**单点登录概要设计文档**

## 引言

### 编写目的

详细说明单点登录(SSO)的设计思想和实现方法，是日后该功能维护和扩展工作的基本依据文档。

### 背景

说明:

* 待开发功能的名称：单点登录。
* 本项目的任务提出者为网路中心总监,开发者为胡俊敏、赵佳星,用户为有用户整合需求平台的开发和设计人员。

### 定义

|  |  |
| --- | --- |
| **名称** | **定义** |
| **SSO** | 是Single Sign On的缩写，该技术主要用于用户同时登录多个网站，即用户只要在一个成员站点登录后，访问其他成员站点时也会自动登录。 |
| **认证中心** | 统一管理成员站点用户登录、验证登录信息、颁发令牌（登录认证信息）的中心站点。 预计绑定域名：passport.boke28.com |
| **成员站点** | 成员站点是遵从认证中心规则，享用认证中心统一用户的站点。 |
| [www.boke28.com](http://www.boke28.com) | **成员站点A** |
| [www.cstd28.com](http://www.cstd28.com) | **成员站点B** |
| www.goodideacn.com | **成员站点C** |
| Crm.goodideacn.com | **成员站点D** |
| Prm.boke28.com | **成员站点E** |
| 令牌 | 即登录认证信息。数据形式为:用户ID+加密后的密码字符串+公钥组合而成的字符串(可按实际情况调整) |
| DRM | 统一操作数据的WebSerivces站点（drm.cstd28.com） |

### 参考资料

本功能的设计和实现参考了下面的资料

* http://download.csdn.net/detail/yongtree/342163

## 程序系统的结构

**本功能包括下面几个应用页面，分别如下**：

|  |  |
| --- | --- |
| 页面 | 主要作用 |
| http:// passport.boke28.com/SSO/Login.aspx | 认证中心的登陆验证页面 |
| http://passport.boke28.com/SSO/crossdomain\_all.aspx | 认证中心向成员站点分发令牌或者删除令牌的总入口 |
| http://passport.boke28.com/SSO/crossdomain.aspx | 认证中心向各成员站点分发令牌或者删除令牌的具体实现页面 |
| [WWW.BOKE28.COM/sso/SetSession.aspx](http://WWW.BOKE28.COM/sso/SetSession.aspx)  [WWW.CSTD28.COM/sso/SetSession.aspx](http://WWW.CSTD28.COM/sso/SetSession.aspx)  WWW.goodideacn.com/sso/SetSession.aspx  Crm.goodideacn.com/sso/SetSession.aspx  Prm.boke28.com/sso/SetSession.aspx | 成员站点获取认证中心分发的令牌、置各自站点所需信息页面 |
| [WWW.BOKE28.COM/SSO/ClearSession.aspx](http://WWW.BOKE28.COM/SSO/ClearSession.aspx)  [WWW.CSTD28.COM/SSO/ClearSession.aspx](http://WWW.CSTD28.COM/SSO/ClearSession.aspx)  [WWW.GOODIDEACN.COM](http://www.goodideacn.com)/SSO/ClearSession.aspx  Crm.goodideacn.com/SSO/ ClearSession.aspx  Prm.boke28.com/SSO/ ClearSession.aspx | 成员站点统一删除认证信息页面 |

**工作流程描述如下**：

* **登陆**

1. **认证中心处理登录流程**

* **第一步：**任意一成员站点向认证中心提出登陆验证请求、并发送用户名、密码等信息
* **第二步：**在认证中心 http://passport.boke28.com/SSO/Login.aspx 接收成员站点发传递来的用户名、密码信息，验证用户有效性

1. **验证通过**：向各成员站点分发令牌，成员站点通过URL参数接收传递过来的令牌，去数据库获取相应的信息，如果有选中“2周内登录”，则把令牌信息同时保持在Session和Cookies里，如果没有，则只把令牌信息保存在Session里。
2. **验证失败**：把错误信息返回给对应的成员站点

**认证中心**

passport.boke28.com

**成员站点**

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

[www.boke28.com](http://www.boke28.com)

[www.cstd28.com](http://www.cstd28.com)

crm.goodideacn.com

prm.boke28.com

prm.boke28.com

用户名

密码

是否2周内登陆

验证用户

验证失败

验证成功

2周内登录

否

在成员站点中写入登录session信息

是

在成员站点中同时写入登录session和Cookies信息

（二）**成员站点的页面登录流程**

* 成员站点打开页面时，先判断有无登录Session信息，如果有，则直接显示登录。如果没有，则还需判断是否有令牌Cookies信息

1. **有：**通过Cookies里的令牌信息去数据库获取相应的信息，同时写到Session中，显示登录。
2. **无：**无登录，不显示登陆信息

**成员站点**

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

[www.boke28.com](http://www.boke28.com)

[www.cstd28.com](http://www.cstd28.com)

prm.boke28.com

prm.boke28.com

Session

有

无

2周内登录Cookies

无

有

根据Cookies取数据

写Session

* **退出**
* **第一步：**在成员站点中，将用户退出信息通过URL参数传入认证中心。
* **第二步：**认证中心向所有成员站点请求删除登录信息，如果原先有勾选“2周内登录”的，则成员站点接受请求后删除各自的Session和Cookies，如果没有，则成员站点接受请求后只删除Session。同时刷新最先请求退出的成员站点。

## 认证中心的接口、页面设计说明1

### 接口、页面描述

|  |  |
| --- | --- |
| 接口、页面名称 | http:// passport.boke28.com/SSO/Login.aspx |
| 功能描述 | 该页面在认证中心完成验证用户有效性、判断用户登录权限操作，并将令牌信息写入Session[“Info”] |
| 输入内容 | 用户名，密码，验证码，是否2周内登陆 |
| 处理逻辑 | 根据用户名密码验证用户有效性。   1. 验证成功：向成员站点发送令牌信息 2. 验证失败：返回错误信息 |
| 输出结果 | 0:成功；1:用户名或密码错误；2:用户锁定；3：用户已经删除；4：用户未激活；5：手机未验证；6邮箱未验证；7：程序异常；8：验证码错误 |
| 基本操作 | 点击按钮后台验证 |
| 备注 | 验证方法 DoLogin |

### 参数及方法

页面接收参数

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名称 | 类型 | 值范围 | 含义 |
| CheckCode | Get参数 | 0000-9999 | 验证码 |
| SaveCookie | Get参数 | 0/1 | 是否保持2周内登陆 |
| Account | Get参数 |  | 用户名 |
| PassWord | Get参数 |  | 密码 |

方法

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | 输入 | 输出 | 备注 |
| Protected int DoLogin(string Account,string Passport,string CheckCode,string SaveCookie) | 用户名  密码  验证码  是否2周内登陆 | 将用户信息保存在认证中心的Session[“Info”]中，同时返回  0:成功；1: 用户名或密码错误；2:用户锁定；3：用户已经删除；4：用户未激活；5：手机未验证；6邮箱未验证；7：程序异常；8：验证码错误 | 验证用户有效性，判断用户登录权限。并将令牌信息写入认证中心的Session。注：参数Account可能是用户名、手机或者邮箱 |

## 认证中心的接口、页面设计说明2

### 接口、页面描述

|  |  |
| --- | --- |
| 接口、页面名称 | http:// passport.boke28.com/SSO/crossdomain\_all.aspx |
| 功能描述 | 认证中心向成员站点分发令牌或者删除令牌的总入口,为认证中心向各成员站点发送令牌、删除令牌，写Session或者删Session做准备。 |
| 输入内容 | Action:login-登陆，lougout-退出  SaveCookie:0-未保持登陆，1-保持2周内登陆 |
| 处理逻辑 | 请求多个<http://www.passport.com/sso/crossdomain.aspx?Acton=login/logout&Domain=成员站点域名> 页面（与成员站点个数相同） |
| 输出结果 | <script type='text/javascript' src='http://www.passport.com/sso/crossdomain.aspx?action=“+Action +”&domain=”+成员站点域名+” &SaveCookie=" + SaveCookie + "'></script> |
| 基本操作 |  |
| 备注 | 有多少个成员站点，则有多少个crossdomain.aspx页面引用 |

### 前端HTML

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | 输入 | 输出 | 备注 |
| 1. <script type='text/javascript' src='http://www.passport.com/sso/crossdomain.aspx?action=“+Action +”&domain=www.boke28.com &SaveCookie=" + SaveCookie + "'></script> 2. <script type='text/javascript' src='http://www.passport.com/sso/crossdomain.aspx?action=“+Action +”&domain=www.goodideacn.com &SaveCookie=" + SaveCookie + "'></script> 3. <script type='text/javascript' src='http://www.passport.com/sso/crossdomain.aspx?action=“+Action +”&domain=crm.goodideacn.com &SaveCookie=" + SaveCookie + "'></script> 4. <script type='text/javascript' src='http://www.passport.com/sso/crossdomain.aspx?action=“+Action +”&domain=www.cstd28.com &SaveCookie=" + SaveCookie + "'></script> 5. <script type='text/javascript' src='http://www.passport.com/sso/crossdomain.aspx?action=“+Action +”&domain=prm.boke28.com &SaveCookie=" + SaveCookie + "'></script> | 页面传入的参数SaveCookie | 请求crossdomain.aspx页面 | 实际上是中转站 |

## 认证中心的接口、页面设计说明3

### 接口、页面描述

|  |  |
| --- | --- |
| 接口、页面名称 | http:// passport.boke28.com/SSO/crossdomain.aspx |
| 功能描述 | 将认证中心发送的令牌传递给成员站点 |
| 输入内容 | Action:login-登陆，lougout-退出  SaveCookie:0-未保持登陆，1-保持2周内登陆  Domain：成员站点域名 |
| 处理逻辑 | 根据Action判断是发送令牌还是删除令牌   1. 发送令牌：根据传入参数重定向到指定成员站点，并将令牌、保持登陆相关信息传给成员站点。 2. 删除令牌：根据传入参数重定向到指定成员站点。 |
| 输出结果 |  |
| 基本操作 | **Response.Redirect**("http://www.a.com/SSO/SetCookie.aspx?Info=" + Session[“Info”] + "& SaveCookie=" + SaveCookie); |
| 备注 | 在 Page\_load 中实现 |

## 认证中心的接口、页面设计说明4

### 接口、页面描述

|  |  |
| --- | --- |
| 接口、页面名称 | [http://WWW.BOKE28.COM/SSO/SetSession.aspx](http://WWW.A.COM/SSO/SetCookie.aspx)  <http://WWW.CSTD28.COM/SSO/SetSession.aspx>  <http://WWW.GOODIDEACN.COM/SSO/SetSession.aspx>  <http://CRM.GOODIDEACN.COM/SSO/SetSession.aspx>  <http://PRM.BOKE28.COM/SSO/SetSession.aspx> |
| 功能描述 | 通过认证中心传递过来的令牌，获取成员站点所需要的信息，保存到Session中 |
| 输入内容 | Info:令牌信息  SaveCookie:是否2周内登陆 |
| 处理逻辑 | 根据令牌查数据库，将相关用户信息保存在Session里面。 |
| 输出结果 |  |
| 基本操作 | 调用方法SetLoginSessionInfo |
| 备注 |  |

### 默认实现

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | 输入 | 输出 | 备注 |
| Public bool SetLoginSessionInfo(string Info) | 页面传入的参数, | false：失败  true：成功 | 保存登录Session信息 |

## 成员站点的接口、页面设计说明

### 接口、页面描述

|  |  |
| --- | --- |
| 接口、页面名称 | <http://WWW.BOKE28.COM/SSO/ClearSession.aspx>  <http://WWW.CSTD28.COM/SSO/ClearSession.aspx>  [http://WWW.GOODIDEACN.COM/SSO/ ClearSession.aspx](http://WWW.GOODIDEACN.COM/SSO/SetSession.aspx)  <http://CRM.GOODIDEACN.COM/SSO/SetSession.aspx>  <http://PRM.BOKE28.COM/SSO/SetSession.aspx> |
| 功能描述 | 删除令牌以及相关登陆信息，实现退出。 |
| 输入内容 |  |
| 处理逻辑 | 清空登陆相关的Session ,Cookies |
| 输出结果 |  |
| 基本操作 | 调用方法 ClearLoginSessionInfo |
| 备注 |  |

### 默认实现

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | 输入 | 输出 | 备注 |
| Public bool ClearLoginSessionInfo () |  | false：失败  true：成功 | 清除登录Session信息 |

## 各成员站点共用的登录方法

### 接口、页面描述

|  |  |
| --- | --- |
| 接口、页面名称 | 认证中心Login.js |
| 功能描述 | 统一登录退出方法的JS类。 |
| 输入内容 | 1. 登陆：**objAccount，objPwd，objCheckCode，objSaveCookie，objIframeDiv，redirectURL，scriptStr** 2. 退出：**objIframeDiv，redirectURL，scriptStr** |
| 处理逻辑 |  |
| 输出结果 | 1. 登陆：Status:0成功，否则失败 message:提示文本信息 2. 退出：0成功，1 失败 |
| 基本操作 |  |
| 备注 |  |

### 主要方法

1. **doLogin** 方法

|  |  |
| --- | --- |
| 参数名 | 输入 |
| **objAccount** | 用户名文本框ID |
| **objPwd** | 2周内保持登陆 checkbox |
| **objCheckCode** | 验证码控件ID |
| **objSaveCookie** | 是否需要“周内保持登陆” |
| **objIframeDiv** | 加载IFRAME的DIV ID |
| **redirectURL** | 登陆后跳转到哪去 |
| **scriptStr** | 登陆后执行的JS |

1. **doLogout** 方法

|  |  |
| --- | --- |
| 参数名 | 输入 |
| **objIframeDiv** | 加载IFRAME的DIV ID |
| **redirectURL** | 登陆后跳转到哪去 |
| **scriptStr** | 登陆后执行的JS |

## 其它关联

### 前台注册

**必填项:**账户名、密码、手机、邮箱为最基本的个人信息。

* **CSTD**

1. 培训管理者注册

* 实名认证中：中文名、性别、城市、企业、职位、办公电话、手机、邮箱

1. 企业会员注册

* 企业认证信息：企业名称、所属行业、年营业额、员工规模、通讯地址、邮编
* 联系人信息：中文名、性别、所属职位、办公电话、邮箱、手机

1. 报名活动添加参会人员

* 姓名、手机、邮箱、部门、职位
* **官网**

1. 注册页

* 公司名、联系人、手机

1. 报名详情页

* 姓名、部门、职位、手机、邮箱
* **易学团**

1. 注册页

* 所在企业、职位、城市

### 后台注册

* CRM

1. 新增潜在客户

* 重要程度、所属行业、电话、公司性质、公司规模、年营业额、地址、分配部门

1. 新增沙龙邀约记录

* 新增学员：姓名、邮箱、移动电话、部门、职务

1. 沙龙报名列表

* 新增到会人员：姓名、邮箱、移动电话、企业、行业、职务、城市

1. 用户管理

* 新增用户：所在部门、查询角色、操作角色、用户类型
* PRM

1. 新增专家

* 性别、所在地、专家类别、专长领域、一句话定位、推荐授课领域、主打\推荐课程、联系电话、移动电话、邮箱

1. 新增机构

所在地、一句话定位、邮箱

**通用方法**

|  |  |  |  |
| --- | --- | --- | --- |
| 方法 | 输入 | 输出 | 备注 |
| Public int AddUser(DataSet ds,Type type) | Dataset ds:注册信息  Type type：网站标识 | 0：成功  非0：失败(1：用户已存在，2：邮箱重复，3：手机重复， 4：程序异常) | DRM中用来添加用户的统一方法。 |