统一认证平台与业务系统交互说明

目 录

[1 概述 1](#_Toc467163458)

[2 统一认证平台职责 2](#_Toc467163459)

[3 业务系统与统一认证平台Token验证 3](#_Toc467163460)

[3.1 交互方式 3](#_Toc467163461)

[3.2 登录以及Token验证流程 4](#_Toc467163462)

[4 业务系统菜单和按钮权限验证 7](#_Toc467163463)

[4.1 菜单权限验证流程 7](#_Toc467163464)

[4.2 按钮权限验证流程 8](#_Toc467163465)

[5 附件 10](#_Toc467163466)

[6 图表目录 11](#_Toc467163467)

# 概述

为了各业务系统更好的了解业务系统与统一认证平台之间的交互流程，本文档进行如下方面的说明：

1. 统一认证平台功能和职责说明
2. 业务系统与统一认证平台Token验证交互流程
3. 业务系统菜单(包括按钮)权限验证说明

# 统一认证平台职责

统一认证平台主要职责如下:

1. 登录验证以及Token管理
2. 菜单(包括页面按钮)权限管理
3. 服务权限管理(主要是针对外部接口)
4. 字典维护
5. 操作日志管理

统一认证平台的意义在于：

1. 数据共享

将多个业务系统(实验室，现勘等)的用户数据(账户，用户信息，组织机构等)以及

字典信息放在统一认证平台，便于数据共享，最典型的就是同一用户可以登录多个

业务系统。

1. 统一权限管理

统一登录(登录和Token管理)，统一权限管理(菜单权限和服务权限管理)

1. 统一操作日志管理

将操作日志统一放在统一认证平台进行管理

# 业务系统与统一认证平台Token验证

## 交互方式



1. 业务系统与统一认证平台交互方式

**说明：**

1. 各业务系统(现勘，实验室等)的**客户端登录或权限验证都不能直接通过访问UAOP**的rest服务进行，而是通过自身服务访问UAOP来进行。

**注:实验室当前版本有些服务时直接访问UAOP的，后续应该按照途中方式统一下改下。**

1. 各业务系统的客户端与自身后台服务之间，通过rest接口进行通信。
2. 各业务系统后台服务与UAOP之间，通过rmi接口进行通信。

## 登录以及Token验证流程

下面以现勘为例，说明下登录流程



1. 登录以及Token验证时序图

**说明：**

1. **用户登录流程：**
2. 用户在现勘客户端输入账号信息进行登陆
3. 现勘服务调用统一认证平台进行登录验证
4. 统一认证平台验证登录账号信息

通过，则生成新的Token信息保存到数据库/Redis

不通过，则返回账号非法

1. 统一认证平台验证结果(登录失败或登录成功后的Token对象)给现勘后台服务

注: 返回的Token对象包含Token串，到期时间(或者有效时长)，用户信息。

1. 若登录通过，现勘后台缓存统一认证平台缓存的Token对象。
2. 现勘后台将登录结果(登录失败或登录成功后的Token对象)返回给现勘客户端。
3. **数据请求访问(带Token)流程:**
4. 现勘客户端登陆成功后，每个rest数据请求，都应该带上Token信息向现勘后台服务发起请求。
5. 现勘服务rest请求拦截器，读取客户端rest请求头部的token信息，根据本地缓存的Token对象，进行Token验证：

若当前缓存的Token未超时：Token验证通过，则直接调用业务方法，返回请求结果给客户端；Token验证不通过，则直接返回客户端Token非法。

若当前缓存的Token超时，则向统一认证平台发起Token检测。

1. 缓存的Token超时检测流程:

(3.1) 现勘服务向统一认证平台发起Token检测

(3.2) 统一认证平台检测当前数据库/Redis中的Token是否到期：

如果未到期，则将Token过期时间向后推延2个小时(具体时长以配置超时间为准)，更新数据库/Redis的Token记录，并且将新的到期时间返回给现勘服务。

如果到期，则直接返回Token已失效。

(3.3). 统一认证平台将Token超时检测结果返回给现勘服务

(3.4). 若现勘服务收到的是新的Token超时时间，则更新本地缓存的Token

1. 现勘服务向前台返回请求结果：Token有效时，返回具体业务方法结果数据；Token失效时，返回Token非法。

**根据上面的流程，下面几点需要注意下：**

1. 现勘(业务系统)服务端缓存的Token超时时长必须比统一认证平台中定义的Token超时时间短，比如统一认证平台定义时长为2小时，则现勘缓存Token超时时长为1.5小时。
2. 业务系统注销只是清空客户端cookie，不会调用后台服务，后台的token还是有效的，其他业务系统不受影响。
3. 登录一次，在同一认证平台就会生成一个新的Token。
4. 同一用户从不同客户端登录，UAOP都是新生成token，不会有冲突。
5. 当从一个业务系统跳转到另一个业务系统时，要将当前业务系统的token传给目标业务系统，由目标业务系统调用UAOP接口验证是否合法，合法则允许进入。

# 业务系统菜单和按钮权限验证

## 菜单权限验证流程



1. 菜单权限验证时序图

**说明：**

1. 现勘客户端向现勘服务请求获取有权限的菜单树
2. 现勘服务检查本地缓存是否已经有该用户权限：

如果有，直接返回缓存的菜单树。

如果没有，调用统一认证平台获取该用户所拥有的所有权限，并缓存在本地，另外根据权限点组织菜单树，缓存在本地并返回给前台。

1. 统一认证平台收到用户权限变更操作时，以消息形式通知现勘服务，现勘服务收到消息后，清空该变更用户对应的权限数据缓存。

## 按钮权限验证流程



1. 按钮权限验证时序图

**说明：**

1. 现勘客户端页面加载时，将要鉴权的按钮权限点ID发送给现勘服务进行验证。
2. 现勘服务检查本地缓存是否已经有该用户权限：

如果有，直接判断请求的权限点ID并且返回鉴权结果。

如果没有，调用统一认证平台获取该用户所拥有的所有权限，并缓存在本地，另外判断请求的权限点ID是否拥有权限，返回鉴权结果。

1. 现勘客户端根据鉴权结果，对按钮显示进行相应设置。
2. 统一认证平台收到用户权限变更操作时，以消息形式通知现勘服务，现勘服务收到消息后，清空该变更用户对应的权限数据缓存。

# 附件

数据模型参见《统一认证平台数据模型.docx》

服务接口参见《统一认证平台服务\_RMI接口整理.xlsx》

# 图表目录

**附图目录：**

[附图1. 业务系统与统一认证平台交互方式 3](#_Toc467163445)

[附图2. 登录以及Token验证时序图 4](#_Toc467163446)

[附图3. 菜单权限验证时序图 7](#_Toc467163447)

[附图4. 按钮权限验证时序图 8](#_Toc467163448)

**附表目录：**

**未找到图形项目表。**