**IDM概要设计文档**

**2014.03**

**修订记录**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修订内容** | **作者** | **日期** |
| 1.0 | 初稿完成 | 袁欢 | 2014/3/26 |
| 1.1 | 修正设计方案：去掉黑白名单；  修改客户端访问限制条件。 | 袁欢 | 2014/4/2 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目 录**

[1 IDM总体架构 4](#_Toc385597409)

[1.1 概述 4](#_Toc385597410)

[1.2 安全框架 4](#_Toc385597411)

[1.3 开源产品分析 4](#_Toc385597412)

[2 用户管理 5](#_Toc385597413)

[2.1 User 5](#_Toc385597414)

[2.2 Group 6](#_Toc385597415)

[2.3 AccessKey 6](#_Toc385597416)

[2.4 Policy 6](#_Toc385597417)

[2.5 权限和策略 7](#_Toc385597418)

[2.5.1 权限分离 7](#_Toc385597419)

[2.5.2 最小权限 7](#_Toc385597420)

[2.6 密码 7](#_Toc385597421)

[2.7 证书 8](#_Toc385597422)

[3 数据安全 8](#_Toc385597423)

[3.1 SSL加密传输 8](#_Toc385597424)

[3.2 安全访问数据库 8](#_Toc385597425)

[3.3 创建安全的响应消息 8](#_Toc385597426)

[3.4 关键数据加密存储 8](#_Toc385597427)

[4 接口安全 8](#_Toc385597428)

[4.1 用户身份验证 8](#_Toc385597429)

[4.2 输入参数安全性检查 8](#_Toc385597430)

[4.3 数字签名 9](#_Toc385597431)

[4.4 请求失效时间 9](#_Toc385597432)

[4.5 可信设备及访问 9](#_Toc385597433)

[4.6 接口访问频率限制 9](#_Toc385597434)

[5 安全审计 9](#_Toc385597435)

[5.1 流量审计 9](#_Toc385597436)

[5.2 行为审计 9](#_Toc385597437)

[5.3 内容审计 10](#_Toc385597438)

# IDM总体架构

## 概述

本文档旨在对IDM系统进行详细设计和描述，以保障整个云计算平台的安全性。

## 安全框架

下面的图片展示了系统平台的整体安全框架。



## 开源产品分析

主要分析了ForgeRock提供的开源IDM、AM产品，详细情况如下表所示。

表 ForgeRock开源IDM、AM产品分析

|  |  |  |  |
| --- | --- | --- | --- |
|  | **OpenIDM** | **OpenAm** | **OpenDJ** |
| **功能** | 用户管理功能，包括：用户身份周期管理、用户和组管理、密码管理、角色管理、权限管理、策略管理、认证和授权、同步功能等核心功能。  并提供REST接口进行管理。  OpenIDM的用户数据可以同步到OpenDJ。 | OpenAM 是一个领先的开源认证、授权的产品，可用于替换即将被取消的 [OpenSSO](http://www.oschina.net/p/opensso)。  OpenAM 提供核心的标识服务用来简化实现在一个网络架构中的透明单点登录，包括集中式或者分布式的单点登录。主要的特性有：   * 完全符合开源AAA产品； * AAA协议：计算机安全领域的协议，AAA指：鉴权，授权，计费（Authentication, Authorization, Accounting）； * 简单易用、易配置； * 纯Java开发； * 可轻松配置联合认证系统，并集成到已有项目中。   并提供REST接口进行管理。 | 提供LDAP服务，并提供REST接口进行方便的管理。 |
| **适用范围** | 用户管理。 | 主要适用于单点登录（SSO）的应用场景。 | LDAP应用。 |
| **认证机制** | 客户端进行认证的时候，向OpenIDM提供用户名密码（明文传输），OpenIDM进行认证并返回认证结果。 | OpenAM提供的认证机制主要是用户登录功能，用户在接口中提供用户名密码，OpenAM验证成功之后会返回一个TokenId，用于后续的SSO步骤。 | 提供标准的LDAP认证机制。 |

分析结论：

1. OpenIDM/OpenAM/OpenDJ功能丰富，接口以及文档齐全，基本满足需求；
2. 部分不满足需求的功能需要自行开发实现，例如：数字签名、AKSK管理、REST接口认证、接口访问频率、黑白名单等。

# 用户管理

## User

分为两种类型的用户：管理员账户和普通用户。管理员账户可以创建新的用户，用户不可以再创建子用户。

两者的关系为一对多的关系，如下图所示：



## Group

一个组下面可以包含多个用户，一个用户也可以同时属于多个组，两者为多对多的关系。如下图所示：



## AccessKey

管理员用户创建了普通用户之后，为其创建了一对访问密钥（AccessKey）和秘密访问密钥（SecretAccessKey），这一对Key用于RESTful接口鉴权。

规则如下：

* AccessKey生成规则：32位包含大小写字母和数字的随机字符串，唯一；
* SecretAccessKey生成规则：48位包含大小写字母和数字的随机字符串。
* 每个用户最多只能创建10对AKSK，并且同时只能有2对AKSK处于激活状态；

## Policy

策略定义为用户或组可以访问资源的访问控制列表，当用户或组请求访问某一个资源的时候，需要检查用户策略是否允许访问。

Policy遵循白名单策略。即：当为用户或组显式创建策略之后才允许该用户或者组内用户访问对应的资源。

用户和组创建成功之后，默认不具有任何策略，即用户不可以访问任何资源。

Policy只对用户和组产生作用，对账户不起作用，即账户默认具有对所有资源的操作权限。

## 权限和策略

### 权限分离

系统权限按照Service进行划分，再细分到单个Service下的接口。



### 最小权限

管理员用户默认具有系统全部Service访问和使用的权限，包括管理用户的权限。

普通用户默认不具有任何Service访问和使用的权限，只有管理员用户为其添加权限之后才具有对应的权限。普通用户不能具有管理用户的权限。

## 密码

管理员用户在创建普通用户的时候可以为其指定一个密码，该密码必须遵守下面的密码规则：

* 每一个用户都必须设定一个密码字段；
* 密码不能为空；
* 密码必须包含至少一个大写字母；
* 密码必须包含至少一个数字；
* 密码的长度至少为8位；
* 密码不能包含用户名；

## 证书

主要用于SOAP接口鉴权，待扩展。

# 数据安全

## SSL加密传输

IDM采用SSL方式加密传输，防止数据泄露。

## 安全访问数据库

数据库必须部署在内网环境下，并且设置为只能特定IP才可以访问。

## 创建安全的响应消息

API接口的响应消息中不能包含系统内部信息，包括系统各部件版本号、不宜扩散的内部错误信息等。

## 关键数据加密存储

对于账号密码这种关键数据，需要在数据库中加密存储，避免信息泄露。

# 接口安全

## 用户身份验证

当用户登录系统页面的时候需要验证用户身份，用户需要提供用户名和密码。IDM系统会对用户身份信息进行认证，只有合法用户才可以登录系统进行访问和操作。

用户客户端程序使用REST接口调用的方式使用系统服务的时候，同样也需要提供用户身份认证信息（AccessKey和SecretAccessKey），IDM对其进行认证，认证通过之后才对用户请求进行授权。

## 输入参数安全性检查

系统必须对用户请求参数进行安全性检查，确保用户输入是在合法范围内，避免出现SQL注入攻击等恶意入侵。

## 数字签名

数字签名用于REST接口验证，客户端在构造接口请求的时候，需要使用AccessKey和SecretAccessKey对请求参数进行签名，并将AccessKey和签名在请求参数中传递到服务端，SecretAccessKey无需传递到服务端。服务端接收到用户传递的AccessKey和签名之后，会对该请求进行一次同样的签名操作，然后对比两个签名，如果相同则认证通过，不同则认证失败。

## 请求失效时间

REST请求中必须包含时间戳，以避免Replay攻击。

系统默认用户请求5分钟后失效。

## 可信设备及访问

系统内部，只有可信设备才可以访问关键服务节点。

## 接口访问频率限制

接口限制用户每个小时只能请求一定的次数。限制分用户维度和IP维度，详述如下：

一、针对一个服务器IP的请求次数限制：120次/分钟；

二、针对一个用户在使用一个应用的请求次数限制：60次/分钟。

# 安全审计

## 流量审计

系统提供基于用户访问的流量分析功能，实时统计出当前系统中的各种用户请求和访问的数据流量，进行综合流量分析，为流量管理策略的制定提供可靠支持。

## 行为审计

系统提供全面的网络行为审计功能，根据设定行为审计策略，对网站访问、数据库访问、远程终端访问、数据传输、文件共享、接口调用等网络应用行为进行监测，对符合行为策略的事件实时告警并记录。

## 内容审计

系统提供深入的内容审计功能，可对网站访问、数据库访问、数据传输等提供完整的内容检测、信息还原功能；并可自定义关键字库，进行细粒度的审计追踪。