单点登录系统详细设计

## 1需求背景

请设计一套单点登录系统，具备以下功能

1. 具备注册登录功能
2. 一个用户只能在一个设备上登录，切换终端登录时，其他已登录的终端会被踢出
3. 后台可以根据管理策略将已登录设备踢出

## 2功能分析

1. 注册功能
2. 登录功能，登录时，如果存在旧的登录设备，将其踢出
3. 管理后台可以将已登录设备踢出

设计思路

1. 请求使用https,并校验证书，防止中间人攻击；
2. 登录过程中，避免传输明文密码；数据库不保存明文密码；

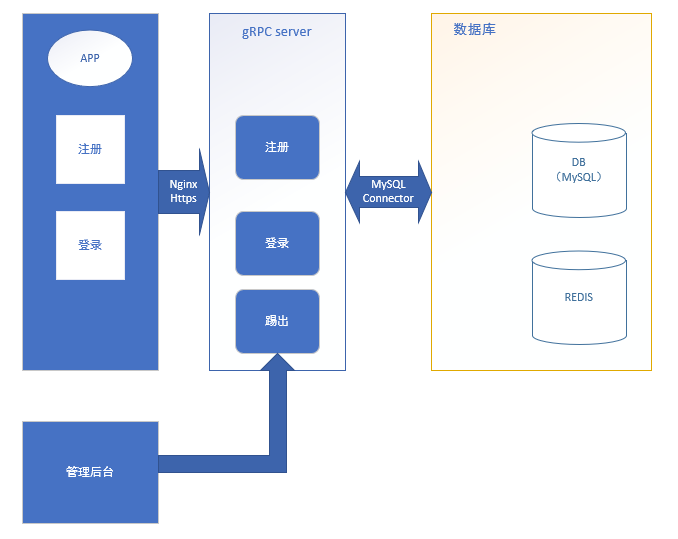
注册时，服务端，生成salt，跟userID关联保存数据库，使用HMAC算法生成密码摘要保存用户密码；并将salt发送给客户端，做持久化保存。

登录时，客户端salt，使用相同HMAC算法生成密文，发送给服务器。服务器接收后与数据库密码对比是否一致。

未避免用户salt泄露或者密文摘要泄露问题，增加时间种子，客户端登录时，密文摘要与时间戳做哈希后传递给服务器，服务器采集当前时间一定时间范围内的时间戳做相同操作。保证了在不同时间，传递的密码不同，进一步增强安全性。

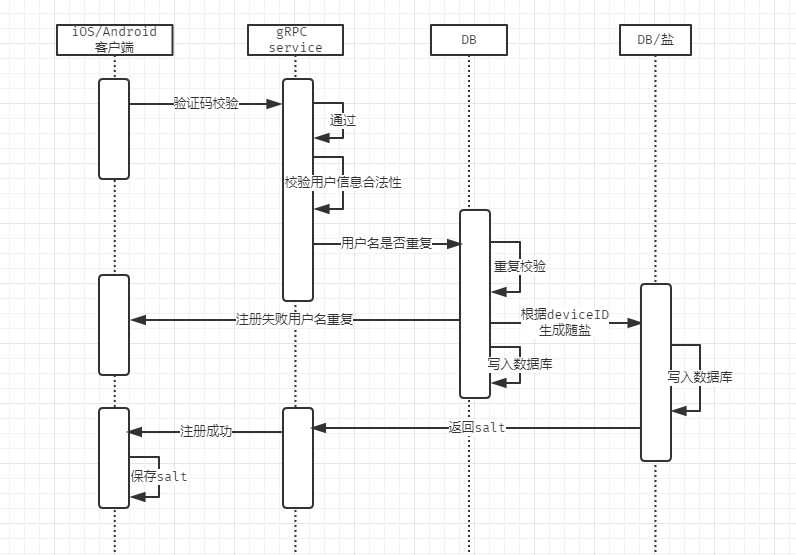
登录成功后，服务器返回认证token，客户端在请求授权资源时，携带token，无效时返回未登录。

## 3整体架构



## 4时序图

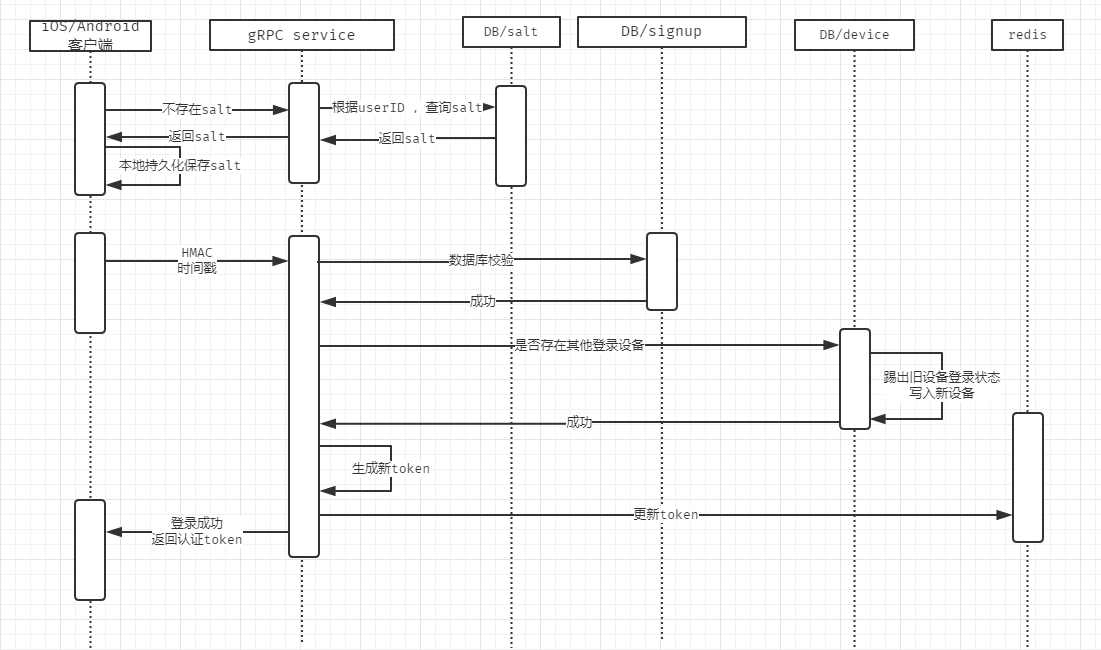
4.1 注册时序图



注册流程

1. 客户端注册时强制走https;
2. 服务端接收到注册请求，校验用户名，密码等是否满足条件（用户名是否有特殊字符，密码复杂性等），并判断是否有重复；
3. 验证通过后，根据userID，生成随机盐salt，并保存到数据库；
4. 根据生成的salt，使用HMAC算法，生成密码摘要，和用户信息一起保存到用户注册表；
5. 返回注册成功，并将salt返回客户端，客户端做持久化保存；

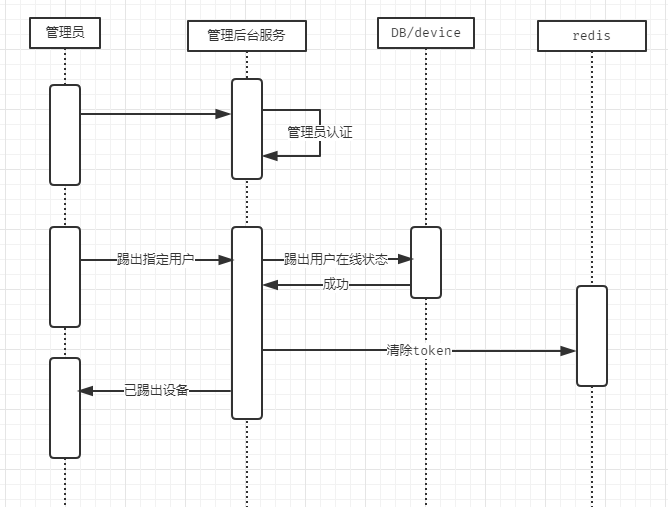
4.2登录时序图



登录流程

1. 判断是否有salt，如果没有，调用服务端请求getSalt，如果有则进行第3步；
2. 服务端根据userID，返回对应salt；
3. 客户端使用相同HMAC算法，生成密码摘要，与当前时间戳（精确到分钟）哈希（md5）后发送给服务端；
4. 服务端根据保存的密码，使用同样方式哈希（md5）后与参数对比，不一致时，取当前时间前后两分钟的时间戳再次对比，有相同结果即为登录成功。
5. 生成认证token，并更新到redis，设置有效时常（客户端有效token校验通过后，刷新有效时常）；
6. 返回认证token；

4.3 管理后台踢出登录设备



管理后台踢出设备流程

1. 管理员账号认证；
2. 管理后台提交指定用户ID，服务端根据userID，查询用户是否在线；

用户没有在线设备，返回用户未在线；

1. 用户有在线设备，更新为下线状态，并清除认证token；
2. 返回已踢出设备登录；

## 5数据库

5.1 用户注册表t\_sign\_up

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 必填 | 说明 |
| userID | Big int | 是 | 用户id，索引 |
| userName | Varchar(128) | 是 | 用户昵称 |
| password | Varchar(128) | 是 | 密码 |
| status | Tiny int | 是 | 用户状态0正常 |
| ext |  |  | 扩展字段 |

5.2 登录历史设备t\_login\_his

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 必填 | 说明 |
| id | bigint(20) unsigned | 是 | 索引 |
| deviceID | Varchar(128) | 是 | 设备id |
| userID | Varchar(128) | 是 | 用户id |
| loginTime | int(10) unsigned | 是 | 设备登录时间 |
| updateTime | int(10) unsigned | 是 | 设备登录更新时间 |
| status | Tiny int | 是 | 登录状态0登录中，1登录失效，2管理员踢出 |

5.3 随机盐t\_salt

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 类型 | 必填 | 说明 |
| id | bigint(20) unsigned | 是 | 索引 |
| userID | Varchar(128) | 是 | 用户id |
| salt | Varchar(128) | 是 | 随机盐 |