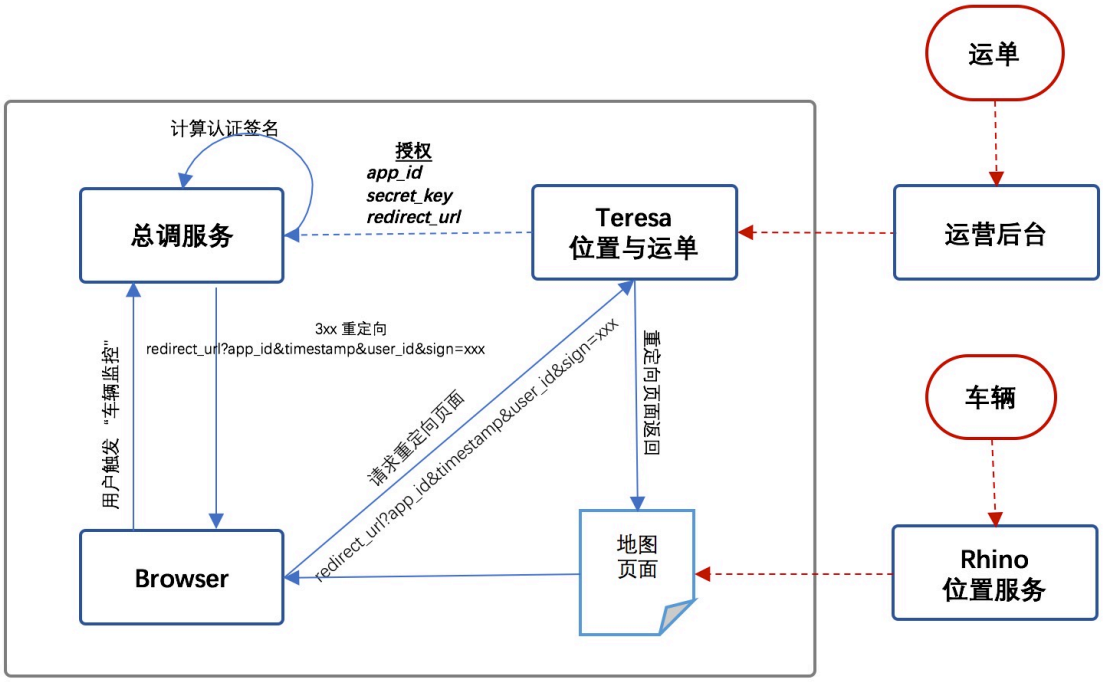
# Teresa安全认证方法

```
v0.1 zhangbin 2017.5.10
```

## 1. 需求

teresa系统提供的基于地图呈现的车辆和位置管理服务被集成到camel系统的**总调系统**。两部分系统独立部署，运行时，用户从 **总调系统** 管理界面触发teresa的业务功能操作。teresa的访问需受控，必须在**总调系统**登录后的用户方可访问teresa，所以teresa与**总调系统**之间需建立一种访问授权的机制来保障服务的访问安全。

## 2. 设计




**过程:**

```
1. 用户触发 车辆监控 操作，请求 总调服务器处理;
2. 总调服务器 根据Teresa分配的授权信息生成数据签名,返回重定向(redirect_url)到 浏览器,并附上授权信息;
3. Teresa接收到请求，提取请求进行数据签名验证、身份验证和时间有效性验证，如果验证通过，则生成地图操作页面;
   验证内容:
     1. 数据签名，防篡改
     2. timestamp检查是否过期(10分钟内为有效url请求)

验证成功，标识此用户身份合法，并将用户置入当前session，teresa的后续http请求访问时，服务器必须对每个请求进行基于
session的身份验证。
```

### 2.1 访问授权

平台的接口访问必须经过**总调系统**的授权后才可以访问与使用，Teresa系统通过向**总调系统**系统发放授权访问信息(app_id&secret_key&redirect_url)，外部系统在访问Teresa的接口时，必须在调用参数中指定app_id，否则接口访问将被

拒绝服务。

## 2.2 数据防篡改

在页面请求时url会传递几部分参数:

```
1.双方持有秘钥签名之后的摘要（sign）
2.时间戳(timestamp) ,标识请求发生的时间
3.应用授权标识( app_id ) ,标识此次请求的应用系统
4.用户标识(user_id)
```

Teresa接收到数据后，以同样的算法进行签名，生成摘要，对比两者的摘要是否相同，如果不同，说明传递过程中发生数据篡改。

## 2.3 接口签名算法

### 2.3.1 请求参数拼装

首先将每一个参数名称按字母顺序做升序排序，然后根据排序好的参数依次把每个参数名与参数值合并拼成一个字符串。

比如现在三个参数及值，foo=1,bar=2,baz=3进行拼装，则:

l a) 排序所有参数，排序后的结果为 bar=2,baz=3,foo=1。 b) 按顺序进行拼装，拼装后结果为 bar2baz3foo1。

2.6.2 签名算法 平台要求接口传递的参数必须做签名，以防止接口参数被任意篡改。签名摘要是根据所传输参数动态生成，具体算法为：md5（密钥+参数按字母升序排列+密钥）后的大写字母。

比如：(本示例中参数仅供参考签名计算方式，使用接口时需根据客户所用接口及相关信息调整参数)

```
某外部系统获得的app_id和secret_key分别为:
    app_id = apitest
    secret_key = ab179020b82d2fdcd4cea176796f7156

接口的参数如下:
    timestamp = 1494579247
    user_id   = abc


则计算:
uppercase(md5('ab179020b82d2fdcd4cea176796f7156app_idapitesttimestamp1494579247user_idabcab179020b8
2d2fdcd4cea176796f7156'))的值为:

686E696253E583F5FFB1B31AD787B423



redirect_url:

    http://<host>/teresa/name?
app_id=apitest&timestamp=1494579247&user_id=abc&sign=686E696253E583F5FFB1B31AD787B423
```

**注意**：secret_key只参与签名摘要的运算，不能放到参数列表中。