# 1、引言 1.1编写目的

              为了单点登录系统(SSO系统)的可行性，完整性，并能按照预期的设想实现该系统，特编写需求说明书。  
        同时，说明书也发挥与策划和设计人员更好地沟通的作用。

## 1.2背景

          a．鉴于集团运营的多个独立网站（称为成员站点），每个网站都具有自己的身份验证机制，这样势必造成：生活中的  
             一位用户，如果要以会员的身份访问网站，需要在每个网站上注册，并且通过身份验证后，才能以会员的身份访问网  
           站；即使用户以同样的用户名与密码在每个网站上注册时，虽然可以在避免用户名与密码的忘记和混淆方面有一定的  
           作用，但是用户在某一段时间访问多个成员站点或在成员站点间跳转时，还是需要用户登录后，才能以会员的身份访   
            问网站。这样不仅给用户带来了不便，而且成员网站为登录付出了性能的代价；

           b．如果所有的成员网站，能够实现单点登录，不仅在用户体验方面有所提高，而且真正体现了集团多个网站的兄弟   
            性。通过这种有机结合，能更好地体现公司大平台，大渠道的理念。同时，这样做也利于成员网站的相互促进与相互  
            宣传。

            正是出于上面的两点，单点登录系统的开发是必须的，是迫在眉睫的。

## 1.3定义

               单点登录系统提供所有成员网站的“单一登录”入口。**本系统的实质是含有身份验证状态的变量，  
           在各个成员网站间共用**。单点登录系统，包括认证服务器(称Passport服务器)，成员网站服务器。

**会员：**用户通过Passport服务器注册成功后，就具有了会员身份。

**单一登录：**会员第一次访问某个成员网站时，需要提供用户名与密码，一旦通过Passport服务器的身份验证，  
                              该会员在一定的时间内，访问任何成员网站都不需要再次登录。

**Cookie验证票：**含有身份验证状态的变量。由Passport服务器生成，票含有用户名，签发日期时间，  
                                 过期日期时间和用户其它数据。

# 2、任务概述

## 2.1目标

         SSO系统，是集团统一的Passport，SSO系统分两个阶段实施。第一阶段对于新注册的用户提供单点登录的功能。  
      第二阶段，整合各个成员网站已有会员到单点登录系统中。

         Passport服务器作为各个成员网站的惟一身份验证入口，需要考虑其性能，扩展性，稳定性，安全性和维护成本。尤其  
      要注意第二阶段的开发，做到统筹考虑。

## 2.2最终用户的特点

         最终用户是数以万计网民。这就确定了用户使用电脑的水平是参差不齐的，在开发单点登录系统时，力争做到界面友  
      好，措词简单明了。用户不用学习，就能使用该系统。

# 3、需求规定

## 3.1 需求概述

           1)   注册：

            a.成员网站重定向到Passport服务器的注册页面，并且带有返回URL和成员网站ID。

            b.通过Passport注册页面创建会员后，保存会员验证票到数据库和passport服务器所在域cookie中。同时，在成员网站  
               的数据库上创建与Passport服务器数据库中会员的映射关系。

            c. 重定向到成员网站，填写会员个性信息。

            d. 保存会员个性信息，并把重定向传入的验证票保存到本地cookie和创建Session状态变量。

         2）登录：

            a、 SSO系统要实现各个成员网站的无缝结合，只要会员经过了认证服务器的登录验证（Passport服务器），该会员访  
                  问其它任何的网站时，都不需要再次登录。

            b、 会员在第一次登录时，Passport服务器验证身份之后，生成的cookie验证票，只需保存到Passport服务器所在域的  
               cookie中，不能采用向每个成员网站所在的域中写cookie,防止响应时间太长，给会员带来不友好的浏览体验。**同  
               时，把下发给会员的cookie票保存到Passport服务器的数据库中，方便验证方式和会员行为统计的扩展。**

         c、 会员一经通过身份验证，成功登录了某个成员网站(假设为网站A),需要利用Session和cookie两种方式保存会员已经登  
               录的状态。

         d、 同一个浏览器进程中，会员在网站A的页面间跳转时，只需要根据Session中的状态变量加载登录框。不需要再与  
               Passport服务器通信验证会员的身份。

         e、 会员通过验证登录了网站A,若会员从网站A跳转或重新打开浏览器登录其它成员网站(假设网站B)，都需要与Passport  
               服务器通信验证会员的票。但是，这次验证不要Passport服务器与数据库中保存的验证票进行比较验证，只需要验证  
               Passport服务器域中的cookie验证票据有效即可。

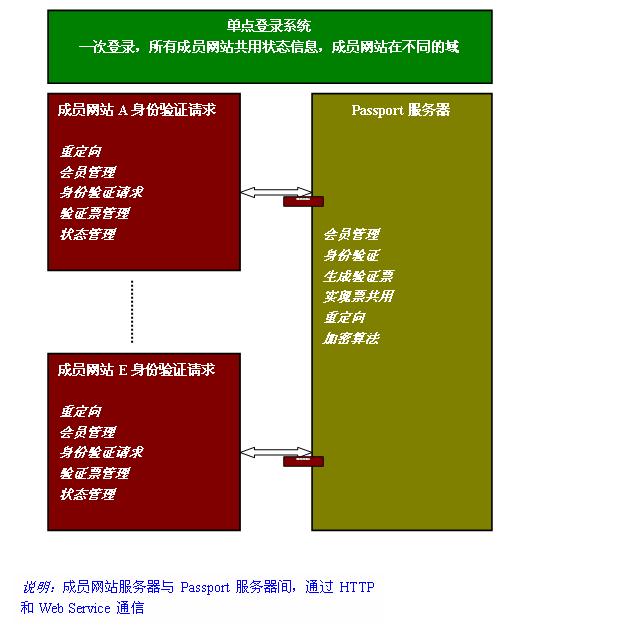
         f、   对于验证cookie票，能够实现加密和数字签名保证cookie的机密性，完整性和不可抵赖性。

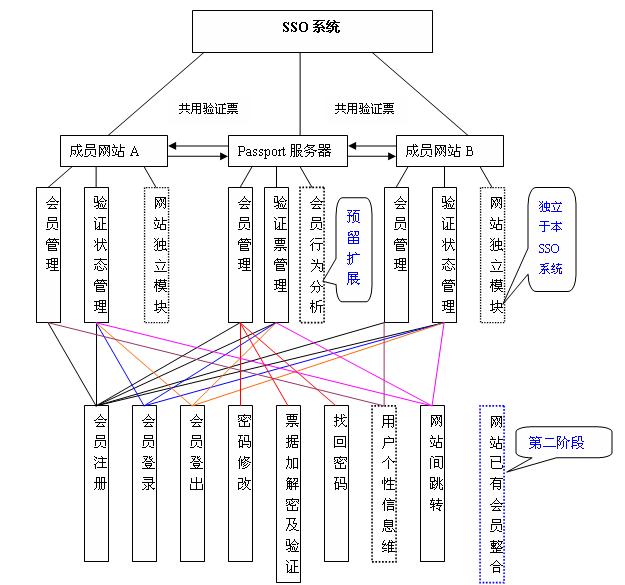
**g、 若果Passport服务器Down掉后，仍可以直接登录成员网站。**

**说明：上面高亮显示的表示二期开发功能。**

         3)登出、修改密码、找回密码和成员网站间的跳转，请查看IPO图表中相应的模块描述。

## 3.2对功能的规定

         SSO系统包括注册、登录、登出、密码修改、密码找回、成员网站间跳转与用户管理模块。本说明书使用HIPO图描述  
      系统机构和模块内部处理功能，它主要包括层次结构图和IPO图两个部分。层次结构图描述了整个系统的结构以及各个  
      模块之间的关系；IPO图则描述了在某个特定模块内部的输入（I）、处理过程（P）、输出（O）思想。  
  
     **A、系统结构图  
         **图1 SSO系统结构图

**B、层次结构图  
                     **  
图2系统层次结构图