**单点登录SSO解决方案**

吴剑 <http://luck0235.cnblogs.com>

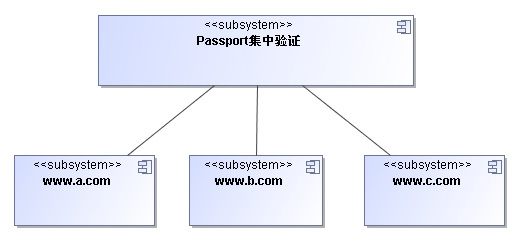
QQ:8935300

2009-6-24 于深圳

# 1设计

## 1.1概述

使用集中验证方式，多个站点集中Passport验证。 如下图所示：



## 1.2名词

为方便清晰描述，定义如下名词，本文中出现之处均含义相同

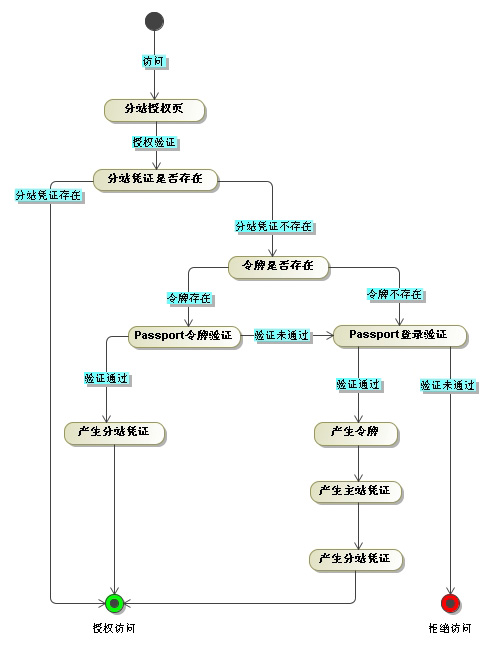
**主站**：Passport集中验证服务器 <http://www.passport.com> 。

**分站**：<http://www.a.com/>、<http://www.b.com/>、<http://www.c.com/>

**凭证**：用户登录后产生的数据标识，用于识别授权用户，可为多种方式，DEMO中主站我使用的是Cache，分站使用Session。

**令牌**：由Passport颁发可在各分站中流通的唯一标识。

## 1.3详细设计



**情形一**、匿名用户：匿名用户访问分站a上的一个授权页面，首先跳转到主站让用户输入帐号、密码进行登录，验证通过后产生主站凭证，同时产生令牌，跳转回分站a，此时分站a检测到用户已持有令牌，于是用令牌再次去主站获取用户凭证，获取成功后允许用户访问该授权页面。同时产生分站a的本地凭证，当该用户需要再次验证时将先检查本地凭证，以减少网络交互。

**情形二**、在分站a登录的用户访问分站b：因为用户在分站a登录过，已持有令牌，所以分站b会用令牌去主站获取用户凭证，获取成功后允许用户访问授权页面。同时产生分站b的本地凭证。

## 1.4关键点

**令牌**：令牌由主站颁发，主站颁发令牌同时生成用户凭证，并记录令牌与用户凭证之间的对应关系，以根据用户提供的令牌响应对应的凭证；令牌要在各跨域分站中进行流通，所以DEMO中令牌我使用主站的Cookie，并指定Cookie.Domain="passport.com"。各分站如何共享主站的Cookie？从分站Redirect到主站页面，然后该页面读取Cookie并以URL参数方式回传即可，可在DEMO代码中查看详细实现。

**主站凭证**：主站凭证是一个关系表，包含了三个字段：令牌、凭证数据、过期时间。有多种实现方式可供选择，要求可靠的话用数据库，要求性能的话用Cache，DEMO中我使用的是Cache中的DataTable。

**分站凭证**：分站凭证主要用于减少重复验证时网络的交互，比如用户已在分站a上登录过，当他再次访问分站a时，就不必使用令牌去主站验证了，因为分站a已有该用户的凭证。分站凭证相对比较简单，使用Session、Cookie均可。

**用户退出**：用户退出时分别清空主站凭证与当前分站凭证。如果要求A站点退出，B、C站点也退出，可自行扩展接口清空每个分站凭证。

**主站过期凭证/令牌清除**：请编写相应代码，定时清除(DataTable)Cache[“CERT”]中timeout字段大于当前时间的即可。

# 2布署

## 2.1在IIS中配置站点

配置4个站点指向相应的目录，并分别指定4个站点的主机头：

[www.passport.com](http://www.passport.com)

[www.a.com](http://www.a.com)

[www.b.com](http://www.b.com)

[www.c.com](http://www.c.com)

## 2.1修改hosts文件以将域名解析到本地站点

127.0.0.1 www.passport.com

127.0.0.1 www.a.com

127.0.0.1 www.b.com

127.0.0.1 www.c.com