口调用处理的信息。字段为 String 类型

返回值	{
	"resultCode": "0",
	"message": "success",
	"orgIdList": ["0000011", "0000012", "0000013"],
	"aimRequestId": "47f591ceca2c410a9fe092af05987f40"
	}

5.3.18 FindOrgByIdService 接口(单个机构详情查询，可选)

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	
请求参数	参数名	中文说明
	iamRequestId	OneAccess 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
	iamRemotePwd	OneAccess 平台调用三方应用接口的授权账号，由应用分配给 OneAccess 系统，String 类型
	orgId	组织机构 ID。必传字段
	iamRemoteUser	OneAccess 平台调用三方应用接口的密码，由应用分配给 OneAccess 系统，String 类型
响应参数	aimRequestId	OneAccess 平台每次调用接口发送的请求 ID，字段为 String 类型
	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。
	organization	应用返回的机构对象。必传字段
	message	接口调用处理的信息。字段为 String 类型

返回值	{
	"organization": {
	"orgName": "信息中心应用处",
	"parOrgId": "000001",
	"orgId": "000012"
	},
	"resultCode": "0",
	"message": "success",
	"aimRequestId": "55528d12ec8a4c1bb75283b8df71308d "
	}

5.3.19 设置票据接口

接口名	setToken		
URL Path	https://{host}:{port}/ idp/restful/setIDPCookie		
请求类型	POST、GET		
请求参数示例	https://{host}:{port}/ idp/restful/setIDPCookie?appId=xxx&tokenId=xxx&jsonpCallback=& remoteIp=		
参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(OneAccess 提供)
	tokenId	用户票据	
	jsonpCallback	回掉函数	Jsonp 回调函数
	remoteIp	客户端 IP	
处理逻辑	判断参数 验证 appId 验证 tokenId 往浏览器中写入 SSO Cookie 返回 app		
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		

5.4 Restful 错误码参考

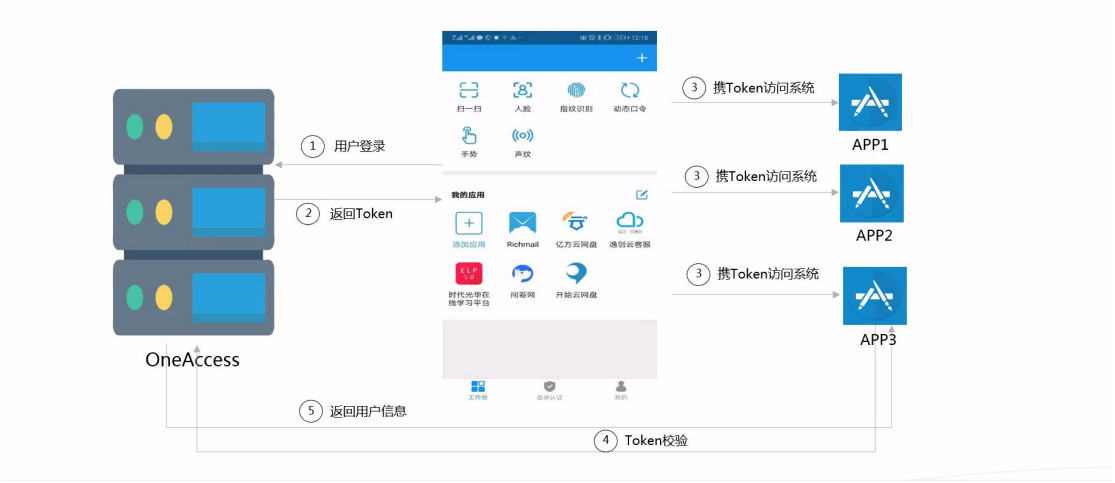
序号	错误代码	错误说明
1	Parameters_missing	参数为空或缺失时
2	invalid_appId	appid 错误
3	invalid_auth_method	authmethod 错误
4	009	使用用户名密码认证，但未配置该认证方式（多种异常）
5	002	用户密码已过期
6	005	管理员强制修改密码
7	004	用户被锁定
8	003	用户被禁用
9	001	userName，password 错误，被删除的用户（用户名密码）

6 移动端应用集成指引

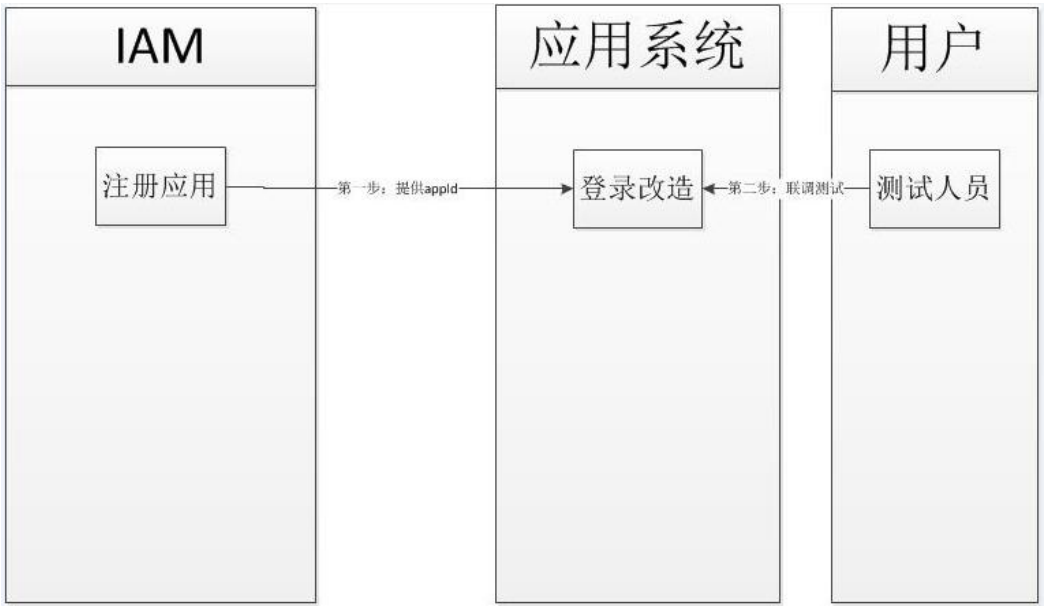
6.1 移动端认证介绍

移动端单点登录集成由 EPASS 平台提供接口服务，采用 Restful 接口协议实现。主要认证接口、获取 SSO 票据接口和获取用户信息接口；同时为了实现 SSO，提供了 1 个认证辅助接口，用于 SSO 票据校验。应用可以根据这 4 个接口，编写应用的访问控制逻辑，实现 SSO 和访问控制。

6.2 移动端认证流程



6.3 移动端集成流程



6.4 移动端 Restful 认证接口规范

6.4.1 认证接口

接口名	doauth
URL Path	https://{host}:{port}/epass-api/api/auth/doauth
请求类型	POST

请求头类型	application/json		
请求体参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(华为 OneAccess 平台提供)
	authPara	认证具体参数	{“loginName”:”sutao”,”password”:”Huawei@123”}
	authType	认证类型	默认 pwd
	device	设备类型	默认 app
	epsessionId	认证会话 ID	默认空字符串
	hostname	认证设备主机名	主机名
	requestType	请求类型	默认 1
请求头参数	operator	鉴权用户名称	默认 hw

返回值	类型：JSON
	正确返回时：
	{
	"code": "info.common.success",
	"message": "",
	"body": {
	"epsessionId": "epsession:admin:20200116094342904:3335",
	"authConsumption": false,
	"jwt": "eyJhbGciOiJIUzI1NiJ9.eyJlcHRva2VuIjoidG9rZW46MTU3OTEzOTAyMjkwNyIsImFwcGlkIjoiZXBhc3NfYXBwIiwic3VidG9rZW4iOiIiLCJ1c2VyaWQiOiJhZG1pbiIsImlhdCI6IjIwMjAtMDEtMTYgMDkuNDMuNDIiLCJ1cGR0IjoiMjAyMC0wMS0xNiAwOS40My40MiJ9.fl8QD9x3DusBAZSdQFG_gJXC9hg3p91Isk0nbC-D-Hw",
	"optkey": "Y2GGCGHBMWH67Q45",
	"lastauthResult": true,
	"authList": "pwd,sms",
	"authedList": "pwd,sms",
	"nextAuthType": "none",
	"addtionalInfo": {
	"voiceModelId": "1",
	"otpKey": "Y2GGCGHBMWH67Q45",
	"faceModelId": "1"
	}
	},
	"status": "success"
	}

6.4.2 令牌校验

接口名	verify		
URL Path	https://{host}:{port}/epass-api/api/jwt/verify		
请求类型	POST		
请求头类型	application/json		
请求体参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(OneAccess 提供)

	jwt	认证接口生成的 jwt	
	token		默认空字符串
请求头参数	operator	鉴权用户名称	默认 hw

返回值	类型：JSON
	正确返回时：
	{
	"code": "info.common.success",
	"message": "操作成功",
	"body": "",
	"status": "success"
	}		

6.4.3 获取 SSO 票据

接口名	getEncryptedString		
URL Path	https://{host}:{port}/epass-api/api/getEncryptedString		
请求类型	POST		
请求头类型	application/json		
请求体参数	参数名	中文说明	描述
	appId	应用标识	客户端应用注册 ID(OneAccess 提供)
	jwt	认证接口生成的 jwt	
	subAccount		默认空字符串
请求头参数	operator	鉴权用户名称	默认 hw

返回值	类型：JSON
	正确返回时：
	{
	"code": "info.common.success",
	"message": "操作成功",
	"body": {
	"encryptedString":
	"P1579080366|pwphkPqwxtFq3i0ofUG7A=#24="
	},
	"status": "success"
	}

6.4.4 获取用户名

接口名	getUserName		
URL Path	https://{host}:{port}/epass-api/api/getUserName		
请求类型	POST		
请求头类型	application/json		
请求体参数	参数名	中文说明	描述
	device	设备类型	默认 app
	entrytedString	sso 票据	
	subAccount		默认空字符串
请求头参数	operator	鉴权用户名称	默认 hw

返回值	类型：JSON
	正确返回时：
	{
	"code": "info.common.success",
	"message": "操作成功",
	"body": {
	"username": "sutao"
	},
	"status": "success"
	}		

6.5 错误码

序号	错误代码	错误说明
1	error.common.param.invalid	参数错误
2	info.common.fail	临时票据失效
3	error.jwtStr.MalformedJwt	JWT 解析失败
4	error.dispatchercenter.jwtsignature	Jwt 令牌签名校验失败
5	error.dispatchercenter.eptoken.search	令牌失效,请重新开启认证
6	error.dispatchcenter.init	认证会话生成失败，请重试
7	error.dispatchercenter.eptoken.content	令牌失效,请重新开启认证
8	error.dispatchercenter.jwt.additional.auth	认证类型有效期过期，请进行补充认证或重新开始认证
9	error.session.time.out	会话已失效，请重新登录

