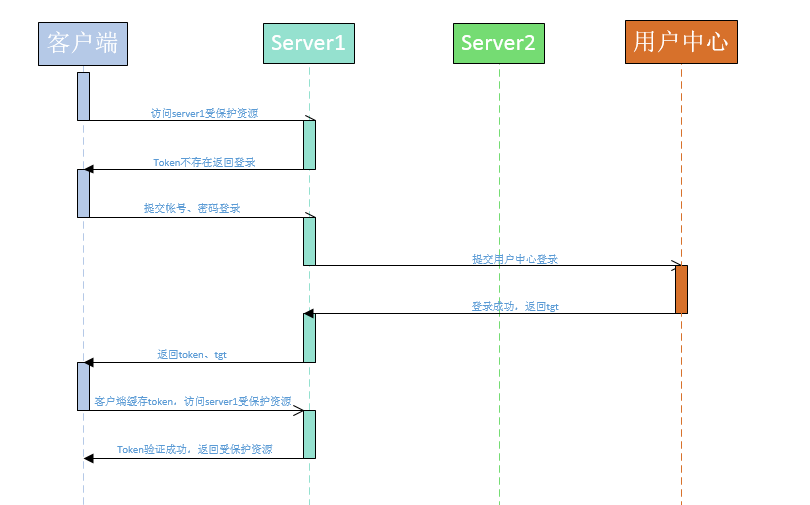
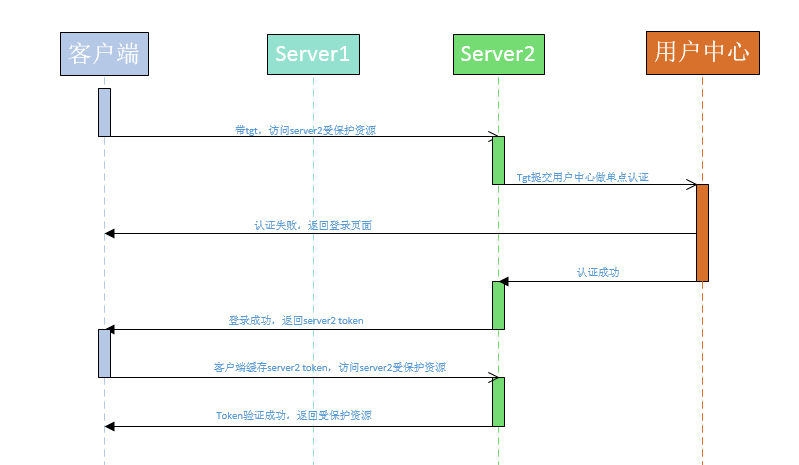
1. 需求分析
   1. 重构用户中心和CAS服务
   2. 使用方为中民未来下所属对公系统（乐家慧、hshop等）
   3. 对外提供无状态API
   4. pc端和移动端？统一登录、登出页面？
   5. 是否需要管理控制台？如果需要都要做什么？
   6. 以票（token）的形式作为返回，有票就有状态
   7. 登录的逻辑：每人可以多票（或仅单票），票与权限的关系，踢票的逻辑
   8. 单点登出逻辑：单个系统登出，还是所有系统登出？各业务系统登录态是否一致？
2. 登录流程设计

首次访问：



单点到其他系统：



1. 功能清单

接口清单：

|  |  |  |
| --- | --- | --- |
| **接口名称** | **接口描述** | **备注** |
| 用户注册 | 支持登录名、手机号、邮箱注册 |  |
| 用户登录 | 支持登录名、手机号、邮箱登录，登陆成功后返回票据tgt |  |
| 单点登录认证 | 不使用cookie/session来保持会话，使用tgt | 使用token去掉服务端状态保持，可以更方便的进行横向扩展以及更好的面向服务失败 |
| tgt延时服务 | 设置tgt从当前时间开始多少秒有效 |  |
| 查询tgt剩余有效时间 | 查询tgt剩余有效时间，单位秒 |  |
| 单点登出 | 登出后需要通知其他系统该票据已失效 |  |
| 用户修改密码 |  |  |
| 获取用户资料 |  |  |
| 登录名唯一性校验 |  |  |
| 手机号唯一性校验 |  |  |
| 邮箱唯一性校验 |  |  |
| 证件号码唯一性校验 |  |  |
| 绑定登录名 |  |  |
| 绑定手机号 |  |  |
| 绑定邮箱 |  |  |
| 绑定证件号码 |  |  |
| 绑定第三方帐号 |  |  |

接口安全：

权限认证

1. 表结构设计

核心历史表结构

|  |  |  |
| --- | --- | --- |
| **表名** | **注释** | **备注** |
| USER\_CENTER\_JOURNAL | 用户中心交互日志 | 接口日志表 |
| ZM\_USER | 用户表 |  |
| ZM\_USER\_AVATAR | 用户头像表 |  |
| ZM\_USER\_BANK\_ACCOUNT | 用户银行账号 | 不需要 |
| ZM\_USER\_CHANNELS | 业务渠道表 | 空表 |
| ZM\_USER\_EMAIL | 用户邮箱 |  |
| ZM\_USER\_IDENTITY | 用户证件表 |  |
| ZM\_USER\_LOGIN | 用户登录历史表 |  |
| ZM\_USER\_PERSON\_MAIN | 个人用户基本信息表 | 空表 |
| ZM\_USER\_PHONE | 用户电话联系方式 |  |
| ZM\_USER\_REFERRER | 用户注册推荐人 | 不需要 |
| ZM\_USER\_SALES | 用户销售经理绑定 | 不需要 |
| ZM\_USER\_SECURITY\_BIND | 用户安全绑定表 |  |
| ZM\_USER\_SECURITY\_BIND\_TRACE | 用户安全绑定轨迹表 |  |
| ZM\_USER\_SMS\_TEMPLATE | 短信模板表 | 不需要 |
| ZM\_USER\_TOKEN | 用户登录令牌表 | 空表 |
| ZM\_USER\_TRACE | 用户轨迹表 | 用户密码修改历史记录 |

* 1. 用户头像、邮箱、电话、证件都是一对多的表结构设计，考虑是什么，是否有必要？
  2. 用户头像不应该把二进制数据存在数据库里，数据量大对数据库查询、备份，迁移性能都有影响，建议只存url
  3. 接口交易日志可以考虑写在文件内
  4. 证件号和电话都是加密存储
  5. 考虑历史数据迁移，加密方式必须保持一致

1. 技术选型
   1. 基于hap框架上做二次开发，优点是快速，缺点是依赖hap但大部分功能是无用，太过笨重
   2. 使用开源工具spring+springmvc+mybatis+redis搭建轻量开发框架