**单点登录系统（Passport）**

**需求说明书**

1. **引言**

**1.1编写目的**

明确单点登录系统的功能范围，性能要求，为开发人员的设计提供依据。

本文档的读者为：需求分析师，架构师，项目经理，UI设计师，以及开发工程师，测试工程师。

**1.2背景**

随着公司业务的发展，公司的业务已经从单个系统扩展到多个系统，从单个区县扩展到省市，公司的业务系统开始有了更多、更高的要求。为了连接各个业务系统，提高用户体验，以让用户能实现一个账号，通行各个业务系统，特构建此系统。

**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。

1. **任务概述**

**2.1目标**

用户一次登陆，全网通行。无需再次登陆。

**2.2最终用户的特点**

公司业务系统的用户，主要分为三类：系统管理人员；一线教研员和教师；学生。随着业务的发展，还有可能有家长。

系统管理人员：系统的运行维护者，负责制定系统的运营规则；系统的基础数据管理。

一线教研员和教师：系统的实际使用着，主要是完成教研工作以及日常工作。

学生：系统的实际使用着，主要是通过系统实现自主学习，并和教师互动。

家长：系统的实际使用者，通过平台了解学生的学习情况，以及和教师互动。

1. **单点登录功能需求**

**3.1 注册**

用户可以通过本系统实现用户注册。注册时，需要填写以下基本信息：用户名、密码、性别，emai、真实姓名，身份，来源市县。（有些系统有昵称，是否所有系统都需要昵称？）

用户登陆后，在访问业务系统时，业务系统根据自身的需要，让用户补充业务系统所需要的信息。

要求：当本系统出现故障时，其他业务系统不能注册用户。

**3.2 登陆**

提供统一登陆的用户入口，此外也要提供统一登陆的接口。登陆验证字段：用户名、密码；来源网站；

系统要求记录用户登陆日志。

要求：当本系统出现故障时，其他业务系统还能各自登陆，但是不能实现跳转自动登陆。

**3.3会员信息修改**

提供会员基本信息修改页面和接口，修改身份，性别，email，真实姓名，身份，来源市县。

系统要求记录会员信息修改日志。

要求：当本系统出现故障时，其他业务系统不能修改会员信息。

**3.4密码修改**

提供密码修改界面和接口，修改用户密码。

要求：当本系统出现故障时，其他业务系统不能修改密码。

**3.5 接入站点管理**

管理接入站点，对非法接入站点，要屏蔽。

**3.6 密码保护**

能对用户设置密码保护。密码保护可以有：邮箱找回密码；密码问题保护。

1. **机构管理**

**4.1设置顶级机构**

在系统还没有机构数据时，可以设置顶级机构。具体包括机构名称、英文名称、网站名称、机构类型。

**4.2添加子机构**

可以给任意机构增加子机构。具体包括机构名称、英文名称、网站名称、机构类型，机构代码。

需要为业务系统提供增加机构的接口。

**4.3编辑机构**

有管理权限的用户，可以编辑修改机构。

需要为业务系统提供编辑机构的接口。

**4.4删除机构**

有管理权限的用户，可以删除修改结构。删除未逻辑删除。

需要为业务系统提供删除机构的接口。

**4.5业务系统的机构管理**

业务系统设置自身所在的机构代码。在业务系统初始化时，可以选择自身所在的组织机构，把相应机构数据同步到业务系统。

业务系统在机构管理时，必须提交到单点登录系统（中心系统）成功后，才可以写本系统数据。

1. **非功能需求**
2. **性能需求**

用户登陆响应时间在1秒内。（1秒比较高，压力大的时候，可以调整为3秒。）是否还有其他性能需求。

1. **并发需求**

能承受并发500个用户登陆。

1. **浏览器需求**

支持IE、 Firefox、Chrome、Opera、Safari的主流版本和基于这些浏览器内核的衍生产品，如360浏览器、猎豹浏览器、搜狗浏览器、QQ浏览器等等，只要符合业界（一般指W3C）规范的浏览器，做法一般都是一样的，都能正常使用，不用额外设置权限、安全性等，也就是浏览器默认设置下可以正常使用；

1. **其他非功能需求**

对现有系统要耦合小。在单点登录系统出现故障的情况下，业务系统要能自身能继续登陆使用业务功能。

要支持移动端的系统登陆。

同时支持IP和域名的接入。