四川省生态环境信息化
统一身份与安全认证接入规范

（试行）

四川省生态环境厅

目 次

前 言 II
1 适用范围 1
2 规范性引用文件 1
3 术语和定义 1
4 总则 3
5 统一身份集成规范 3
6 数据规范 4
7 统一安全认证过程 6
8 认证内容要求 6
附 录 A 统一身份集成说明 8
附 录 B 认证集成配置说明 19
附 录 C 组织机构编码 23

前 言

基于四川省环境信息化三级统筹项目建设的 4A 系统，可充分利用已有资源，做到统一管理、统一协调、数据同步、统一管理、统一认证。为四川环境信息化各业务系统中的数据完整性、可靠性、可用性提供保障，避免各业务系统出现各自为政和信息孤岛的现象。

本规范在充分考虑四川省环境信息化建设需求的基础上，制定了基础统一身份管理的数据规范、同步规范、接口规范、接入规范。同时就各业务系统如何与基础支撑平台 4A 系统实现统一身份管理的对接进行详细的说明，各业务系统需要按照本规范中给出的配置信息修改系统相应的配置文件，从而实现统一身份管理与安全认证功能。

本规范规定了统一身份集成规范和数据规范两大类，其中数据规范规定了组织机构数据规范、内设部门数据规范、直属单位数据规范和用户命名数据规范。

本规范由四川省环境信息中心负责解释。

统一身份与安全认证接入规范

1 适用范围

本规范适用于需要与基础支撑平台 4A 系统对接，实现统一身份管理的各业务系统，包括省级统建的、省级自建的以及市/州/县自建的系统。所有已建和待建系统的均参照该接入规范进行对接。本规范是统一身份管理的集成文档。

2 规范性引用文件

本规范引用下列文件中的条款。凡是未注明日期的引用文件，其有效版本适用于本规范。

GB/T 2260-2019　中华人民共和国行政区划代码

GB/T 18336-2015 信息技术安全技术信息技术安全性评估准则

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 20272-2006 信息安全技术_操作系统安全技术要求

GB/T 21064-2007 电子政务系统总体设计要求

GB/T 22239-2008 信息安全技术_网络安全等级保护基本要求

GB/T 25070-2010 信息系统等级保护安全设计技术要求

GB/T 28448-2012 信息系统安全等级保护测评要求

HJ/T 418-2007 环境信息系统集成技术规范

3 术语和定义

以下术语和定义适用于本规范。

3.1 应用集成

将业务流程、应用软件、硬件和各种标准联合起来，在两个或更多的企业应用系统之间实现无缝集成，使它们像一个整体一样进行业务处理和信息共享。

3.2 对象简谱

JSON(JavaScript Object Notation, JS 对象简谱) 是一种轻量级的数据交换格式。JSON 简洁和清晰的层次结构使得它成为理想的数据交换语言。

3.3 单点登录

Single Sign On,简称 SSO，SSO 使得在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统。

3.4 统一认证框架

CAS（Central Authentication Service）是实现 SSO 单点登录的框架。是 Yale（耶鲁）大学的一个开源的企业级单点登录框架。

3.5 证书认证

即 Certificate Authority 的缩写，是电子政务服务的证书中心，是 PKI（Public Key Infrastructure）体系的核心，它为用户的公开密钥签发公钥证书、发放证书和管理证书，并提供一系列密钥生命周期内的管理服务。它将用户的公钥与用户的名称及其他属性关联起来，为用户之间电子身份进行认证。

3.6 实体

可对系统或服务发起访问或请求的对象。

3.7 身份

实体在信息系统中的映射，包括实体的标识和相关属性。

3.8 身份管理

对实体的身份标识、属性和生命周期所进行的管理。

3.9 身份同步

使同一个实体在不同信息系统中的属性保持一致的相对关系。

3.10 组织机构

省级、市级、区县级环保机构以及直属单位。

3.11 内设部门

各级环保单位下的部门。

3.12 机构同步

使同一个组织机构在不同信息系统中属性保持一致的相对关系。

3.13 消息中间件

ActiveMQ 是 Apache 出品的开源消息总线。ActiveMQ 是一个完全支持 JMS1.1 和 J2EE 1.4 规范的 JMS Provider 实现，支持 Java,C,C++,C#,Ruby,Perl,Python,PHP 等多种语言。

4 总则

基于四川省环境信息化三级统筹项目建设的 4A 系统，可充分利用已有资源，做到统一管理、统一协调、数据同步、统一管理、统一认证。为四川环境信息化各业务应用系统中的数据完整性、可靠性、可用性提供保障，同时减少重复建设，避免各业务应用系统出现各自为政和信息孤岛的现象。

本规范在充分考虑四川省环境信息化建设需求的基础上，制定了基础统一身份管理的数据规范、同步规范、接口规范、接入规范。同时就四川省环境信息化领域内，各个业务系统如何与基础支撑平台 4A 系统实现统一身份管理的对接进行了详细的说明，各业务系统需要按照本规范中给出的配置信息修改各自系统相应的配置文件，从而实现统一身份管理与安全认证的功能。

5 统一身份集成规范

5.1 集成模式介绍

4A 系统统一用户身份集成，采用基于消息队列的数据交换模式实现。4A 系统通过不同的消息队列，向各业务系统同步组织机构与用户数据。各业务系统从各自的消息队列接收数据并保存在本地，保存之后，将操作结果发送至反馈消息队列中，4A 系统对反馈结果进行处理，完成数据同步过程。

5.2 技术要求

集成到 4A 系统的各应用系统技术要求为：

a) 所有遵循 HTTP 协议的开发语言。

b) 可以从消息队列 ActiveMQ 中获取数据。

c) 数据交互的双方必须对数据加密处理。4A 系统提供加解密算法。

6 数据规范

定义统一身份数据规范的目的是使用统一的命名和编码规则，使不同的机构、部门和用户命名及编码风格标准化，以便于阅读、理解和继承。

通过命名规范的定义，为各级信息化人员管理和新增机构、部门和用户信息提供参考依据和规范准则。

6.1 组织机构数据规范

使用正规表述作为机构名称，与行政区划匹配、可基于既定通用规则进行管理；命名规范可方便后期与其他业务子系统的对接，规范参考《GB/T 2260-2019 中华人民共和国行政区划代码》。

组织机构编码由20位组成，第1，2位表示省级，第3，4位表示市级，第5，6位表示区县级，第7，8位表示乡镇级，第9，10位表示村级，第11-20位表示村级管理单位或预留扩充编码使用。

以成都市为例：51010000000000000000

表 1 组织机构编码示例表

省级编码	市级编码	区县编码	乡镇编码	村级编码	预留
51	01	00	00	00	0000000000

6.2 内设部门数据规范

对于每一层级环保组织机构根据自身实际情况设置各自的内设部门信息。内设部门目前主要划分为“综合部门”、“业务部门”、“信息化部门”几类。

内设部门编码由20位组成，前十位表示部门所在组织机构，最后四位表示部门独立编码。前十位中第1，2位表示省级，第3，4位表示市级，第5，6位表示区县级，第7，8位表示乡镇级，第9，10位表示村级。中间6位预留，最后四位是部门独立编码，以‘D’开头，按顺序增加。

以成都市环保局办公室为例：51010000000000000D001

表 2 内设部门编码示例表

省级编码	市级编码	区县编码	乡镇编码	村级编码	预留编码	部门编码
51	01	00	00	00	000000	D001

6.3 直属单位数据规范

对于每一层级环保组织机构根据自身实际情况设置各自的直属单位信息。

直属单位编码由20位数字+字母组成，数字表示所属组织机构，字母表示直属单位独立编码。字母放在数字后，由‘AA’起始，到‘ZZ’结束，按顺序增加。

以成都市环境监察执法支队为例：5101AA00000000000000

表 3 直属单位编码示例表

省级编码	市级编码	直属单位编码	默认编码	默认编码	默认编码
51	01	AA	00	00	0000000000

6.4 用户命名数据规范

用户命名数据规范主要分为三类。

a) 用户登录帐号规范

用户登录帐号为登录系统的用户名，此名称为系统的唯一登录ID，以用户邮箱为登录帐号。

b) 用户名称规范

用户名称为用户姓名，要求必须为真实名称，将用户登录帐号与用户名称绑定。要求只能输入汉字。

c) 用户密码规范

按照保密规范要求，登录密码强度必须采用组成复杂、不易猜测的口令。输入的密码必须是字母、数字和特殊字符中两者以上的组合且长度不小于10位，特殊字符包括~!@#$%^&*()_+-=。

7 统一安全认证过程

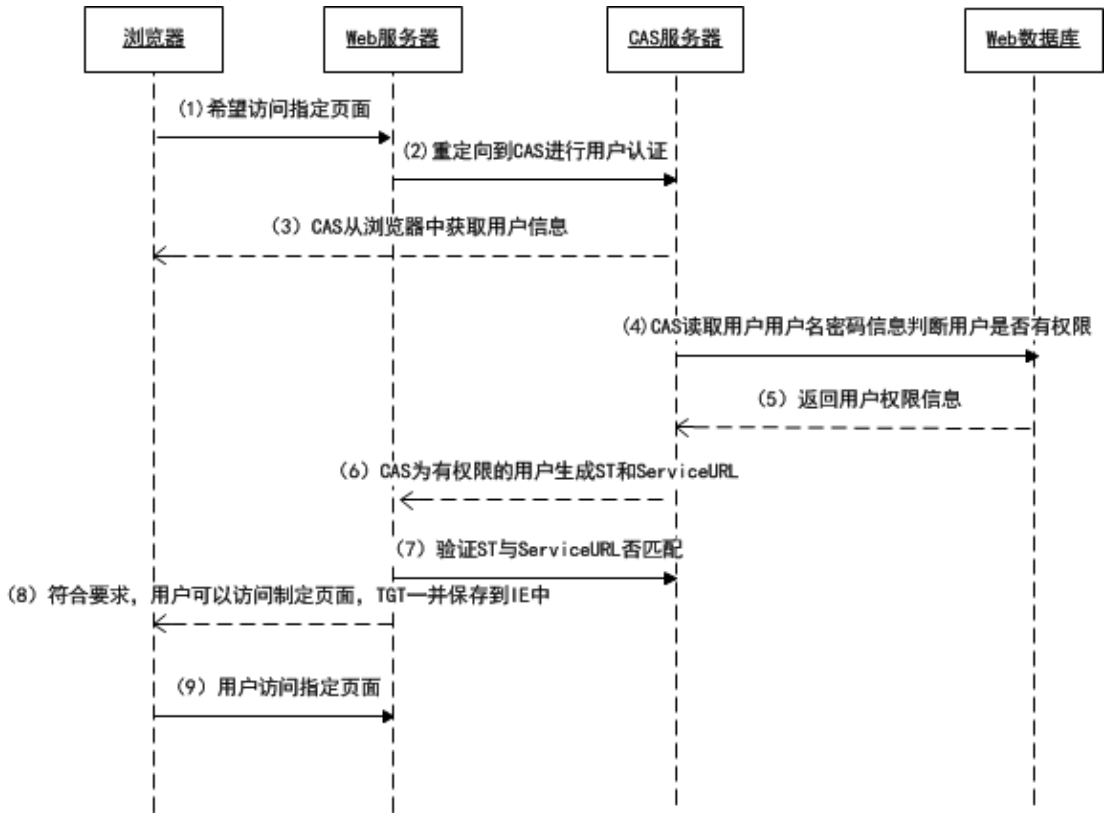

图 1 统一安全认证过程

8 认证内容要求

4A 系统根据《信息系统等级保护安全设计技术要求》（GB/T 25070-2010）基本要求，支持用户帐号/密码和 CA 证书认证两种方式登录系统，用户登录密码按照保密规范要求设置，密码强度必须采用组成复杂、不易猜测的口令。输入的密码必须是字母、数字和特殊字符中两者以上的组合且长度不小于 10 位。

用户帐号在系统中采用唯一性约束，保证无重复帐号存在。

用户名或密码错误导致登录失败时，显示登录错误提示信息与剩余登录次数，但不提示具体错误内容。同时记录用户登录审计日志，在同一帐号登录失败达到 5 次时，锁定该帐号 10 分钟。10 分钟后再次登录失败达到 5 次时，帐号将被锁定，无法登录，必须由管理员进行解锁后才能正常使用。

当用户登录系统后，根据不同的角色与权限显示相应的页面内容。如果在 10 分钟内无任何操作，系统自动退出，必须再次登录后才可使用系统。

用户在系统中的所有操作都将记录详细的操作日志，为审计功能使用。包括

在系统中操作的内容、类型、时间、结果等信息。

当新用户登录业务系统时，如果尚未分配具体权限，该用户应具有最小化基本访问权限。

用户信息发生变更时，状态变为无效的，应不能再访问各系统。用户其它信息发生变化时，不能对已分配的权限产生影响。

附 录 A 统一身份集成说明

1. 系统集成模式

采用数据交换模式的业务系统与4A系统首次对接时，由4A系统向各业务系统提供系统编码，消息中间件地址。

系统编码一般由区域简称+系统简称组成。例如成都市信用评价系统编码为：cd-xypj。

各业务系统以4A系统提供的系统编码为主题，监控消息队列，如果有数据同步请求，4A系统会向该消息队列中发送数据，业务系统接收到数据后，根据数据类型进行相应处理。业务系统在对数据进行业务处理后，向反馈消息队列反馈操作结果。

数据交换示意图

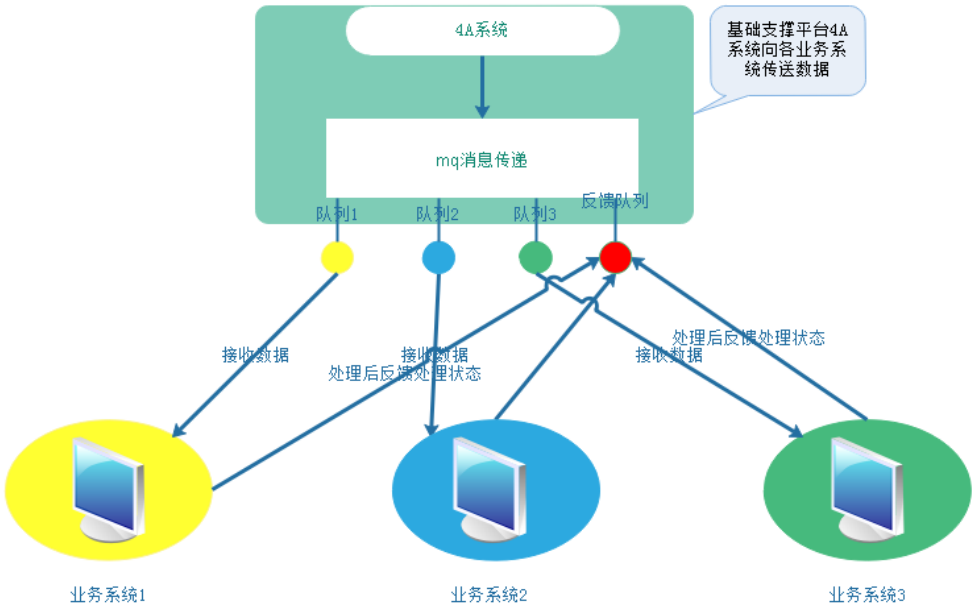

图 2 统一身份数据交换示意图

集成思路

a) 机构映射

对于业务系统已经存在历史数据的情况下，需要提供机构展示接口供4A系统查询，建立映射关系。建立映射关系后业务系统的机构统一由4A系统进行维护管理。

b）机构管理

对于已经与4A系统建立机构映射关系的业务系统，机构的日常维护（增、改操作）将交由4A系统来统一管理。但是各个业务系统需要提供与4A系统进行机构同步的接口。机构的增加和修改操作可以批量进行，所以各个业务系统需要考虑如何批量接收4A系统的数据。

c）用户管理

业务系统在与4A系统机构建立映射的情况下，通过映射机构下的用户帐号与各个业务系统建立一一对应关系。如果同一机构下用户名称出现重复，或者没有匹配上的，则通过人工干预方式匹配。

4A系统通过用户帐号与各个业务系统的用户建立一一对应的关系。各个系统需保证用户帐号的唯一性。

集成内容

各业务系统需要提供以下接口方法的实现，用于与基础支撑平台4A系统的机构、用户的同步：

a）机构映射：分层次查询机构数据的接口；

b）机构同步：批量新增、修改机构、部门数据的接口；

c）用户同步：批量新增、修改用户数据的接口；

集成示例

a）与 4A 系统对接的业务系统可以使用 4A 系统提供的 ConsumerSessionAwareMessageListener.java 获取消息数据。也可通过配置消息监听器。如果使用附带的消息监听器，首先在业务系统中导入 activeMq 的 jar 包。可手动导入 actimeMq 的 jar 包，如图 3 ActiveMQ jar 包清单所示。

图 3 ActiveMQ jar 包清单

也可通过 maven 的 pom.xml 方式导入：

```
<dependency>
                <groupId>org.jasig.cas.client</groupId>
                <artifactId>cas-client-core</artifactId>
                <version>3.5.0</version>
            </dependency>
```

b）在配置文件中配置消息监听器

```
<!-- 消息队列监听者（Queue） -->
    <bean                                                    id="queueMessageListener"
class="com.sinosoft.mq.util.ConsumerSessionAwareMessageListener" />

    <!-- 消息监听容器（Queue） -->
    <bean id="jmsContainer"
class="org.springframework.jms.listener.DefaultMessageListenerContainer">
        <property name="connectionFactory" ref="connectionFactory" />
<!—监听的队列名称 -->
        <property name="destination" ref="zxfw" />
<!—消息处理类引用 -->
        <property name="messageListener" ref="queueMessageListener" />
    </bean>
```

c）在 ConsumerSessionAwareMessageListener.java 中将获取到的数据进行业务处理。

```
/*
*获取消息方法
```

```
*/
@SuppressWarnings({ "unchecked", "rawtypes" })
public void onMessage(Message message, Session session) {
    //接收到的消息
    TextMessage tm = (TextMessage) message;
    try {
        String receiveMessage = tm.getText();
        System.out.println("receiveMessage 接收到消息(加密)： "+receiveMessage);
//对数据进行业务逻辑处理
……
        } catch (JMSException e) {
            e.printStackTrace();
        }
    }
```

接口说明

实现统一身份集成的各业务系统，需实现表 4 机构映射接口接口。

a）机构映射接口（getOrgTree）

表 4 机构映射接口

功能	维护 4A 系统与业务系统机构之间的对应关系。
函数定义	getOrgTree
适用范围	通用
参数	输入参数 ： node：机构 id
返回	Json 格式的组织机构数据

该接口主要作用是用来维护4A系统与业务系统机构之间的对应关系，同时，也是用户同步的前提条件。

此接口需要根据机构的层级关系，分层展示机构信息。各个业务系统每次只提供当前层级的机构信息，4A系统异步加载每一层级的机构数据。

为了统一规范，接口建议命名为getOrgTree。

根据传入的参数信息返回json格式的机构信息，如：

```
{id:'00fd015383e84d7b0027',
text:'测试部门',
orgCode:'AI0000000000',
purpose:'1',
parentDeptId:'000000                    ',
leaf:true,
```

```
expanded:false
},{id:'00fd015383e8940e0035',
text:'信息中心',
orgCode:'AJ0000000000',
purpose:'1',
parentDeptId:'000000',
leaf:true,expanded:false}
```

Json串参数含义见 表 5 机构映射接口返回结果表所示：

表 5 机构映射接口返回结果表

属性名	说明	类型	长度	示例
id	节点 ID	String	20	00fd015383e84d7b0027
orgCode	节点编码	String	12	AI0000000000
text	节点名称	String	60	测试部门
parentDeptId	父节点 ID	String	12	000000
leaf	是否有下级节点	Boolean		true 有下级 / false 无下级
expanded	是否展开	Boolean		false
purpose	机构或部门标志	String	1	1/2（1 为机构，2 为部门）

b）机构同步接口（deptSynchronize）

表 6 机构同步接口

功能	4A 系统与业务系统之间同步机构与部门信息。
函数定义	deptSynchronize
适用范围	通用
参数	具体参数见【机构同步接口输入参数表】
返回	Json 格式的组织机构数据

该接口用于4A系统与业务系统之间同步机构与部门信息。各业务系统以4A系统提供的系统编码为主，监控消息队列，如果有机构或部门数据同步请求，4A系统会向该消息队列中发送数据，业务系统监听消息队列获取数据。业务系统在对数据进行业务处理后，向消息队列中的反馈队列推送消息，反馈同步结果。

系统编码一般由区域简称+系统简称组成。例如成都市信用评价系统编码为：cd-xypj。

机构同步接口主要功能有：

a） 批量新增机构；

b） 批量修改机构；

c）批量删除机构；

各个业务子系统提供的接口需要兼容以上三种操作。在每次接口调用时，4A系统会给各个业务系统传输“操作类型”参数用于判断当前操作类型

当“操作类型”为“addDept”时：为批量新增或者修改机构；各个业务系统通过4A系统传递的机构标识来判断是新增操作或修改操作。

当操作类型为“deleteDept”时：为批量删除机构操作。

为了统一规范，接口建议命名为deptSynchronize。

输入参数

业务系统通过监控消息队列，得到json格式的机构信息，如下所示：


```
{"flag":"true",
"deptInfos":
[
{"id":"00fd015ac59f142f0001",
"deptCode":"22060000D016",
"deptName":"综合技术科",
"invalidFlag":"1",
"deptShortName":"综合技术科",
"regionCode":"220600000000",
"deptId":"",
"parentDeptId":"",
"purpose":"2",
"orgMappingType":"",
"sortNo":"5",
"deptType":"01",
"returnId":"00fd015ac59f142f9991"}
],"operate":"addDept"}
```


表 7 机构同步接口输入参数表

属性名	说明	类型	长度	例子
Id	机构 id	String	20	00fd01549e9549ac005b
deptCode	机构编码	String	20	220600000000
deptName	机构名称	String	100	四川省环境信息中心
deptShortName	机构简称	String	100	综合技术科

regionCode	行政区划编码	String	14	14 位行政区划编码，如：51000000000000
invalidFlag	有效标志	String	1	1/2（1 为有效，2 为无效）
purpose	机构部门标志	String	1	1/2（1 为机构，2 为部门）
sortNo	机构顺序	String	6	100000
deptType	机构类型	Stirng	2	01 综合部门，02 业务部门，03 信息化部门
deptId	接入系统机构 id	String	不定长	00fd013efa753b860029
parentDeptId	接入系统父机构 id	String	不定长	0000000efa753b860001
returnId	反馈 id	String	32	数据处理完成后的反馈结果 ID
operate	操作类型	String		addDept / deleteDept

各业务系统在处理完数据后向消息队列反馈处理结果，如下所示：

```
{
"returnId":"00fd014d3ba73527007d",   反馈数据 id
" appSysCode":"XXXX",                系统编码
"flag":"true",                       操作结果
"orgId": "00fd0100fd01",             业务系统组织 Id
"orgCode":"001"                      业务系统组织编码
}
```

表 8 机构同步接口返回结果表

属性名	说明	类型	长度	例子
returnId	反馈数据 id	String	32	0000000efa753b869991
appSysCode	系统编码	String		YWXT
flag	操作结果	String		true 成功，false 失败
orgId	业务系统组织 Id	String		0000000efa753b8691213
orgCode	业务系统组织编码	String		120000000000

c）用户同步接口（personSynchronize）

表 9 用户同步接口

功能	4A 系统与业务系统之间同步用户信息。
函数定义	personSynchronize

适用范围	通用
参数	具体参数见【用户同步接口输入参数表】
返回	Json 格式的组织机构数据

该接口用于4A系统与业务系统之间同步用户信息。各业务系统以4A系统提供的系统编码为主，保持长连接监控消息队列，如果有数据同步请求，4A系统会向该消息队列中发送数据。业务系统在对数据进行业务处理后，向消息队列中的反馈队列推送消息，反馈同步结果。

用户同步接口实现的主要功能有：

a） 批量新增用户；

b） 批量修改用户；

c）批量删除用户；

各个业务子系统提供的该接口需要兼容以上三种操作。

注意：为了准确定位用户信息，当且仅当组织机构同步以后，该机构中的用户才能进行同步操作。

为了统一规范，接口建议命名为personSynchronize。

业务系统通过监控消息队列，得到json格式的用户信息，如下所示：


```
{
"flag":"true",
"userInfos":
[{
"innerCode":"350000000000ba78be16ce7945beb1a9",
"account":"zhangsan",
"fullName":"张三",
"userStatus":"1",
"leaderFlag":"2",
"deptType":"02",
"deptId":"000000",
"userDeptId":"00fd01549ea0a2f9055f",
"userDeptName":"信息中心",
"userOrgId":"350000                    ",
"userOrgName":"四川省环保厅",
"userType":"1",
"userRankCode": "11",
"userRank":"科员",
```

```
"userTypeCode":"1",
"position":"副主任，办事员，工作人员",
"positionCode":"10,11,12",
"majorPosition":"0",
"sex":"1",
"md5Pwd":"9b868260dcfa1b12fdea2cfd48a281f3",
"office":"1306",
"regionCode":"51010000000000000000",
"regionName":"成都市",
"sortNo":"123456789",
"email":"123456789@qq.com",
"returnId":"00fd014d3ba73527007d "
}],
"operate":"addUser"
}
```


表 10 用户同步接口输入参数表

属性名	说明	类型	字长	例子
innerCode	32 位码	String	32	00000000000062d1b2e0c6384ad18c70
account	账号	String	100	Zhangsan
fullName	用户名字全称	String	30	张三
userStatus	用户状态	String	1	1 有效，2 无效。无效帐号不能进入或使用系统。
leaderFlag	是否领导	String	1	2 非领导，1 领导
deptType	用户所在部门类型	String	30	01 综合部门，02 业务部门，03 信息化部门
deptId	该用户所在的部门的 id，此 id 为接入子系统的主键 id 和机构映射提供的树节点 id 一致	String		用户所在部门 ID，此 ID 不是 4A 系统中的部门 ID，而是对接的业务系统中的部门 ID，在机构映射接口中取得，例如：00fd0154f5139f7e0004
userDeptId	该用户所在的部门的 id，此	String	20	4A 系统中用户所在部门的 id,如果对接的业务系统无单独的组织机构部门信息

	id为4A系统的部门id			表时，可以将此信息项作为用户的部门id
userDeptName	该用户所在的部门的名称，此名称为4A系统的部门名称	String	60	4A系统中用户所在部门的名称，如果对接的业务系统无单独的组织机构部门信息表时，可以将此信息项作为用户的部门名称，例如：信息中心
userOrgId	该用户所在的机构的id，此id为4A系统的机构id	String	20	4A系统中用户所在机构的id,如果对接的业务系统无单独的组织机构信息表时，可以将此信息项作为用户的机构id。一个机构中包含多个部门
userOrgName	该用户所在的机构的名称，此名称为4A系统的机构名称	String	60	4A系统中用户所在机构的名称，如果对接的业务系统无单独的组织机构信息表时，可以将此信息项作为用户的机构名称，例如：四川省环保厅
position	职务名称	String	50	用户的主职，副职，兼职。以逗号分隔。例如：常委，主任，书记，
positionCode	职务编码	String	15	用户的主职，副职，兼职职务编码，以逗号分隔。例如：01,02,03
majorPosition	岗位标识	String	1	0主岗位/1兼职岗位。用于一人在多个部门下任职的情况，标记主职部门或兼职部门。各系统需支持一具人在多个部门下任职的情况
userRank	职级	String	10	
userType	人员类别	String	20	
Sex	性别	String	10	1男/2女
md5Pwd	帐户密码	String	64	Md5加密后的密码字符串
office	办公室	String	10	1306
regionCode	行政区域编码	String	20	51010000000000000000
regionName	行政区域名称	String	100	成都市

sortNo	人员顺序	String	9	100000000
email	用户邮箱	String	100	12345@qq.com
returnId	反馈 Id	String	32	数据处理完成后的反馈结果 ID
operate	操作类型	String		addUser / deleteUser

业务系统在处理完数据后向消息队列反馈处理结果，如下所示：

```
{
"returnId":"00fd014d3ba73527007d",   反馈数据 id
" appSysCode":"XXXX",                系统编码
"flag":"true"                        操作结果
}
```

表 11 用户同步接口返回结果表

属性名	说明	类型	字长	例子
returnId	反馈数据 id	String	32	0000000efa753b869991
appSysCode	系统编码	String		YWXT
Flag	操作结果	String		true 成功，false 失败

附 录 B 认证集成配置说明

1. JDK 环境准备

凡是需要与基础支撑平台 4A 系统实现单点登录对接的业务系统需要将各自系统的 JDK 升级到 1.6 及其以上版本，从而能够与 cas 客户端文件进行无缝集成。

2. JAR 包的准备

需要与基础支撑平台 4A 系统做统一认证的业务系统首先需要在各自的项目中引入以下 jar 文件。这些 jar 包是用来与 cas 的服务端进行通信的。

表 12 单点登录必要 jar 包表

序号	Jar 包名称	描述
1	cas-client-core-3.3.3.jar	CAS 客户端的核心包
2	cas-client-integration-atlassian-3.3.3.jar	CAS 客户端集成包
3	cas-client-support-distributed-ehcache-3.3.3.jar	CAS 客户端数据缓存包
4	cas-client-support-distributed-memcached-3.3.3.jar	CAS 客户端数据缓存包

3. web.xml 中需要添加的配置信息

如果业务系统需要让基础支撑平台 4A 系统做统一认证，从而实现单点登录的功能，那么需要在各业务系统的 web.xml 文件中的合适位置添加如下配置。

```
<filter>
    <filter-name>CAS Single Sign Out Filter</filter-name>
    <filter-class>org.jasig.cas.client.session.SingleSignOutFilter</filter-class>
  </filter>
  <filter>
    <filter-name>CASFilter</filter-name>
<filter-class>org.jasig.cas.client.authentication.AuthenticationFilter</filter-class>
    <init-param>
      <param-name>casServerLoginUrl</param-name>
      <param-value>统一认证服务器 IP 地址</param-value>
    </init-param>
    <init-param>
      <param-name>serverName</param-name>
      <param-value>业务系统 IP 地址</param-value>
```

```
    </init-param>
    <init-param>
        <param-name>encoding</param-name>
        <param-value>UTF-8</param-value>
    </init-param>
  </filter>
  <filter>
    <filter-name>CAS Validation Filter</filter-name>
    <filter-class>
    org.jasig.cas.client.validation.Cas20ProxyReceivingTicketValidationFilter</filter-class>
    <init-param>
      <param-name>casServerUrlPrefix</param-name>
      <param-value>统一认证服务器 IP 地址</param-value>
    </init-param>
    <init-param>
      <param-name>serverName</param-name>
      <param-value>业务系统 IP 地址</param-value>
    </init-param>
    <init-param>
        <param-name>acceptAnyProxy</param-name>
        <param-value>true</param-value>
    </init-param>
  </filter>
  <filter>
<filter-name>AutoSetUserAdapterFilter</filter-name>
<filter-class>com.sinosoft.scjw.util.AutoSetUserAdapterFilter</filter-class>
  </filter>
  <filter-mapping>
    <filter-name>encodingFilter</filter-name>
    <url-pattern>/*</url-pattern>
    <dispatcher>REQUEST</dispatcher>
    <dispatcher>FORWARD</dispatcher>
  </filter-mapping>
  <filter-mapping>
    <filter-name>CAS Single Sign Out Filter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
  <filter-mapping>
    <filter-name>CAS Validation Filter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
  <filter-mapping>
    <filter-name>CASFilter</filter-name>
    <url-pattern>/*</url-pattern>
```

```
</filter-mapping>
<filter-mapping>
    <filter-name>AutoSetUserAdapterFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

4. 参数说明

a）参数 casServerLoginUrl：该参数是用来配置单点登录的服务地址，根据实际情况做相应修改。

b）参数 casServerUrlPrefix ：该参数是用来配置单点登录的服务地址，根据实际情况做相应修改。

c）参数 serverName ：该参数是用来配置本地服务的地址，根据实际情况做相应修改。

d）参数 acceptAnyProxy ： 该参数是用来设置是否开启代理模式，其值应设置为 true。

e）统一认证服务器 IP 地址：统一认证服务器的地址，对接时由 4A 系统提供。

f）业务系统 IP 地址：需要接入统一认证的业务系统 IP 地址。

g）其余参数配置不需要做任何修改，按照本例给出的配置放到相应位置即可。

5. 过滤器配置

获取用户信息的过滤器

为实现单点登录的功能，各个业务系统首先需要与基础支撑平台 4A 系统实现用户统一。即各业务系统的用户与基础支撑平台 4A 系统的用户存在一定的对应关系。当用户登录平台后，单点登录服务器会将用户信息存放在 Session 中，各个业务系统需提供一个过滤器从 session 中获取用户数据，从而控制用户的角色权限等信息。

本例中给出的过滤器为 AutoSetUserAdapterFilter，该过滤器主要功能是从 session 中获取用户信息。该类的具体内容根据各个业务系统自身情况编写，但是获取用户信息的来源是统一的。具体的代码如下：

```
// _const_cas_assertion_是 CAS 中存放登录用户名的 session 标志
```

```
Object object = httpRequest.getSession().getAttribute(
                    "_const_cas_assertion_");
if (object != null) {
            Assertion assertion = (Assertion) object;
          //获取登录用户帐号
            String loginName = assertion.getPrincipal().getName();
}
```

进行编码转换的过滤器

进行编码转换的目的是为了防止各个系统在传输数据的过程中出现中文乱码问题。

在使用的 Spring 的情况下，编码转换和过滤都是统一的，即本例给出的 encodingFilter 参数。在不使用 Spring 情况下，各系统可以自己编写转码的过滤器并配置的相应的位置即可。

附 录 C 组织机构编码

组织机构参考《GB/T 2260-2019　中华人民共和国行政区划代码》使用，可参照表 13 组织机构及编码表。

表 13 组织机构及编码表

序号	组织机构名称	编码
1	四川省	51000000000000000000
2	成都市	51010000000000000000
3	锦江区	51010400000000000000
4	青羊区	51010500000000000000
5	金牛区	51010600000000000000
6	武侯区	51010700000000000000
7	成华区	51010800000000000000
8	天府新区	51011000000000000000
9	高新区	51011100000000000000
10	龙泉驿区	51011200000000000000
11	青白江区	51011300000000000000
12	新都区	51011400000000000000
13	温江区	51011500000000000000
14	金堂县	51012100000000000000
15	双流区	51012200000000000000
16	郫县	51012400000000000000
17	大邑县	51012900000000000000
18	蒲江县	51013100000000000000
19	新津县	51013200000000000000
20	都江堰市	51018100000000000000
21	彭州市	51018200000000000000

序号	组织机构名称	编码
22	邛崃市	51018300000000000000
23	崇州市	51018400000000000000
24	自贡市	51030000000000000000
25	自流井区	51030200000000000000
26	贡井区	51030300000000000000
27	大安区	51030400000000000000
28	沿滩区	51031100000000000000
29	荣县	51032100000000000000
30	富顺县	51032200000000000000
31	攀枝花市	51040000000000000000
32	东区	51040200000000000000
33	西区	51040300000000000000
34	仁和区	51041100000000000000
35	米易县	51042100000000000000
36	盐边县	51042200000000000000
37	泸州市	51050000000000000000
38	江阳区	51050200000000000000
39	纳溪区	51050300000000000000
40	龙马潭区	51050400000000000000
41	泸县	51052100000000000000
42	合江县	51052200000000000000
43	叙永县	51052400000000000000
44	古蔺县	51052500000000000000
45	德阳市	51060000000000000000

序号	组织机构名称	编码
46	旌阳区	51060300000000000000
47	中江县	51062300000000000000
48	罗江县	51062600000000000000
49	广汉市	51068100000000000000
50	什邡市	51068200000000000000
51	绵竹市	51068300000000000000
52	经开区	51068400000000000000
53	绵阳市	51070000000000000000
54	涪城区	51070300000000000000
55	游仙区	51070400000000000000
56	安州区	51070500000000000000
57	三台县	51072200000000000000
58	盐亭县	51072300000000000000
59	安县	51072400000000000000
60	梓潼县	51072500000000000000
61	北川羌族自治县	51072600000000000000
62	平武县	51072700000000000000
63	江油市	51078100000000000000
64	科创区	51078200000000000000
65	广元市	51080000000000000000
66	昭化区	51080100000000000000
67	利州区	51080200000000000000
68	元坝区	51081100000000000000
69	朝天区	51081200000000000000

序号	组织机构名称	编码
70	旺苍县	51082100000000000000
71	青川县	51082200000000000000
72	剑阁县	51082300000000000000
73	苍溪县	51082400000000000000
74	遂宁市	51090000000000000000
75	船山区	51090300000000000000
76	安居区	51090400000000000000
77	蓬溪县	51092100000000000000
78	射洪县	51092200000000000000
79	大英县	51092300000000000000
80	内江市	51100000000000000000
81	市中区	51100200000000000000
82	东兴区	51101100000000000000
83	威远县	51102400000000000000
84	资中县	51102500000000000000
85	隆昌县	51102800000000000000
86	乐山市	51110000000000000000
87	市中区	51110200000000000000
88	沙湾区	51111100000000000000
89	五通桥区	51111200000000000000
90	金口河区	51111300000000000000
91	犍为县	51112300000000000000
92	井研县	51112400000000000000
93	夹江县	51112600000000000000

序号	组织机构名称	编码
94	沐川县	511129000000000000000
95	峨边彝族自治县	511132000000000000000
96	马边彝族自治县	511133000000000000000
97	峨眉山市	511181000000000000000
98	乐山高新区	511182000000000000000
99	南充市	511300000000000000000
100	顺庆区	511302000000000000000
101	高坪区	511303000000000000000
102	嘉陵区	511304000000000000000
103	南部县	511321000000000000000
104	营山县	511322000000000000000
105	蓬安县	511323000000000000000
106	仪陇县	511324000000000000000
107	西充县	511325000000000000000
108	阆中市	511381000000000000000
109	眉山市	511400000000000000000
110	东坡区	511402000000000000000
111	彭山区	511403000000000000000
112	仁寿县	511421000000000000000
113	彭山县	511422000000000000000
114	洪雅县	511423000000000000000
115	丹棱县	511424000000000000000
116	青神县	511425000000000000000
117	宜宾市	511500000000000000000

序号	组织机构名称	编码
118	翠屏区	511502000000000000
119	南溪区	511503000000000000
120	宜宾县	511521000000000000
121	南溪县	511522000000000000
122	江安县	511523000000000000
123	长宁县	511524000000000000
124	高县	511525000000000000
125	珙县	511526000000000000
126	筠连县	511527000000000000
127	兴文县	511528000000000000
128	屏山县	511529000000000000
129	临港区	511530000000000000
130	广安市	511600000000000000
131	广安区	511602000000000000
132	前锋区	511603000000000000
133	岳池县	511621000000000000
134	武胜县	511622000000000000
135	邻水县	511623000000000000
136	华蓥市	511681000000000000
137	达州市	511700000000000000
138	通川区	511702000000000000
139	达川区	511703000000000000
140	达县	511721000000000000
141	宣汉县	511722000000000000

序号	组织机构名称	编码
142	开江县	511723000000000000000
143	大竹县	511724000000000000000
144	渠县	511725000000000000000
145	万源市	511781000000000000000
146	雅安市	511800000000000000000
147	雨城区	511802000000000000000
148	名山区	511803000000000000000
149	名山县	511821000000000000000
150	荥经县	511822000000000000000
151	汉源县	511823000000000000000
152	石棉县	511824000000000000000
153	天全县	511825000000000000000
154	芦山县	511826000000000000000
155	宝兴县	511827000000000000000
156	巴中市	511900000000000000000
157	巴州区	511902000000000000000
158	恩阳区	511903000000000000000
159	通江县	511921000000000000000
160	南江县	511922000000000000000
161	平昌县	511923000000000000000
162	资阳市	512000000000000000000
163	雁江区	512002000000000000000
164	安岳县	512021000000000000000
165	乐至县	512022000000000000000

序号	组织机构名称	编码
166	简阳市	512081000000000000000
167	阿坝藏族羌族自治州	513200000000000000000
168	马尔康市	513201000000000000000
169	汶川县	513221000000000000000
170	理县	513222000000000000000
171	茂县	513223000000000000000
172	松潘县	513224000000000000000
173	九寨沟县	513225000000000000000
174	金川县	513226000000000000000
175	小金县	513227000000000000000
176	黑水县	513228000000000000000
177	壤塘县	513230000000000000000
178	阿坝县	513231000000000000000
179	若尔盖县	513232000000000000000
180	红原县	513233000000000000000
181	甘孜藏族自治州	513300000000000000000
182	康定市	513301000000000000000
183	康定县	513321000000000000000
184	泸定县	513322000000000000000
185	丹巴县	513323000000000000000
186	九龙县	513324000000000000000
187	雅江县	513325000000000000000
188	道孚县	513326000000000000000
189	炉霍县	513327000000000000000

序号	组织机构名称	编码
190	甘孜县	513328000000000000000
191	新龙县	513329000000000000000
192	德格县	513330000000000000000
193	白玉县	513331000000000000000
194	石渠县	513332000000000000000
195	色达县	513333000000000000000
196	理塘县	513334000000000000000
197	巴塘县	513335000000000000000
198	乡城县	513336000000000000000
199	稻城县	513337000000000000000
200	得荣县	513338000000000000000
201	凉山彝族自治州	513400000000000000000
202	西昌市	513401000000000000000
203	木里藏族自治县	513422000000000000000
204	盐源县	513423000000000000000
205	德昌县	513424000000000000000
206	会理县	513425000000000000000
207	会东县	513426000000000000000
208	宁南县	513427000000000000000
209	普格县	513428000000000000000
210	布拖县	513429000000000000000
211	金阳县	513430000000000000000
212	昭觉县	513431000000000000000
213	喜德县	513432000000000000000

序号	组织机构名称	编码
214	冕宁县	513433000000000000000
215	越西县	513434000000000000000
216	甘洛县	513435000000000000000
217	美姑县	513436000000000000000
218	雷波县	513437000000000000000