中国石化统一身份
身份认证 JAVA 版集成指南

(V4.8)

石化盈科信息技术有限责任公司

2025 年 7 月

文档变更纪录

版本编号	版本时间	更新说明	作者
V3.0	2018-1-11	1、应用申请证书流程改为向企业应用管理员申请 2、4.1 中 Demo 页面去掉“命中账号、账号类型”，用户权限判断修改获取应用账号 API 接口。 3、4.2 中增加集成环境和生产网址，完善配置文件修改说明 4、4.3 中完善生产环境注册提交文件说明 5、增加 4.2.2 生产网址，增加 6 补充说明	霍峰峰
V3.1	2018-4-26	1、修正引用参考文献 2、添加 demo 部署 host 配置 3、修改引用上线文档名称 4、修改注册和申请证书的顺序	霍峰峰
V3.2	2018-6-4	1、 调整文档结构、优化集成指导流程 2、 增加图表目录 3、 生产域名更新	建平
V3.2	2018-8-2	1、修证部分描述 2、更新证书申请	冯小龙
V3.2	2019-1-4	1、准生产环境 IP 地址更新	霍峰峰
V3.3	2019-8-16	1、增加了时间同步风险提示	建平
V3.4	2019-11-26	1、配置文件增加了是否自动下载 metadata 开关	建平
V3.5	2019-12-12	1、配置文件增加了断言有效时间差配置;	建平
V3.5	2020-08-03	1、修改了申请流程图步骤 2、修改了日志配置文件配置路径	霍峰峰
V3.6	2020-09-18	1、修改了 8.2 申请流程中提交测试报告等注意事项	霍峰峰
V3.8	2021-12-16	1、修改 5.2 开通防火墙信息 2、修改 7.2.1 证书申请操作方法	统一身份项目组
V3.9	2022-1-20	变更集成环境说明	统一身份项目组
V4.0	2022-4-19	正式环境说明	统一身份项目组
V4.1	2022-8-10	申请流程变更	统一身份项目组
V4.2	2023-6-5	示例更新	统一身份项目组
V4.3	2023-7-4	优化证书相关内容	统一身份项目组
V4.4	2023-10-10	修改邮件地址,优化证书相关内容	统一身份项目组
V4.5	2023-10-31	Ngnix、负载均衡配置说明更新	统一身份项目组
V4.6	2024-3-29	去掉短信验证	统一身份项目组
V4.6	2024-6-5	性别说明中女性值 2 改为 0	统一身份项目组

V4.7	2024-12-18	修改图 5 证书操作流程示意图	统一身份项目组
V4.8	2025-7-29	3、 修改 5.2 开通防火墙信息	统一身份项目组

目录

文档变更纪录 2

1 文档介绍 6

1.1 文档目的 6
1.2 读者对象 6
1.3 参考文献 6
1.4 术语与缩写解释 6

2 概述 7

3 身份认证服务介绍 8

3.1 支持认证方式 8
3.2 认证流程 8
3.3 全局退出流程 9

4 支持版本 10

5 集成准备 10

5.1 环境说明 11
5.2 开通防火墙 11
5.3 示例快速入门 12

6 集成开发 13

6.1 引入类包 13
6.2 引入页面 14
6.3 加载配置项 14
6.3.1 证书配置 14
6.3.2 SP 拦截配置 14
6.3.3 SP 认证配置 15
6.3.4 SP 日志配置 17
6.4 调用 API 17

7 上线准备 19

7.1 开通防火墙 19
7.2 申请证书 19
7.2.1 证书申请操作方法 19
7.2.2 证书操作指导 20
7.3 应用申请集成流程 21
7.3.1 测试环境联调-应用申请流程 21
7.3.2 生产环境上线-应用申请流程 23
7.4 修改配置文件 24

8 上线 25

9 技术支持 25

10 补充说明 25

10.1 认证方式参数说明 25
10.2 用户属性说明 26

11 附件 27

附件 1 需要示例 27
附件 2 证书请求及证书库合成 27

表格 1 术语解释表 6
表格 2 认证方式及类型说明表 8
表格 3 支持的版本说明表 10
表格 4 集成环境地址说明表 11
表格 5 生产环境地址说明表 11
表格 6 集成环境防火墙开通说明表 11
表格 7 生产环境防火墙开通说明表 11
表格 8 集成联调使用 ENTITYID 说明表 13
表格 9 示例页面用途说明表 14
表格 10 用户属性属性获取接口 API 说明表 18
表格 11 上线前需要修改的配置文件参数说明表 24
表格 12 认证方式及参数值说明表 25
表格 13 认证级别及返回的参数值说明表 25
表格 14 用户属性及说明表 26

图 1 认证流程图 9
图 2 统一登出流程图 10
图 3 示例首页下效果图 13
图 4 示例认证成功过后的属性效果图 13
图 5 证书操作流程示意图 19
图 6 在线申请证书示意图 20
图 7 系统登记图 21
图 8 流程申请图 1 22
图 9 系统登记图 2 22
图 10 系统登记图 3 22
图 11 系统登记图 23
图 12 流程申请图 1 23
图 13 流程申请图 2 23
图 14 流程申请图 3 24
图 15 查询已提交集成应用 24

1 文档介绍

1.1 文档目的

本文档描述了如何使用 SAML（联邦认证）对 B/S 应用系统进行统一身份认证集成的步骤方法，为进行统一身份应用集成的开发人员提供参考指导。

1.2 读者对象

本文档的阅读对象为需要与统一认证服务通过 SAML 方式集成用户身份认证的应用开发人员。

1.3 参考文献

《中华人民共和国网络安全法》

《GB/T 25056-2010 信息安全技术 证书认证系统密码及其相关安全技术规范》

《中国石油化工集团公司信息系统安全管理办法》

《中国石化信息系统等级保护技术要求》

《中国石化信息系统等级保护管理要求》

1.4 术语与缩写解释

表格 1 术语解释表

缩写、术语	解释
SAML	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(securitydomain)之间交换认证和授权数据
SP	服务提供者(service provider)即应用系统
IDP	身份提供者(identityprovider)即身份认证中心
TS	认证拓扑

2 概述

中国石化用户统一身份管理系统认证服务采用联邦认证体系进行建设，统一认证服务是一个支撑全石化所有应用的集中服务，为确保认证服务的可靠性和稳定性，认证服务部署在多个节点上，包括：总部、区域中心和灾备中心。

在联邦认证体系中，主要组件包括 IDP、SP 和 TS。IDP（identity provider 身份服务提供方）负责提供身份认证和票据签发服务。SP（service provider 服务提供方）作为服务使用端，接收票据并通过 IDP 验证票据的有效性，完成后转换为应用自己的会话信息。智能 DNS 作为 SP 请求时的第一服务点，会根据用户的认证或 SSO 请求及 ip 地址，判断由统一认证服务中的哪个节点来提供认证服务或由哪个 IDP 来完成对用户已有 SSO 票据进行验证。通过智能 DNS 来帮助应用完成在整个认证服务中的访问和使用，确保认证服务中只要有一个节点可提供服务，就不会中断 IDP 的服务能力。TS（topologry service 拓扑服务）管理整个统一认证中各节点的 IDP、SP 的注册和发布。

其中 IDP、TS 组件运行在统一认证服务服务端。SP 运行在应用服务器环境中。

身份票据将在标准的安全断言标记语言（SAML）基础上，扩展中国石化 SIAM 系统扩展定义的信息，通过扩展信息实现除验证断言外的身份、访问控制信息断言。

3 身份认证服务介绍

3.1 支持认证方式

表格 2 认证方式及类型说明表

序号	安全级别	认证方式
1	安全级别 2	用户名密码
		Ukey
		用户名密码+otp
		用户名+otp
		二维码扫码
		用户名密码+Ukey
2	安全级别 3a	二维码扫码
		用户名密码+otp
		用户名密码+Ukey
3	安全级别 3b	用户名密码+Ukey

注：安全级别高低：安全级别 3>安全级别 2>安全级别 1

3.2 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 完成用户身份认证和单点登录业务流程如下图如示：

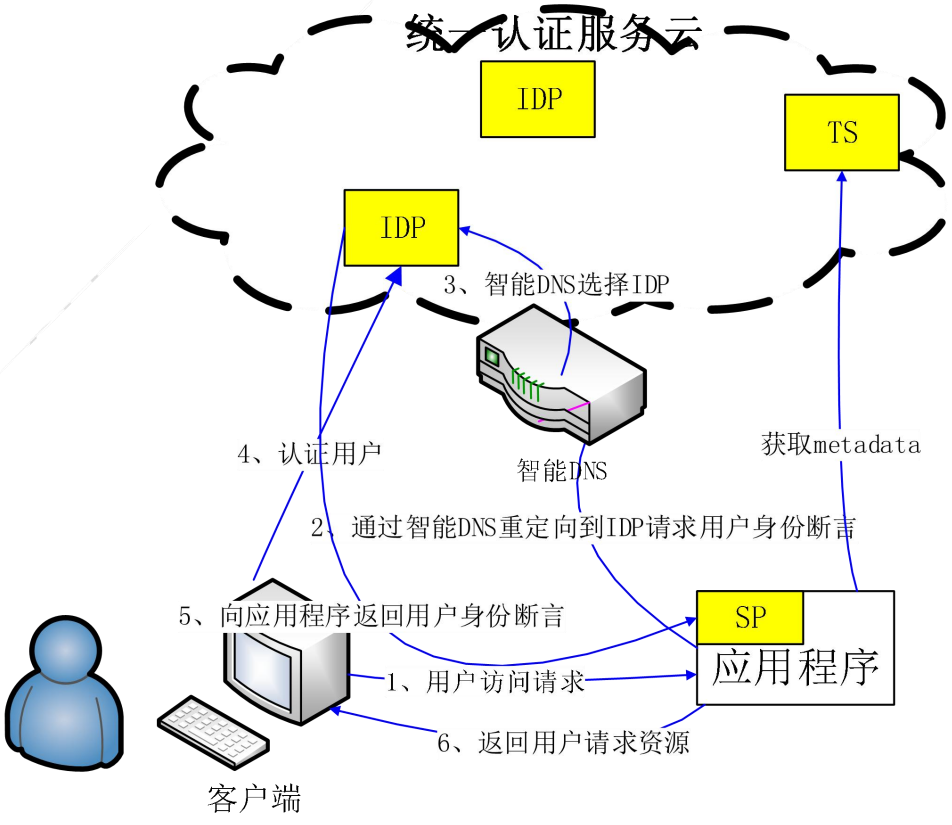


图 1 认证流程图

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 解析到就近的 IDP 认证中心；
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，用户在此输入用户名（支持邮箱标识、别名、手机号、用户标识 UID）/口令；
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 全局退出流程

统一认证服务支持全局退出功能。用户在一个应用程序提交退出，将退出用户此次登录后访问过的所有 B/S 应用程序。

全局退出流程如下：

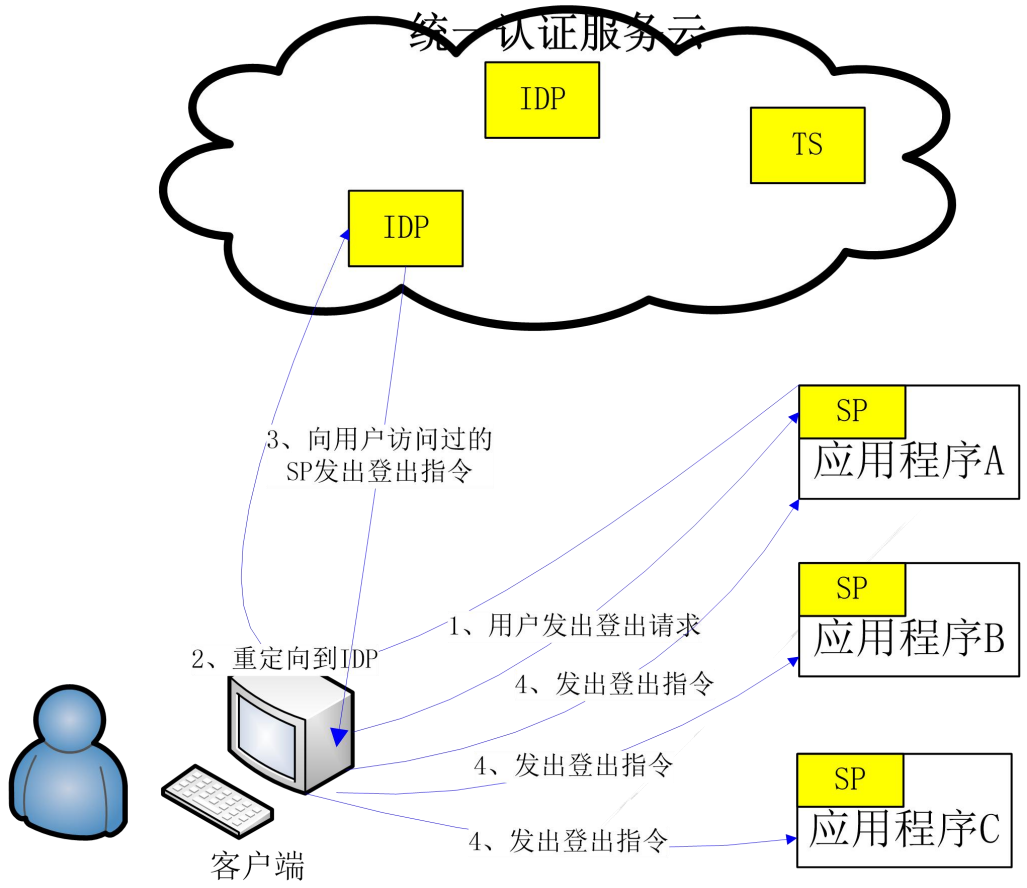


图 2 统一登出流程图

1. 用户在登录后访问过的任一应用系统中发出退出指令（如按退出链接）；
2. SP 获得退出消息，根据应用系统配置要求（如登录后返回页面要求等），生成退出请求，重定向到 IDP；
3. IDP 查找用户登录后访问过的应用系统，依次向用户访问过的应用系统发出退出指令并销毁会话；
4. 根据系统配置要求，返回到指定的页面。

4 支持版本

表格 3 支持的版本说明表

类型	版本
JDK	>=1.5
中间件服务器	Tomcat、weblogic、jboss、webspher e、glassfish 等

5 集成准备

5.1 环境说明

表格 4 集成环境地址说明表

序号	域名	功能介绍
1	ts.uat.siam.sinopec.com	IDP metadata 同步，故障转移
2	auth.uat.siam.sinopec.com	IDP 认证服务
3	idm.uat.siam.sinopec.com	集成环境的控制台，可以添加测试账号。
4	ids.uat.siam.sinopec.com	集成环境自助服务，用于个人信息维护

表格 5 生产环境地址说明表

序号	域名	功能介绍
1	ts.siam.sinopec.com	IDP metadata 同步，故障转移
2	auth.siam.sinopec.com	IDP 认证服务
3	idm.sinopec.com	生产的控制台
4	ids.sinopec.com	生产自助服务

5.2 开通防火墙

应用集成开发时连接统一身份集成环境，针对集成环境地址开通从应用系统开发环境服务器到统一身份集成环境的防火墙策略。详细地址如下：

集成环境：

表格 6 集成环境防火墙开通说明表

序号	域名	地址	端口	通信用途说明
1	ts.uat.siam.sinopec.com	10.249.128.228（沙河区域中心）	443	IDP metadata 同步
2	mqs.uat.siam.sinopec.com	10.249.128.125（沙河区域中心）	443	消息订阅服务

生产环境：

表格 7 生产环境防火墙开通说明表

序号	域名	地址	端口	通信用途说明
1	ts.siam.sinopec.com	10.249.201.228（沙河区域中心）	443	IDP metadata 同步，故障转移
2	ts.siam.sinopec.com	10.54.106.112（胜利区域中心）	443	IDP metadata 同步，故障转移
3	ts.siam.sinopec.com	10.54.86.250（广州区域中心）	443	IDP metadata 同步，故障转移

4	ts.siam.sinopec.com	10.54.149.242（成都区域中心）	443	IDP metadata 同步，故障转移
5	ts.siam.sinopec.com	10.54.139.242（新疆区域中心）	443	IDP metadata 同步，故障转移
6	ts.siam.sinopec.com	10.53.234.247（香港区域中心）	443	IDP metadata 同步，故障转移
7	mqs.siam.sinopec.com	10.249.201.232（沙河区域中心）	443	消息订阅服务

风险提示：

a) 智能 DNS 通过域名进行解析，host 中不要写固定的 IP，否则无法做到故障转移。

b) 应用系统服务器与时间同步配置修改为与 time.sinopec.com 进行同步。

5.3 示例快速入门

通过在应用开发环境部署示例、试运行，测试示例可用性及熟悉示例运行过程，部署步骤如下：

1) 从 https://auth.uat.siam.sinopec.com/help 下载示例。

2) 准备好中间件部署服务器环境，部署 SPForJava1.5-V**.rar 包。按 tomcat 举例，删除原先的 ROOT，修改示例包名为 ROOT.war，并启动 tomcat。

3) 在用 PC 计算机配置 hosts,在 C:\Windows\System32\drivers\etc\hosts 文件第一行添加：

```
#应用服务器 IP（若部署在本机设置为如下） test.java.sinopec.com
    127.0.0.1              test.java.sinopec.com
```

4) 访问地址：https://test.java.sinopec.com:9443

效果图如下：



图 3 示例首页下效果图

认证成功后返回属性，效果图如下：

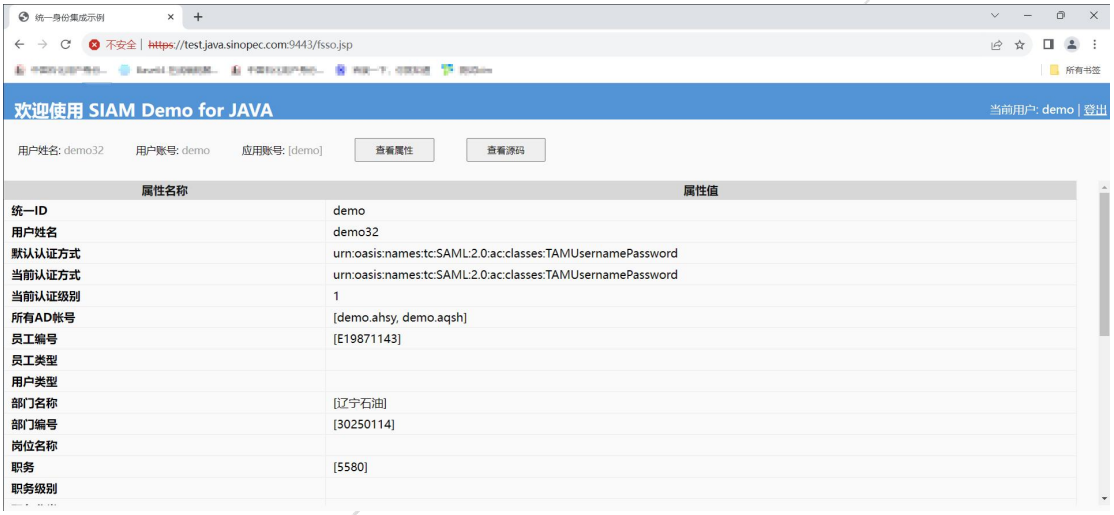


图 4 示例认证成功过后的属性效果图

6 集成开发

应用系统与统一身份认证服务集成从引入类包、引入页面、加载配置项、调用 API 等 4 个方面进行。为方便应用方在集成环境进行集成改造，准备了如下域名及 IP 地址供应用系统集成联调使用。如下表：

表格 8 集成联调使用 entityid 说明表

序号	Entityid	tsysAccount	应用名称
1	https://test.java.sinopec.com:9443	\u793A\u4F8B	示例

6.1 引入类包

将 demo 示例中的 siam-am-agent-simple-*.*.RELEASE.jar 包加入到应用的 lib 类库。

6.2 引入页面

表格 9 示例页面用途说明表

序号	文件名	描述	是否必选
1.	appdebug.jsp	显示当前用户认证报文，以 xml 格式显示；	可选
2.	error.jsp	应用访问过程中出现错误时跳转到此页，title 改为应用系统名称，显示报错详细信息；	必选
3.	fsso.jsp	显示用户属性信息；	可选
4.	index.jsp	demo 首页，显示认证方式、安全级别及元数据下载按钮；	可选
5.	init.jsp	下载元数据；	必选
6.	no_access.jsp	用于无权限访问应用时跳转到此页面，title 改为应用系统名称；	必选
7.	spversion.html	显示 demo 版本信息；	可选

6.3 加载配置项

6.3.1 证书配置

在配置文件\WEB-INF\classes\conf\sp-simple-config.properties 中配置了证书的存放位置，参数为：sp.credential.keyStorePath，可根据应用自身情况修改。将证书库文件存放在配置文件中指定的目录。对应修改配置文件中的证书密码及别名，参照《6.3.3 SP 认证配置》。

6.3.2 SP 拦截配置

在应用工程 web.xml 中增加如下配置项，加载配置文件项：

```
<context-param>
<param-name>spSimpleConfigFile</param-name>
<param-value>classpath:/conf/sp-simple-config.properties</param-value>
</context-param>
```

认证拦截配置项：

```
<!-- Filter for SAML handler -->
<filter>
    <filter-name>com.sinopec.siam.agent.web.SAMLProfileFilter</filter-name>
 <display-name>com.sinopec.siam.agent.web.SAMLProfileFilter</display-nam
e>
 <filter-class>com.sinopec.siam.agent.web.SAMLProfileFilter</filter-class>
</filter>
<filter-mapping>
 <filter-name>com.sinopec.siam.agent.web.SAMLProfileFilter</filter-name>
 <url-pattern>/SSO/*</url-pattern>
```

```
    </filter-mapping>

    <!-- Merge Filter -->
      <filter>
     <filter-name>AccessEnforcerAuthen</filter-name>
     <display-name>AccessEnforcerAuthen</display-name>
     <filter-class>com.sinopec.siam.agent.web.AccessEnforcer</filter-class>
     <init-param>
      <param-name>noFilterURLs</param-name>
    <!—下面的 param-value 内容根据实际情况进行修改，修改后的内容不被 filter 拦截 -->
      <param-value>/;/test/test.jsp;/test1/*/a.txt;/index.jsp;/images/*;/js/*;/styles/*;/init.jsp;/init2.jsp;/spversion.html</param-value>
     </init-param>
    </filter>
    <filter-mapping>
     <filter-name>AccessEnforcerAuthen</filter-name>
    <!—下面的 url-pattern 内容根据实际情况进行修改，修改后的内容被 filter 拦截，跳转到 IDP-->
     <url-pattern>/*</url-pattern>
    </filter-mapping>
```

6.3.3 SP 认证配置

将\WEB-INF\classes\conf\sp-simple-config.properties 文件放置 web.xml 中配置的对应目录。修改如下参数：

```
    #默认认证方式（根据实际情况配置）
    sp.auth.method.default=TAMUsernamePassword
    #集成环境获取 sp、 idp 的 metadata 文件地址
    sp.metadata.ts.download.url=https://ts.uat.siam.sinopec.com
    #生产环境获取 sp、 idp 的 metadata 文件地址
    #sp.metadata.ts.download.url=https://ts.siam.sinopec.com
    #SP 应用节点 ID（根据实际情况配置）
    sp.metadata.url.entityId=https://test.java.sinopec.com:9443
    #应用 code，将汉字转换为 ASCII 码（根据实际情况配置）
    sp.login.tsysAccount=\u793A\u4F8B
    #证书路径（根据实际情况配置，集成环境测试使用示例包中的配置）
    sp.credential.keyStorePath=classpath:/certs/test.uat.siam.sinopec.com.jks
    #证书库密码（根据实际情况配置,需 help 网站 DES 加密，集成环境测试使用示例包中的配置）
    sp.credential.keyStorePassword=6ArCSisuIHxZ4/RvJPpWdA==
    # 证书密码（根据实际情况配置，需 help 网站 DES 加密，集成环境测试使用示例包中的配置）
```

```
sp.credential.keyPassword=6ArCSisuIHxZ4/RvJPpWdA==
#证书别名（根据实际情况配置，集成环境测试使用示例包中的配置）
sp.credential.keyAlias=test.uat.siam.sinopec.com
#集成环境 IDP 应用节点 ID
sp.saml2.idp.entityId=https://auth.uat.siam.sinopec.com/idp
#生产环境 IDP 应用节点 ID
#sp.saml2.idp.entityId=https://auth.siam.sinopec.com/idp
#metadata 请求超时时间，单位毫秒（根据实际情况配置）
ts.metadata.requestTimeout=30000
#ts 下载是否为 https，此项必须为 true
ts.metadata.disregardSSLCertificate=true
#metadata 是否自动下载 true:自动下载，false:使用本地文件，需要手工考入
ts.metadata.download.auto=true
#metadata 最小自动更新时间，单位毫秒（根据实际情况配置）默认 10 天不能超过 23 天
ts.metadata.minRefreshDelay=864000000
#metadata 最大自动更新时间，单位毫秒（根据实际情况配置）默认 15 天不能超过 23 天
ts.metadata.maxRefreshDelay=1296000000
# SP Key Store Type: jks
sp.credential.keyStoreType=jks

#saml 返回报文和本地校验安全区间，单位秒，默认 10 分钟
siam.reponse.safe.time.range=600
```

下面部分，如果应用使用了 nginx、apache、负载均衡等代理服务时配置，默认为 false 状态。

```
#siam.sp.proxy.web.urls:应用服务器 url 列表
#F5/nginx 负载代理时使用如下配置 flag=true
siam.sp.proxy.web.urls 中配置分发的应用服务器 URL
#配置示例:siam.sp.proxy.web.urls=[http://java.uat.sinopec.com:8080/spv32/SSO/SAML2/POST],[http://127.0.0.1:8088/spv32/SSO/SAML2/POST],[http://java.uat.sinopec.com:8088/spv32/SSO/SAML2/POST]
siam.sp.proxy.load.url 中配置访问地址
#配置示例:siam.sp.proxy.load.url=https://java.uat.sinopec.com:8443/proxy_path
#配置示例:siam.sp.proxy.flag=true
siam.sp.proxy.web.urls=
siam.sp.proxy.load.url=
siam.sp.proxy.flag=false
```

6.3.4 SP 日志配置

将\WEB-INF\classes\conf\sp-saml-Log4j.properties 文件放置在 classpath:/conf 下面。

```
#回滚日志配置
#方式 1：每日生成一个文件
#DEBUG,INFO,ERROR,建议切换生产后使用 INFO 或 ERROR
log4j.rootLogger=ERROR,C3
#方式 2：按文件大小个数保留最新限定日志文件
#DEBUG,INFO,ERROR,建议切换生产后使用 INFO 或 ERROR
#log4j.rootLogger=ERROR,R
```

方式 1：每日生成一个文件

通过修改配置实现控制台打印日志输出配置、认证日志输出配置和 metadata 下载日志输出配置。分别为：

```
认证日志配置项
log4j.appender.C3.Threshold=ERROR
log4j.appender.C3.File=${catalina.home}/logs/saml_auth.log
metadata 下载日志配置项
log4j.appender.C4.File=${catalina.home}/logs/metadata_down.log
```

方式 2 按文件大小个数保留最新限定日志文件

通过修改配置，实现对应用日志文件的切割，Log4j 支持对日志文件大小及个数的配置。如下参考：

```
# 应用于文件回滚
log4j.appender.R=com.sinopec.siam.apache.log4j.RollingFileAppender
log4j.appender.R.Threshold=ERROR
log4j.appender.R.File=${catalina.home}/logs/saml_authR.log
log4j.appender.R.Append=true
#文件大小按情况设置
log4j.appender.R.MaxFileSize=100MB
#保留文件个数按情况配置
log4j.appender.R.MaxBackupIndex=10
log4j.appender.R.layout=com.sinopec.siam.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern=[%-5p] %d{yyyy-MM-dd HH\:mm\:ss,SSS}\:%c[%M][line\:%L] %m%n m\:ss}\: %c %m%n
```

6.4 调用 API

用户在通过统一身份认证之后，统一身份系统会将用户信息返回到应用，其中包括应用账号及用户基础信息，应用账号根据 API 接口 ssoPrincipal.getAppAccount()来判断是否存在本应用的账号。如果不存在则提示用户没有权限访问应用系统。如果存在并且应用已经授权，则进入应用系统。更多 API 接口请看《附录：API 接口说明表》。

备注：getAppAccount()的取值取决于配置文件 sp-simple-config.properties 中的参数 sp.login.tsysAccount 的值。

附录：API 接口说明表

通过对象 ssoPrincipal 获取以下属性，例如：ssoPrincipal.getUid()。

表格 10 用户属性属性获取接口 API 说明表

序号	属性名称	属性获取
1	应用账号	getAppAccount()
2	统一 ID	getUid()
3	用户姓名	getCn()
4	员工编号	getValueAsList("employeeNumber")
5	员工类型	getValueAsList("employeeType")
6	部门名称	getValueAsList("ou")
7	部门编号	getValueAsList("departmentNumber")
8	岗位名称	getValueAsList("spPositionName")
9	职务	getValueAsList("title")
10	职务级别	getValueAsList("spTitleLevel")
11	职务分类	getValueAsList("spTitleCategory")
12	职务编码	getValueAsList("spTitleNumber")
13	所有 AD 账号	getAdAccounts()
14	默认 AD 账号	getValueAsList("ADAccountName")
15	组织编码全路	getValueAsList("spOrgCodePath")
16	组织名称全路径	getValueAsList("spOrgNamePath")
17	电子邮件地址	getValueAsList("mail")
18	性别	getValueAsList("spGender")
19	国籍	getValueAsList("spCountry")
20	用户级别	getValueAsList("spEmployeeLevel")
21	国家代码	getValueAsList("c")
22	默认认证方式	getLastAuthenMethod()
23	当前认证方式	getActualAuthMethod()
24	当前认证级别	getActualAuthLevel()
25	密码最后修改时间	getValueAsList("ChangePwdAt")

7 上线准备

7.1 开通防火墙

参照步骤《5.2 开通防火墙》。

7.2 申请证书

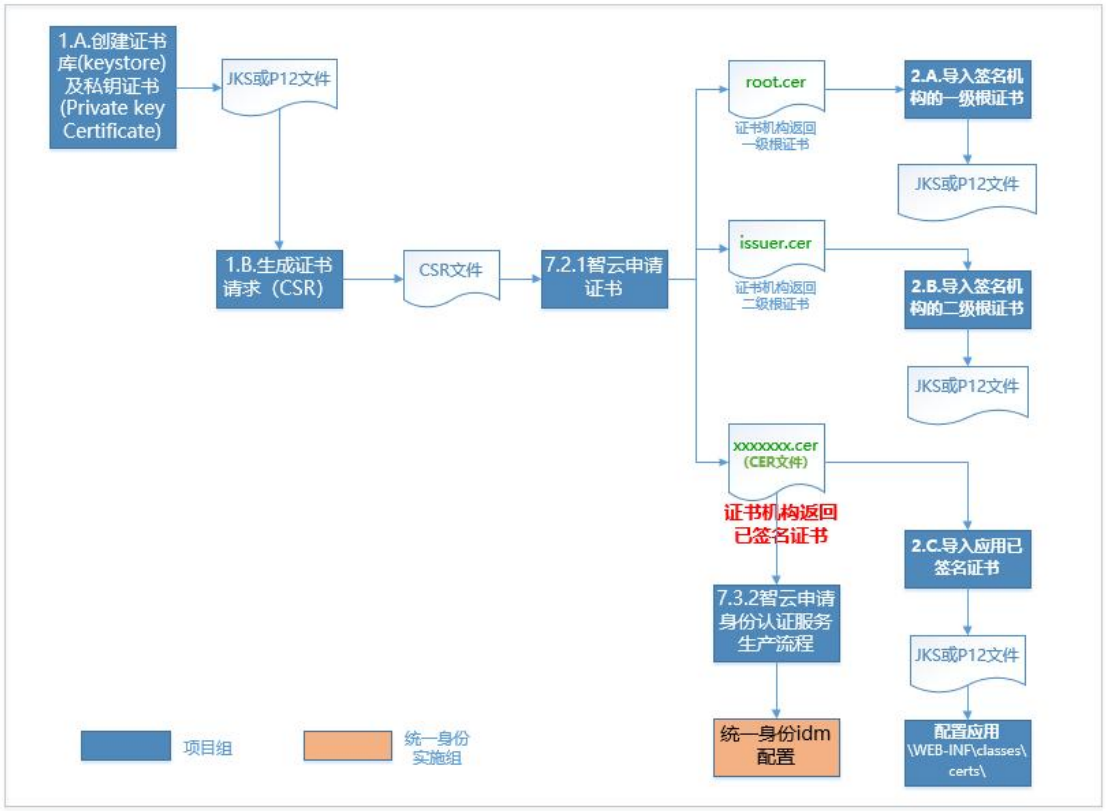


图 5 证书操作流程示意图

7.2.1 证书申请操作方法

- 企业应用证书申请流程
  企业申请证书联系各企业证书管理员。
- 总部应用证书申请流程
  在中国石化智云平台 http://icloud.sinopec.com【服务目录】-->【安全服务】-->【数字证书服务】提交申请。如图：



图 6 在线申请证书示意图

7.2.2 证书操作指导

1、 生成证书请求

A. 创建证书库(keystore)及私钥证书(Private key Certificate):

命令	参数
Keytool -genkeypair \ -alias test.mydomain.com \ -keyalg RSA \ -keysize 2048 \ -keypass mypassword \ -sigalg SHA256withRSA \ -dname "CN=test.mydomain.com,OU=SINOPEC,O=SINOPEC,L=beijing,C=CN" \ -validity 5475 \ -keystore D:\test.mydomain.com_keystore.jks \ -storetype JKS \ -storepass mypassword	 别名 证书类型 密钥长度 私钥密码 签名算法 证书域名 证书有效天 JKS 文件 证书库类型 证书库密码

注：红色、绿色部分变化即可

B. 生成证书请求(CSR)

命令	参数
keytool -certreq -keyalg RSA \ -alias test.mydomain.com \ -keystore D:\test.mydomain.com_keystore.jks \ -storetype JKS \ -storepass mypassword \ -file D:\test.mydomain.com_certreq.csr	 别名 JKS 文件 证书库类型 证书库密码 证书请求文件

注：D:\test.mydomain.com_certreq.csr 用于申请证书，参见 7.2.1 章节。

2、 将颁发证书导入证书库

A. 导入签名机构的一级根证书：

命令	参数
keytool -import -trustcacerts \ -keystore D:\test.mydomain.com_keystore.jks \ -storepass mypassword \ -alias root \ -file D:\root.cer	 JKS 文件 证书库密码 根证别名 证书机构返回一级根证

B. 导入签名机构的二级根证书：

命令	参数
keytool -import -trustcacerts \ -keystore D:\test.mydomain.com_keystore.jks \ -storepass mypassword \ -alias issuer \ -file D:\issuer.cer	 JKS 文件 证书库密码 根证别名 证书机构返回二级根证

C. 导入 test.mydomain.com 的已签名证书

命令	参数
keytool -import -trustcacerts \ -keystore D:\test.mydomain.com_keystore.jks \ -storepass mypassword \ -alias test.mydomain.com \ -file D:\test.mydomain.com_cert.cer	 JKS 文件 证书库密码 别名 证书机构返回应用证书

注：D:\test.mydomain.com_keystore.jks 用于替换原有的测试证书。

7.3 应用申请集成流程

登录中国石化智云平台（https://icloud.sinopec.com）进行注册，注册申请审批通过后，统一身份项目组将注册后的信息通过邮件形式反馈给申请人。

7.3.1 测试环境联调-应用申请流程

第一步：系统登记。在智云平台中登记应用系统。登记后系统与项目进行关联。（**若已登记，请跳过此步**）



图 7 系统登记图

第二步：身份认证服务。在智云平台【首页】-【服务目录】-【安全服务】-【身份认证服务】-【加入购物车】-填写表单内容-【加入申请单】。



图 8 流程申请图 1



图 9 系统登记图 2

【开发运维】-【服务订阅】-【订阅申请】-【提交】

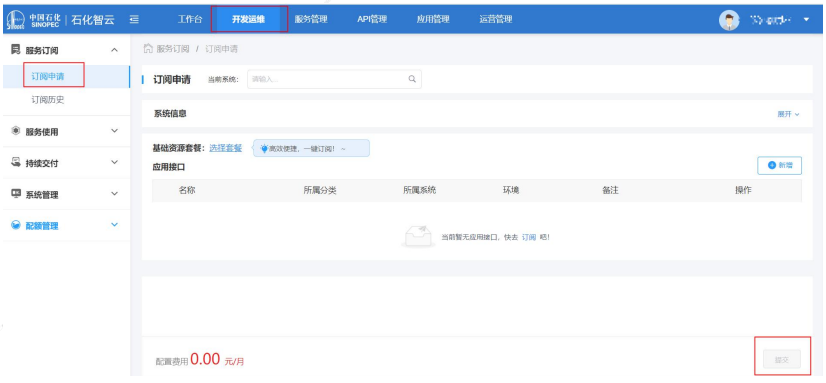


图 10 系统登记图 3

第三步：统一身份团队评估，通过后转交系统业务主管理部门或项目管理处室进行审批。

第四步：系统业务主管理部门或项目管理处室审批通过后，转交服务归属责任人审批。

第五步：服务归属责任人审批通过后，转交统一身份集成组实施。

第六步：统一身份集成组实施完后，将信息通过邮件反馈申请人。应用项目组完成联调测试后，**将联调测试报告发给 tysf01@sinopec.com。（提示：为保证生产环境上线成功，请通过测试后，再提生产上线流程）**

第七步：申请人确认资源已收到。

7.3.2 生产环境上线-应用申请流程

第一步：系统登记。在智云平台中登记应用系统。登记后系统与项目进行关联。（**若已登记，请跳过此步**）



图 11 系统登记图

第二步：身份认证服务。在智云平台【首页】-【服务目录】-【安全服务】-【身份认证服务】-【加入购物车】-填写表单内容-【加入申请单】。（**在此环节同时申请数字证书，见 7.2 申请证书。请测试联调通过再提交此流程，流程提交时上传证书机构返回的应用已签名证书 CER 文件**）。



图 12 流程申请图 1



图 13 流程申请图 2

【开发运维】-【服务订阅】-【订阅申请】-【提交】

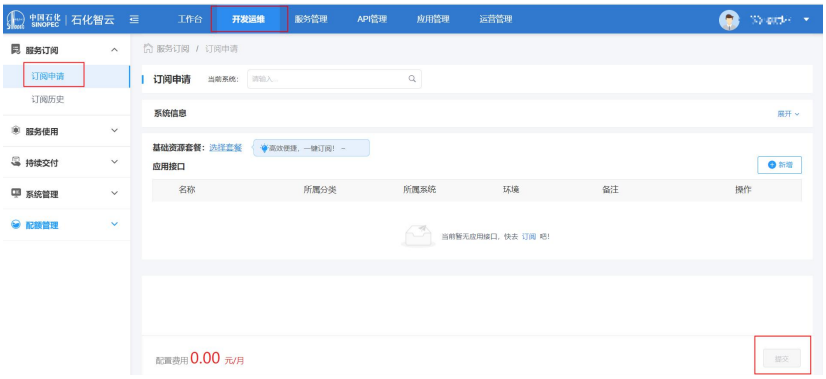


图 14 流程申请图 3

第三步：统一身份团队评估，通过后转交系统业务主管理部门或项目管理处室进行审批。

第四步：系统业务主管理部门或项目管理处室审批通过后，转交服务归属责任人审批。

第五步：服务归属责任人审批通过后，转交统一身份集成组实施。

第六步：统一身份集成组实施完后，将信息通过邮件反馈申请人。

第七步：申请人确认资源已收到。

7.3.3 已提交应用流程查询

【首页】-【云工作台】-【工作台】-【我的发起】-查询应用系统



图 15 查询已提交集成应用

7.4 修改配置文件

在 sp-simple-config.properties 文件中修改配置为生产环境所需的值，参照《6.3.3 SP 认证配置》，需要修改的参数如下：

表格 11 上线前需要修改的配置文件参数说明表

序号	配置项	地址
1	sp.metadata.ts.download.url	ts.siam.sinopec.com
2	sp.saml2.idp.entityId	auth.siam.sinopec.com
3	sp.metadata.url.entityId	参照注册申请表
4	sp.credential.keyStorePath	证书库文件存放路径
5	sp.credential.keyStorePassword	证书库密码
6	sp.credential.keyPassword	证书密码

7	sp.credential.keyAlias	证书别名
8	siam.sp.proxy.flag	使用了代理负载时 true
9	siam.sp.proxy.web.urls	按实际情况配置
10	siam.sp.proxy.load.url	负载 URL

8 上线

部署集成后的应用系统包部署到正式环境，并在线上进行联调测试，联调测试成功即上线成功。

9 技术支持

统一身份实施支持：

电话：010-84191129

证书咨询：

电话：010-84191128

10 补充说明

10.1 认证方式参数说明

表格 12 认证方式及参数值说明表

序列	参数说明	说明
1	TAMUsernamePassword	用户名+密码
2	OTPUsername	用户名+OTP
3	SIAMTLSClient	Ukey
4	OTPUsernamePassword	用户名密码+OTP
5	UsernamePasswordClientCert	用户名密码+Ukey
6	QRUsername	二维码扫码

获取当前认证级别以及认证方法说明

SAML 认证后，获取当前认证级别以及认证方法的接口：

```
SSOPrincipalssoPrincipal = ((SSOPrincipal) session.getAttribute(NAME_OF_SESSION_ATTR));
getValueAsList("spActualAuthLevel") ;
getValueAsList("spActualAuthMethod") ;
```

返回认证级别和认证方式说明

表格 13 认证级别及返回的参数值说明表

spActualAuthLevel	spActualAuthMethod	说明
1	urn:oasis:names:tc:SAML:2.0:ac:classes:T	用户名+密码

	AMUsernamePassword	
1	urn:oasis:names:tc:SAML:2.0:ac:classes:OTPUsername	用户名+OTP
1	urn:oasis:names:tc:SAML:2.0:ac:classes:QRUsername	二维码扫码
2	urn_oasis_names_tc_SAML_2.0_ac_classes_SIAMTLSClient	UKEY+PIN 码
2	urn:oasis:names:tc:SAML:2.0:ac:classes:OTPUsernamePassword	用户名+密码+OTP
3	urn:oasis:names:tc:SAML:2.0:ac:classes:UsernamePasswordClientCert	用户名+密码+UKEY

10.2 用户属性说明

表格 14 用户属性及说明表

序号	属性名称	属性类型	属性描述
1	account_uid	string	应用账号
2	uid	string	用户 ID
3	cn	string	姓名
4	employeeNumber	string	员工编号
5	employeeType	string	员工类型（HR 员工才有）
6	userType	string	用户类型 HR 用户: person 非 HR 用户： 非 HR-海外用户 spForeignExternalPerson 非 HR-临时用户 spTemporaryPerson 非 HR-长期用户 spExternalPerson
7	ou	string	部门名称
8	departmentNumber	string	部门编号
9	spPositionName	string	岗位名称
10	title	string	职务
11	spTitleLevel	string	职务级别
12	spTitleCategory	string	职务分类
13	spTitleNumber	string	职务编码
14	ADAccountName	string	默认 AD 账号
15	spOrgCodePath	string	组织编码全路径
16	spOrgNamePath	string	组织名称全路径
17	mail	string	电子邮件地址
18	spGender	string	性别 1:男 0:女
19	spCountry	string	国籍

20	spEmployeeLevel	string	用工级别
21	c	string	国家代码（标准属性）
22	spUpdateDate	string	最后更新时间
23	ChangePwdAt	string	密码最后修改时间
24	spPluralityOrgCodePath	string	兼职组织 code 全路径
25	spPluralityOrgNamePath	string	兼职组织名称全路径
26	spTransferStatus	string	用户借调状态:true(开始);false(结束);none(非借调、交流)
27	appgroup	string	应用账号所属组（多值）

11 附件

附件 1 示例

请参见网址：https://auth.uat.siam.sinopec.com/help

附件 2 证书请求及证书库合成

请参见网址：https://auth.uat.siam.sinopec.com/help/FAQ.jsp