|  |
| --- |
| 融创中国统一身份管理平台系统项目  精装修系统统一访问控制设计方案  版本1.0  2017/11/28 |

**文档修订记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本/状态** | **作者** | **参与者** | **起止日期** | **备注** |
| 1.0/A | 付国亮 |  | 2017.11.28 | 初始文档 |
|  |  |  |  |  |
|  |  |  |  |  |

注：变化状态：A—增加，M—修改，D—删除

**审批**

|  |  |  |  |
| --- | --- | --- | --- |
| **审批日期** | **审批版本** | **审批人角色** | **审批人** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

目录

[1 .概述 4](#_Toc499625996)

[2 .融创精装修系统统一访问控制集成规范 4](#_Toc499625997)

[2.1 单点登录集成方案 4](#_Toc499625998)

[2.1.1 登录流程 4](#_Toc499626002)

[2.1.2 单点集成详细说明 5](#_Toc499626007)

[2.2 业务系统登录逻辑改造 5](#_Toc499626008)

[2.3 业务系统单点登出改造 6](#_Toc499626009)

## .概述

OAM统一访问控制集成原理：当用户通过浏览器请求访问应用系统的相关IT资源时，请求被WebGate拦截并转发给OAM认证服务器进行身份认证，该用户通过身份认证后，OAM产生一个会话凭证，并将此会话凭证以及认证策略里配置的返回参数发送给应用系统，应用系统根据返回参数进行相应的细粒度授权

## .融创精装修系统统一访问控制集成规范

### 单点登录集成方案

OAM产品为不同的应用系统提供了丰富的集成方案，为了保证融创精装修系统与原有已集成单点的系统不受影响，具体集成方案如下



#### 登录流程





#### 单点集成详细说明

对于使用.NET开发平台开发的应用，一般是部署在IIS上，由于Oracle提供了与IIS匹配的WebGate，因此可以直接安装配置，然后直接修改应用系统的登陆逻辑即可，采用IIS部署的应用集成架构如下图所示：



IIS应用的单点登录集成一般包含以下六个步骤：

1. 确定和IIS相适应的WebGate版本，上传至应用系统服务器
2. 应用系统登录逻辑改造，见2.2章节说明
3. 在OAM端新建WebGate服务端，同时新建相关的验证、授权策略，配置好需要传送的变量类型和名称
4. 在应用服务器上安装WebGate客户端，相关的配置信息，依照WebGate服务端的配置填写
5. 重启IIS服务器
6. 相关的功能测试

### 业务系统登录逻辑改造

统一访问控制平台上线以后，访问被集成的业务系统时，用户的用户名和密码的验证工作将由OAM接管。所有业务系统需要接收OAM的响应，然后取得相应的验证信息，再进行下一步的细粒度认证和授权。

针对非套装软件的业务系统，其登录逻辑改造的伪代码如下：

String userId = request.getHeader ("OAM\_UID");//登陆用户的用户名

If (userId 为 空){

跳转到业务系统原有登录界面//以防止OAM宕机时，按照原有方式访问

}else{

以userId查询本地数据库，取得业务系统登录名 login\_ID；

If(login\_ID 为空){

返回到错误界面

}else{

以login\_id对用户认证和授权

}

}

### 业务系统单点登出改造

应用系统将本系统内的session注销掉后跳转到IDM单点注销注销地址完成OAM的session注销或将应用系统注销功能屏蔽。