国家虚拟仿真实验教学项目技术接口规范

（2019版）

# 1 前言

## 1.1 编写说明

服务“国家虚拟仿真实验教学项目共享平台（实验空间）”（以下简称：实验空间）的用户与学校实验教学项目的用户管理系统之间的身份自动识别，避免二次登录。识别后的用户在学校实验教学项目上的实验操作状态和产生的实验结果数据，将自动回传到国家虚拟仿真实验教学项目共享平台，支撑数据统计和监测。

数据接口方式分两种，分别是： **用户验证令牌方式**和**验证接口方式**。基于C/S架构的应用**只能选择验证接口方式**。

本文中所有Host站点统一为：<http://www.ilab-x.com>

## 1.2 服务对象

项目经理

技术开发人员

应用测试人员

## 1.3 业务实现示意图



# 2 用户身份识别规范



当用户登录“实验空间”后点击【我要做实验】时（如下图），“实验空间”会以参数形式提供Token。

链接组成样例：实验平台的URL?token, 例如：http://life.scnu.edu.cn/biology/vrlab/co2/?token=AAABZKECn4ABAAAAAAABhqM%3D.fKf3J5DN6Ym0Fo3I5CJYdzQMR0iwEz7QnQIit2Mfl6v03jpEJ%2Fr4FMRFqh5kN4yw.tqIPoyvkHe2MGOXMimE9O554Lo6AbBCQkZlsqQI4XRQ%3D

实验空间用户验证时使用XJWT标准，此标准基于JSON Web Token (JWT)开发。XJWT包含三个参数：**header,** **payload**, **signature**，因此生成token就要先获得这三个参数。

## 2.1 用户验证令牌token

token的组成结构：based64(raw header) +'.' + base64(raw payload) +'.' +base64(raw signature)

token组成参数header, payload, signature说明如下：

### 2.1.1 header

组成结构：[expiry:long][type:byte][issuer id:long]

参数说明：

|  |  |
| --- | --- |
| 项目 | 说明 |
| expiry | 过期时间，UTC以毫秒为单位，二进制8byte，Big endian。 |
| type | 类别，值为二进制，必填。1- JSON, 2-SYS. 0-保留 |
| Issuer id | 由“实验空间”分配给各实验平台的唯一编号，二进制8 byte，Big endian。 |

### 2.1.2 payload

payload 是64 bytes的整数倍。其组成结构：aes256(random long + body +aes padding, aes key)。其中：aes256是AES256加密算法；random long是随机的8 byte数字；aes padding是自定义的字符串，为补足64 bytes的整数倍；aes key 由“实验空间”生成分配给各实验教学项目。body为UTF8编码的JSON格式字符串。

“实验空间”发送给各实验平台的验证令牌（token）格式如下表：

|  |  |
| --- | --- |
| 项目 | 说明 |
| id | 用户id。 |
| un | 用户username |
| dis | 用户姓名显示 |

### 2.1.3 signature

组成结构：base64(HmacSHA256(based64(raw header) +'.' + base64(raw payload), secret key))

其中：raw header是上述中生成的header；raw payload是上述中生成的payload；secret key是生成aes key的密码，由“实验空间”提供。

4.验证与解密。

使用base64解码signature，通过secret key验证, 如果验证失败，则token失效。使用base64解码header，将得到的过期时间（expiry）和当前时间进行比较，如果已过期，则token失效；如果没有提供header type，则token失效；使用base64解码，并使用aes key进行解密，得到的数据前8 byte和aes padding数据将被丢弃，返回剩余的数据json。各实验教学项目取得用户数据后，可自行进行保存。

验证返回码及说明：

|  |  |
| --- | --- |
| code | 说明 |
| 0 | 验证成功 |
| 26 | token失效 |
| 其他值 | 系统错误 |

## 2.2 验证接口开发规范

当用户直接访问各实验教学项目时、token失效时、用户处于未登录状态访问各实验教学项目时、或者实验教学项目采用C/S架构模式，则第三方接入端可按照给定的登录接口形式，开发可使用“实验空间”用户名及密码获取用户基本信息的接口。

需要发送数据到http://www.ilab-x.com/sys/api/user/validate服务进行登录。

接口名称：[http://www.ilab-x.com/sys/api/user/validate](http://ilab-x.com/sys/api/user/validate)。

调用方法：GET。

详细说明见下表：

|  |  |  |
| --- | --- | --- |
| 参数 | 说明 | 参考值 |
| username | 用户名 | test |
| password | 加密后密码：password = sha256(nonce+sha256(password). toUpperCase() + cnonce). toUpperCase()。sha256是SHA256加密算法 | 2760F0245D3C03E7ABDA1CCA310187E2E33EEB886FDE0FCD5C827E971AED44D7 |
| nonce | 安全验证随机数：自建函数，随机生成16位字符串。允许字符：['0','1','2','3','4','5','6','7','8','9','A','B','C','D','E','F'] | 0F2785E6ED1B59AC |
| cnonce | 二次安全验证随机数：自建函数，随机生成16位字符串。允许字符：['0','1','2','3','4','5','6','7','8','9','A','B','C','D','E','F'] | F5A981C203030722 |

调用示例：

http://www.ilab-x.com/sys/api/user/validate?username=test&password=2760F0245D3C03E7ABDA1CCA310187E2E33EEB886FDE0FCD5C827E971AED44D7&nonce=0F2785E6ED1B59AC&cnonce=F5A981C203030722。

返回结果示例：

{ "code":0,"username":"test","name":"测试用户"}

返回参数说明：

|  |  |
| --- | --- |
| code | 说明 |
| 0 | 调用成功 |
| 3 | 发送的参数缺失（username、password、nonce、cnonce） |
| 4 | 密码（password）错误 |
| 5 | 用户名（username）错误 |
| 其他值 | 系统错误或非法操作 |

# 3 实验结果数据回传接口

回传数据接口是指：“实验空间”用户完成实验教学项目后，所产生的实验结果数据。如果有实验报告，则先调用附件上传接口，然后再将这些数据和用户信息一起通过回传数据接口同步至“实验空间”。

## 3.1 实验数据回传字典

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 字段名称 | 类型 | 备注 |
| 1 | username | 用户名 | String |  |
| 2 | projectTitle | 实验名称 | String |  |
| 3 | childProjectTitle | 子实验名称 | String | 可选，适用于一个实验中包含多个子实验项目 |
| 4 | status | 实验结果 | Int | 1：完成；2：未完成 |
| 5 | score | 实验成绩 | Int | 0 ~100，百分制 |
| 6 | startDate | 实验开始时间 | Time | 13位时间戳 |
| 7 | endDate | 实验结束时间 | Time | 13位时间戳 |
| 8 | timeUsed | 实验用时 | Int | 分钟 |
| 9 | issuerId | 接入平台编号 | String | 由“实验空间”分配给实验教学项目的编号 |
| 10 | attachmentId | 实验报告（PDF、DOC等） | Int | 通过附件上传服务获取到的附件ID |

## 3.2 附件上传服务

接口名称：http://www.ilab-x.com/project/log/attachment/upload。

调用方法：POST

详细说明见下表：

|  |  |
| --- | --- |
| 项目 | 说明 |
| 文件上传方法 | chunk |
| 发送URL示例 | http://www.ilab-x.com/project/log/attachment/upload?totalChunks=" + totalChunks + "&current=" + currentChunk + "&filename=" + filename + "&chunkSize=" + size +"&xjwt="+ xjwt参数说明：totalChunks：总分片数；current：当前上传的分片数；filename：上传文件的名称，需要带文件扩展名，如：实验报告.pdf；chunkSize：分片大小，一般设置为1024\*1024；xjwt：使用type=2 body="SYS"生成的XJWT。filename及xjwt在发送到接口时，需要做URL encode。当分片大于1时，第一次上传成功后会返回cookie ，在之后的上传中http cookie中需要设置返回的cookie。 |
| Request Payload | 上传文件的分片内容 |
| 调用成功示例 | {"code":0, “id”:12}其中id为附件在服务器上的id。在上传成绩时，返回ID。 |
| 调用失败示例 | {"code":其他值,“系统错误” }，常见错误Not logged in是因为xjwt解码失败。 |

## 3.3 实验结果加密数据格式示例

{

“username”:”用户名”,

” projectTitle”:”项目名称”,

” childProjectTitle”:”子项目名称”,

” status”:1,

”score”:80,

”startDate”: 1522646936000,

”endDate”:” 1522647936000”,

”timeUsed”: 15,

”issuerId”: ” PK1502”,

”attachmentId”:12

}

## 3.4 数据发送接口地址

接口名称：http://www.ilab-x.com/project/log/upload。

调用方法：POST。

详细说明见下表：

|  |  |
| --- | --- |
| 项目 | 说明 |
| 发送URL示例 | http://www.ilab-x.com/project/log/upload?xjwt="+ xjwt参数说明：xjwt：使用type=2 body=参考《**[3.3实验结果加密数据格式示例](#3.3 实验结果加密数据格式示例)**》组合的JSON字符串，生成的XJWT。xjwt在发送到接口时，需要做URL encode。 |
| Request Payload | 空 |
| 调用成功示例 | {"code":0,”msg”:”no error”}或{"code":0,”id”:12 }; |
| 调用失败示例 | {"code":其他值,“系统错误” } |

返回参数说明：

|  |  |
| --- | --- |
| code | 说明 |
| 0 | 调用成功 |
| 2 | 解密失败，返回invalid token或者msg为加密的内容或者其他的错误说明。 |
| 3 | xjwt参数缺失 |
| 4 | 未分配的issueId |
| 5 | 加密的数据格式错误，请仔细对照示例进行修改 |
| 6 | 返回实验用户名错误，请检查username字段，必须为“实验空间”发送给实验平台的用户名 |
| 其他值 | 系统错误或非法操作 |

# 4 实验操作状态回传接口

此接口适用于用户从“实验空间”平台进入第三方实验平台开始做实验教学项目情况。当用户有操作时，第三方平台可调用此接口，完成实验操作状态的数据回传。

## 4.1实验操作状态回传数据字典

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 字段名称 | 类型 | 备注 |
| 1 | username | 用户名 | String |  |
| 2 | issuerId | 接入平台编号 | String | 由“实验空间”分配给各实验平台的唯一编号 |

## 4.2 数据发送接口地址

接口名称：http://www.ilab-x.com/third/api/test/result/upload。

调用方法：POST。具体情况见下表中案例说明。

|  |  |
| --- | --- |
| 项目 | 说明 |
| 发送URL示例 | http://www.ilab-x.com/ third/api/test/result/upload?xjwt="+ xjwt参数说明：xjwt：使用type=2 body=参考《[**3.3实验操作状态加密数据格式示例**](#3.3 实验结果加密数据格式示例)》组合的JSON字符串，生成的XJWT。xjwt在发送到接口时，需要做URL encode。 |
| Request Payload | 空 |
| 调用成功示例 | {"code":0,”msg”:”no error”}或{"code":0,”id”:12}； |
| 调用失败示例 | {"code":其他值,“系统错误” } |

返回参数说明：

|  |  |
| --- | --- |
| code | 说明 |
| 0 | 调用成功 |
| 3 | xjwt参数缺失 |
| 4 | 未分配的issueId |
| 5 | 加密的数据格式错误或xjwt解码失败，请仔细对照示例进行修改 |
| 6 | 返回实验用户名错误，请检查username字段，必须为“实验空间”发送给实验平台的用户名 |
| 7 | 此用户已经增加过此实验状态 |
| 其他值 | 系统错误或非法操作 |

## 4.3实验操作状态加密数据格式示例

{

“username”:”用户名”,

”issuerId”: ” PK1502”,

}

# 5 Demo与测试平台

Demo下载地址：

<https://github.com/haohe/xpe_doc/blob/master/manual/jwt.md>

JAVA版源码：

https://github.com/softtouchit/xjwt/tree/master/src/com/softtouchit/jwt

如需用测试平台进行调试，请联系“实验空间”技术负责人员（010-58582325）获取测试平台地址。