**详细设计说明书**

# 1引言

## 1.1编写目的

详细说明单点登录组件(SSO)的设计思想和实现方法，是日后该组件维护和扩展工作

的基本依据文档。预期读者是要实现单点登录(SSO)系统的系统设计人员，系统开发人员，系统维护人员。

## 1.2背景

说明：

1. 待开发软件系统的名称；jillzhang的SSO组件
2. 本项目的任务提出者为jillzhang、开发者为jillzhang、用户为有用户整合需求平台的开发和设计人员。

## 1.3定义

**SSO**是Single Sign On的缩写，该技术主要用于用户整合。

**认证中心**：认证中心是用户注册，成员站点管理，用户登录，验证登录信息，保存登录

信息，颁发登录认证的中心站点。

**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。

**注册站点：**如果想成为成员站点，必须先在认证中心进行站点登记，登记后，认证中心

会保存注册站点的配置信息，并将该配置信息发给注册站点。注册站点也需保存这些配

置信息，供日后与认证中心交互时候使用。

**联盟用户**：指在认证中心注册的用户，这些用户能被所有的成员站点所共享。

**登录请求**：指成员站点向认证中心发出的带有站点配置的用户登录请求信息。

**登出请求**：只用户向认证中心发出的要求退出登录的请求。

**登录请求验证：**指的是认证中心根据存储的站点信息对成员站点的登录请求信息进行来

源和真实性的验证。

**登出请求验证：**指认证中心在接受来自成员站点的登出请求的时候，对请求的来源和真

实性进行的验证

**登录答复：**指认证中心对经过验证的登录请求作出的答复信息。该答复包含用户的登录

信息。

**在线联盟用户数**：指的是在成员站点中，在线的联盟用户数量。

**在线联盟用户列表**：指的是在成员站点中，在线的联盟用户的列表信息。

**登录站点清单：**是由认证中心维护的用户的登录站点信息，当用户注销的时候，会遍历

此清单，逐个登出。

## 1.4参考资料

本组件的设计和实现参考了下面的系统和书籍

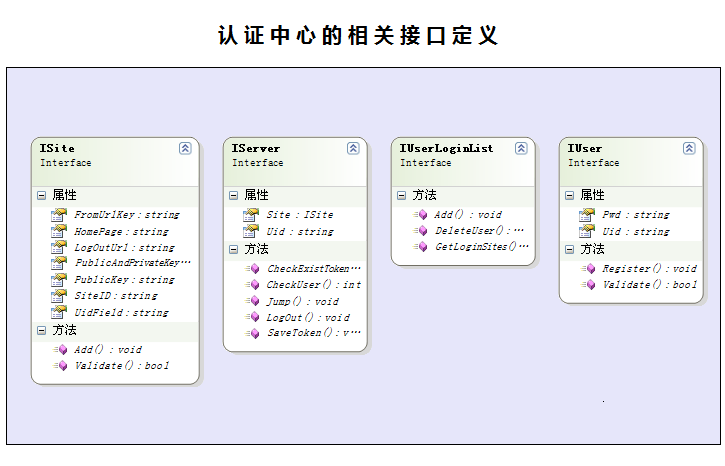
1. <http://www.cnblogs.com/David-weihw/archive/2007/01/25/630621.html>(已经失效)
2. 《数字签名技术原理及技术》

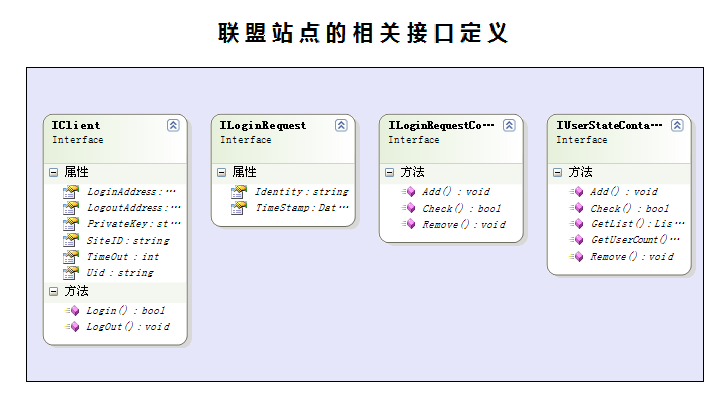
# 2程序系统的结构

本组件包括下面几个应用接口，分别如下：

1. ISite：ISite是用于描述和操作成员站点的接口
2. IUser : IUser是用于描述和操作联盟用户的接口
3. IServer:IServer是认证中心处理登录请求和登出请求的接口
4. IClient: IClient是成员站点发出登录请求和处理登录答复的接口
5. IUserLoginList：IUserLoginList是描述和操作用户登录站点清单的接口
6. ILoginRequest：是记录和操作成员站点发送登录请求的接口。
7. ILoginRequestContainer：用于保存和维护登录请求列表的接口
8. IUserStateContainer：是联盟站点中保存用联盟用户登录信息的接口。

它们的定义如下：





组件的工作流程描述如下：

1. 第一步，首先注册联盟站点，注册联盟站点用到接口ISite
2. 第二步：注册好联盟站点之后，将认证中心产生的站点配置信息（包括站点编号，站点公钥，站点私钥，认证中心的登录地址，认证中心登出地址）存储到联盟站点本地。
3. 在认证中心上注册一新用户，注册用户需要使用IUser接口
4. 在联盟站点对认证中心发出登录请求
5. 认证中心验证登录请求
6. 在认证中心进行登录
7. 登录成功后，保存登录票据，认证中心对联盟站点发送登录答复，并将此次登录记录到登录站点清单
8. 联盟站点接收到登录答复后，先进性验证，正确后，根据登录答复中的信息产生用户登录票据，并且更新联盟用户登录数和登录列表
9. 在联盟站点中发出登出请求
10. 认证中心验证登出请求，正确的话，销毁认证中心用户登录票据，通过用户的登录站点清单，逐个调用联盟站点的登出页面
11. 在认证中心回调联盟站点的登出页的时候，联盟站点会在登出页中销毁各个的登录票据，并更新在线用户数和用户列表。

# 3 ISite接口设计说明

## 3.1接口描述

ISite接口包括7个属性和2个方法，分别用于在认证中心用于描述和操作站点的配置

信息。



其中，各个属性的含义如下

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 含义 |
| SiteID | string | 站点编号，用于表示站点的唯一性。 |
| HomePage | string | 当登录请求中未提供来源网址项的时候，登录答复发送的地址 |
| LogOutUrl | string | 在进行统一登出的时候，回调的联盟站点页面地址，这个页面会负责销毁本站的登录票据信息。 |
| PublicKey | string | 用于数据交换时加密或签名用的公钥 |
| PublicAndPrivateKey | string | 用于数据交换时加密或签名用的私钥 |
| FromUrlKey | string | 用于指示联盟站点在发送登录请求和认证站点进行请求验证的时候来源网址存储位置。 |
| UidField | string | 用于指示联盟站点在发送登录请求和认证站点进行请求验证的时候用户信息的存储位置。 |

还包括两个方法，分别为：

|  |  |
| --- | --- |
| 方法名 | 含义和作用 |
| Add | 添加新的联盟站点。 |
| Validate | 验证联盟对象是否已经存在 |

## 3.2功能

该接口能在认证中心完成新联盟站点添加操作，添加之前可以验证站点是否存在。

## 3.3 默认实现

在SSO组件中，已经实现了一个默认的ISite对象。为DefaultServer/ DefaultSite.cs，它将放置在认证中心根目录下的sites.config文件作为存储介质，通过Add方法添加新联盟站点后的效果为：附件中的site.config文件，可自行下载文件后，看其结构。

# 4 IUser接口设计说明

## 4.1接口描述

IUser接口包括2个属性和2个方法，用于在认证中心端描和操作述联盟用户。



其中，各个属性的含义如下

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 含义 |
| Uid | string | 用户编号，是用户的标识 |
| Pwd | string | 用户密码 |

还包括两个方法，分别为：

|  |  |
| --- | --- |
| 方法名 | 含义和作用 |
| Validate | 验证用户是否存在 |
| Register | 添加新用户 |

## 4.2功能

该接口能在认证中心完成新联用户添加操作，添加之前可以验证用户是否存在。

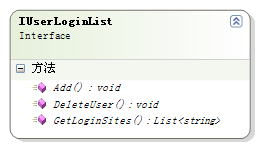
## 4.3 默认实现

在SSO组件中，已经实现了一个默认的IUser对象。为DefaultServer/ DefaultUser.cs，它将放置在认证中心根目录下的users.config文件作为存储介质，通过Register方法添加新联盟用户的效果为：附件中的users.config文件，可自行下载文件后，看其结构。

# 5 IUserLoginList接口设计说明

## 5.1接口描述

IUserLoginList接口包括3个方法，用于在认证中心描述和操作用户登录的站点清单。



还包括三个方法，分别为：

|  |  |
| --- | --- |
| 方法名 | 含义和作用 |
| Add | 验证用户是否存在 |
| GetLoginSites | 获取用户的登录站点清单 |
| DeleteUser | 删除用户的登录站点清单数据 |

## 5.2功能

该接口在认证中心用于用户记录和维护用户登录的站点清单

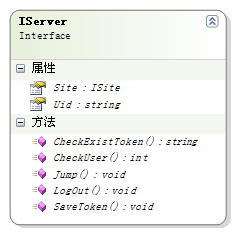
## 5.3 默认实现

在SSO组件中，已经实现了一个默认的IUserLoginList对象。为DefaultServer/ UserLoginLog.cs，它通过一个Collection对象来实现用户登录站点清单的维护工作。

# 6 IServer接口设计说明

## 6.1接口描述

IServer接口包括2个属性和5个方法，用于接收，验证登录请求，发送登录答复，接搜，验证登出请求，创建本地登录票据，维护用户登录清单。



两个属性为：

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 含义 |
| Site | ISite | 当前上下文处理请求和答复的站点对象 |
| Uid | string | 当前处理的上下文中的用户编号 |

还包括三个方法，分别为：

|  |  |
| --- | --- |
| 方法名 | 含义和作用 |
| CheckUser | 验证用户对象是否存在 |
| CheckExistToken | 验证登录票据已经存在 |
| SaveToken | 在认证中心本地保存登录票据 |
| Jump | 通过url跳转，发送登录答复 |
| LogOut | 统一登出。 |

## 6.2功能

该接口在认证中心，用于接收，验证登录请求，发送登录答复，接搜，验证登出请求，创建本地登录票据，维护用户登录清单

## 6.3 默认实现

在SSO组件中，已经实现了一个默认的IServer对象。为DefaultServer/ LoginRequest.cs。

# 7 ILoginRequest接口设计说明

## 7.1接口描述

ILoginRequest接口包括2个属性，用于记录和描述联盟站点的登录请求，这些信息在发出登录请求的时候创建，在收到登录答复的时候销毁。用于确保登录答复的不可复用性。



两个属性为：

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 含义 |
| Identity | string | 登录请求标志符，该标志符会发送给服务端，服务端在发送登录答复的时候会回传该标志，联盟站点会根据此标志来验证请求是否是伪造的。 |
| TimeStamp | DateTime | 请求的时间戳 |

## 7.2功能

该接口在联盟站点，用于记录和描述联盟站点的登录请求，这些信息在发出登录请求的时候创建，在收到登录答复的时候销毁。用于确保登录答复的不可复用性。7.3 默认实现

## 7.3 默认实现

在SSO组件中，已经实现了一个默认的ILoginRequest对象。为DefaultServer/ LoginRequest.cs。

# 8 ILoginRequestContainer接口设计说明

## 8.1接口描述

ILoginRequestContainer接口包括3个方法，用于在联盟站点中记录和维护登录请求



|  |  |
| --- | --- |
| 方法名 | 含义和作用 |
| Add | 添加登录请求信息 |
| Check | 检查登录请求是否存在 |
| Remove | 销毁存在的登录请求 |

## 8.2功能

该接口在联盟站点，用于在联盟站点中记录和维护登录请求

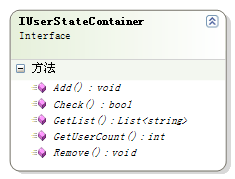
## 8.3 默认实现

在SSO组件中，已经实现了一个默认的ILoginRequestContainer对象。为DefaultServer/ LoginRequestContainer.cs。

# 9 IUserStateContainer接口设计说明

## 9.1接口描述

IUserStateContainer接口包括5个方法，用于在联盟站点中记录和维护在线联盟用户信息



|  |  |
| --- | --- |
| 方法名 | 含义和作用 |
| Add | 添加登录用户 |
| GetList | 获取在线用户清单 |
| Check | 检查某个用户是否已经在线 |
| Remove | 移除某个在线用户。 |
| GetUserCount | 获取在线用户个数 |

## 9.2功能

该接口在联盟站点，用于在联盟站点中记录和维护在线联盟用户信息

## 9.3 默认实现

在SSO组件中，已经实现了一个默认的IUserStateContainer对象。为DefaultServer/ UserState.cs。

# 10 IClient接口设计说明

## 10.1接口描述

IClient接口包括6个属性和2个方法，用于发出登录请求和登出请求



8个属性为：

|  |  |  |
| --- | --- | --- |
| 属性名称 | 类型 | 含义 |
| SiteID | string | 站点编号 |
| PrivateKey | string | 数据交换时加密或者签名用的公钥 |
| LoginAddress | string | 认证中心登录地址 |
| LogoutAddress | string | 认证中心登出地址 |
| Uid | string | 登录的用户编号 |
| TimeOut | int | 登录答复的超时时间，单位s |
| UidField | string | 登录登出请求中的用户信息的存储位置 |
| FromUrlField | string | 登录请求中的来源网址存储位置 |

2个方法为

|  |  |
| --- | --- |
| 方法名 | 含义和作用 |
| Login | 发出登录请求，并处理登录答复 |
| LogOut | 登出 |

## 10.2功能

该接口在联盟站点，用于发出登录请求和登出请求

## 10.3 默认实现

在SSO组件中，已经实现了一个默认的IClient对象。为DefaultServer/ DefaultClient.cs

# 11 本系统的安全性

## 11.1 登录请求的格式

联盟站点向认证中心发送的登录请求格式如下：

站点信息+登录请求编号+时间戳+空用户信息+对站点信息和登录清秋号的签名信息。

除了签名信息之外的全部信息均为明文传送，但因为重要的数据均经过数字签名，结果是站点信息和登录请求编号是不能被篡改的，保证了认证中心收到的登录请求的真实性。

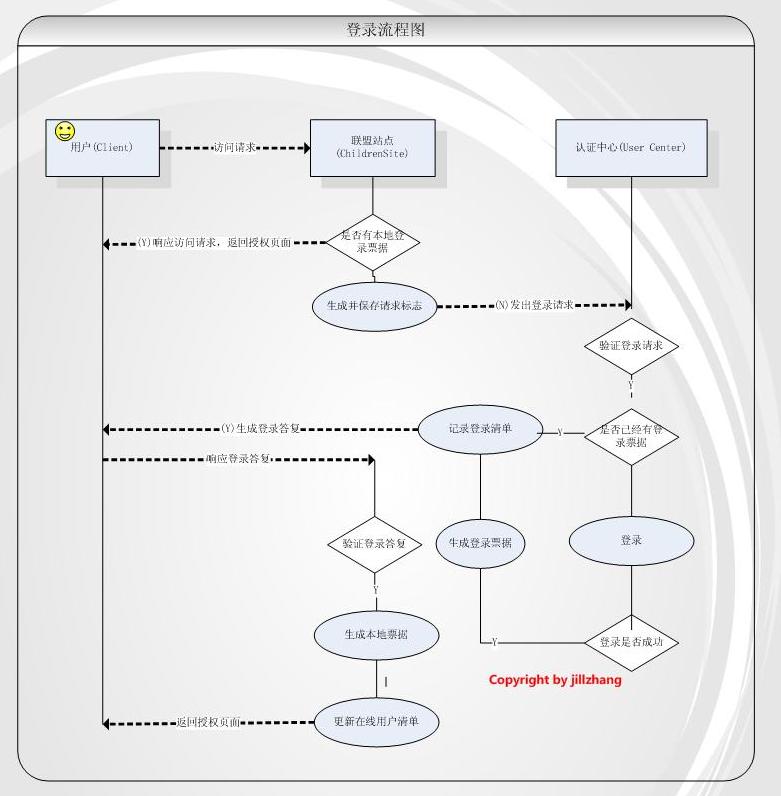
## 11.2 登录答复的格式

认证中心发给联盟站点的登录答复格式如下

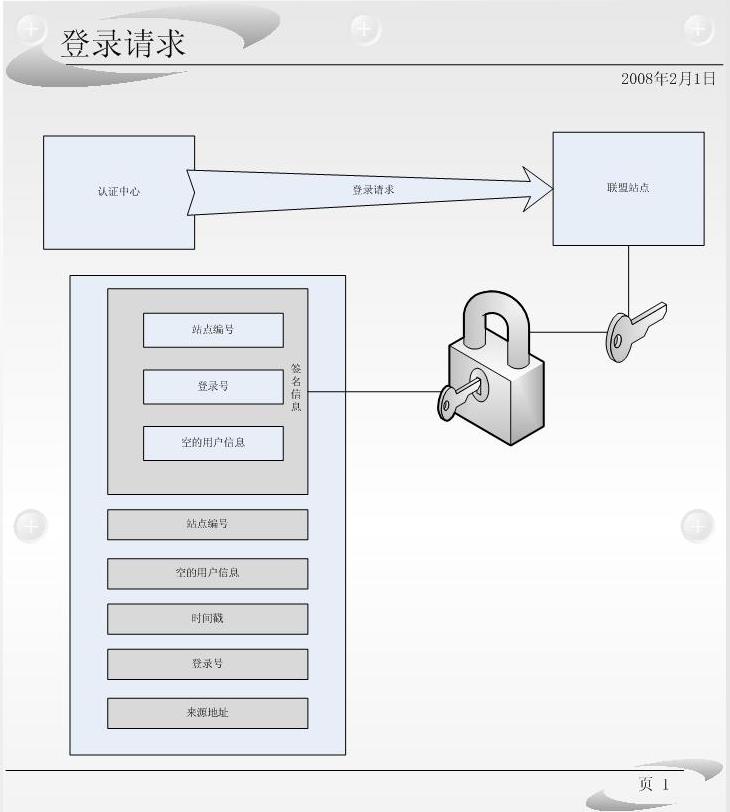
登录用户信息+登录请求编号+时间戳+对用户信息和登录请求号和时间戳的签名信息

其中登录用户信息是经过非对称加密的。请求号和时间戳因为经过签名，故也不能篡改，这样就可以保证联盟站点收到的登录答复的真实性和完整性。并且非正常联盟站点无法解密用户信息，也无法从中获取好处。

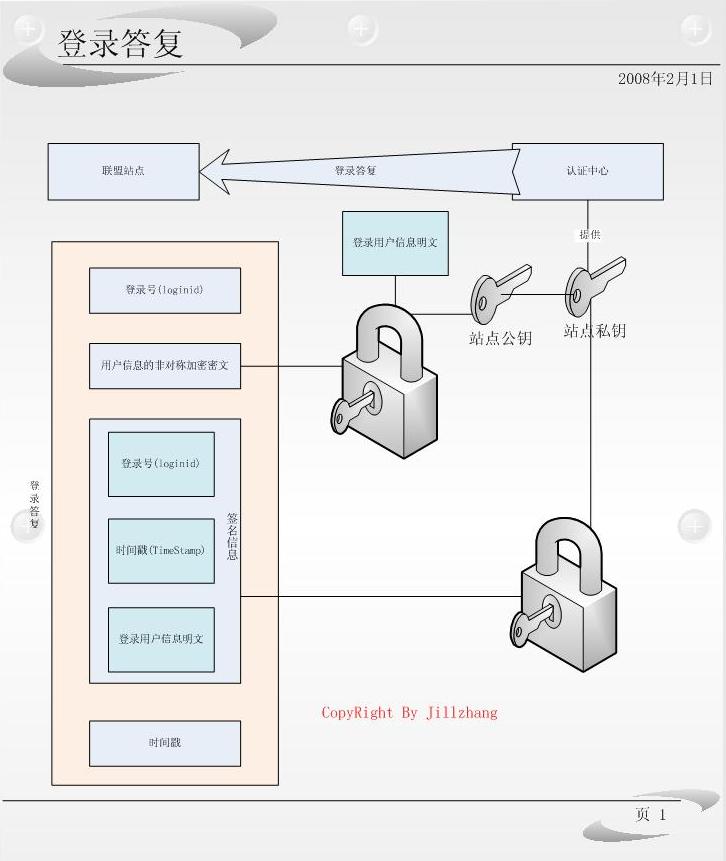
## 11.3 请求+答复流程图



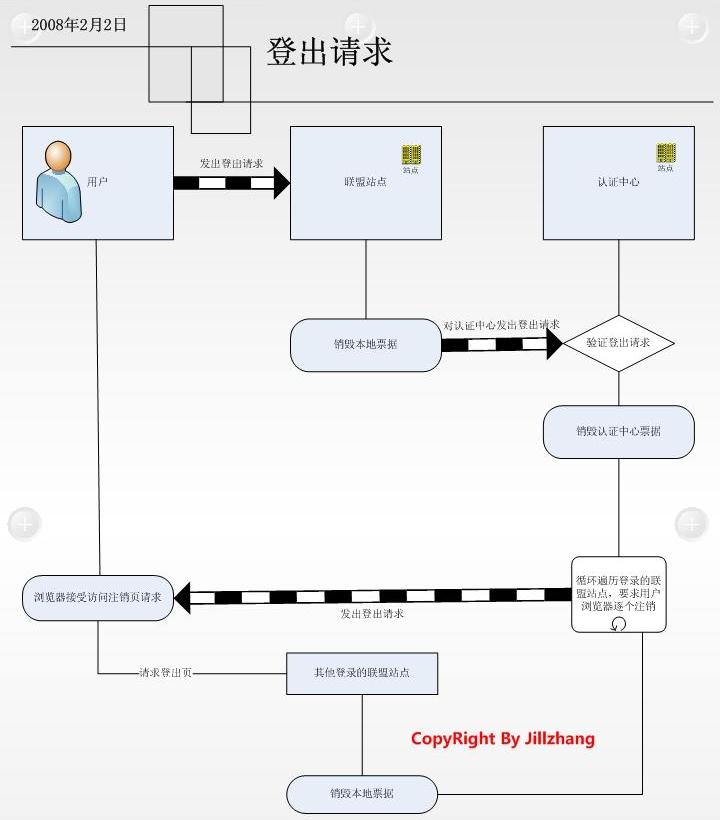
上面是整体流程图，这个SSO组件在安全上有了很充分的考虑，可以说是非常安全，那么下面看看登录请求数据的格式，和为何它能保证真实性和完整性



这样，当数据在传输过程中，如果站点编号，用户编号，请求号任意一项做任何的修改，当认证中心接收到数据之后，均无法与签名信息进行匹配。凡是认证中心能验证通过的请求均为合法的，真实的，完整的请求信息。  
  
登录答复的格式如下图所示



因为登录号，时间戳，用户信息均加入数字签名信息，所以这些数据在传输中不能被伪造和篡改，而用户信息经过非对称性加密，也防止非真正请求发送者能解析出用户信息，这样在接受和发送请求和响应的时候，就实现了绝对的安全。  
当然不是没有破绽，破绽在于当请求答复未到达联盟站点之前，有人截获并先于正常用户登录了联盟站点，此时我们可以将用户的ip信息作为答复数据的一部分，加入签名，以此实现很高的安全保证  
  
登出流程图



附上源码:

