



上海震旦职业学院

统一身份平台（UIP）技术方案



上海龙盟信息科技有限公司

The Dcux Documentation Project Team <ddpt@dcux.com>

上海震旦职业学院：统一身份平台（UIP）技术方案

上海龙盟信息科技有限公司

The Dcux Documentation Project Team <ddpt@dcux.com>

版权 © 2015 上海龙盟信息科技有限公司

修订历史		
修订 1.0	2015年9月30日	ddpt
发布第一个Draft		

版权声明

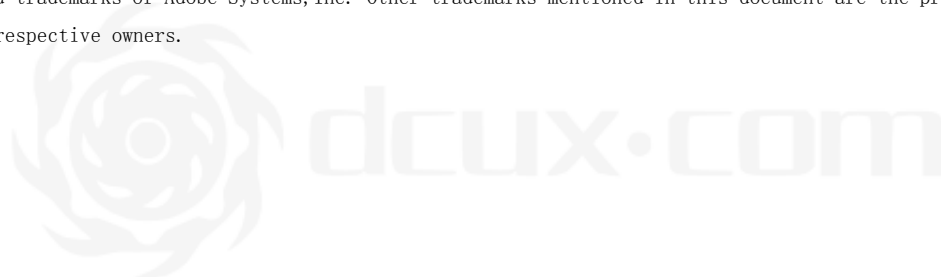
本文中出现的任何文字叙述、文档格式、插图、照片、方法等内容，在项目确定以前，除另有特别声明外，版权均属于上海龙盟信息科技有限公司，受到有关产权及版权法的保护。任何个人、机构未经过上海龙盟信息科技有限公司的书面许可，不得以任何方式复制或引用文中的任何片段。

商标声明

“dcux”、“unitforge”、“sepia”、“EventsMaster”、“osslab”为上海龙盟信息科技有限公司的注册商标，在未经上海龙盟信息科技有限公司的许可下，任何个人或机构不得使用。

Trademarks

“dcux”、“unitforge”、“sepia”、“EventsMaster” and “osslab” logos are registered trademarks of dcux.com Ltd. **dcux** and **dcux** logo are registered trademarks of dcux.com Ltd. PostScript and PDF are registered trademarks of Adobe Systems, Inc. Other trademarks mentioned in this document are the property of their respective owners.



目录

1 - 概述	1
1.1 - 项目背景	1
1.2 - 系统概述	1
2 - 如何工作	3
2.1 - 模块组成	3
2.2 - 工作流程	4
3 - 系统技术功能	8
4 - 特点和优势	9
4.1 - 集群化的设计	9
4.2 - 标准化的接口	9
4.3 - 丰富的SDK和丰富的User-Agent	10
4.4 - 详细的日志记录	10
4.5 - 高度的兼容性	11
4.6 - 科学的管理	11
5 - 系统配置	13



插图清单

2.1 - 系统工作过程	5
2.2 - 用户在浏览器中输入OA的URL	5
2.3 - UIP的授权页面	6
2.4 - UIP认证授权的URL说明	6
4.1 - 日志信息	11
4.2 - 添加应用	12



第 1 章 概述

1.1. 项目背景

随着信息化的迅猛发展，学校、政府、企业、机构等不断增加基于Internet/Intranet的业务系统，如各类网上申报系统，网上查询系统，OA系统等。系统的业务性质，一般都要求实现用户管理、身份认证、授权等必不可少的安全措施。而新系统的涌现，在与已有系统的集成或融合上，特别是针对相同的用户群，会带来以下的问题：

1. 如果每个系统都开发各自的身份认证系统将造成资源的浪费，消耗开发成本，并延缓开发进度；
2. 多个身份认证系统会增加整个系统的管理工作成本；
3. 用户需要记忆多个帐户和口令，使用极为不便，同时由于用户口令遗忘而导致的支持费用不断上涨；
4. 无法实现统一认证和授权，多个身份认证系统使安全策略必须逐个在不同的系统内进行设置，因而造成修改策略的进度可能跟不上策略的变化；
5. 无法统一分析用户的应用行为。

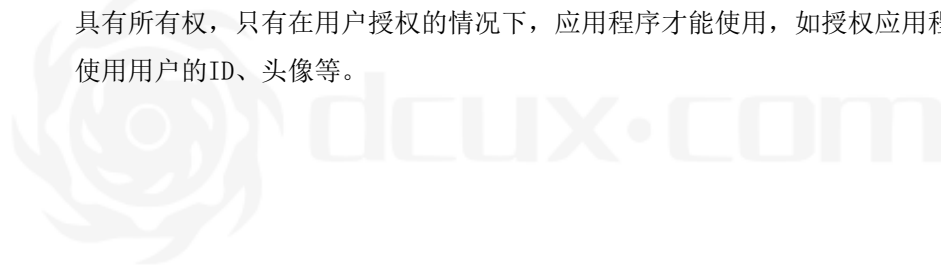
因此，对于有多个业务系统应用需求的学校、政府、企业或机构等，需要配置一套统一的身份认证系统，以实现集中统一的身份认证，并减少整个系统的成本。统一身份平台（UIP）的目的就是为这样的应用系统提供集中统一的身份认证，实现“一点登录、多点漫游、应用无关”的目标，方便用户使用。

1.2. 系统概述

针对上述状况，企事业单位或公司希望为用户提供统一的信息资源认证访问入口，建立统一的、基于角色的和个性化的信息访问、集成平台的单点登录平台系统。龙盟科技在此背景下研发了“统一身份平台”该系统具备如下特点：

1. **单一的用户信息存储系统：**无论网络中有多少个应用，都统一的使用一套用户系统，避免资源的浪费，减少维护的成本。
2. **单点登录：**用户只需登录一次，即可通过单点登录系统（SSO）访问后台的多个应用系统，无需重新登录后台的各个应用系统。

3. **登录和授权在授权服务器进行：**用户登录输入口令只对授权服务器可见，无需其他应用系统的参与，从而保证应用系统无法获取用户的密码，保证用户的安全。
4. **遵循OAuth2国际标准协议：**具有安全、灵活、简易、通用等特点，国内外知名企业都在使用，如阿里巴巴、腾讯、百度、Google、Facebook等等，协议内容参考见RFC6749。
5. **基于Web界面管理：**系统所有管理功能都通过Web方式实现。网络管理人员和系统管理员可以通过浏览器在任何地方进行远程访问管理。
6. **集群功能：**通过集群功能，提供高效、可靠的服务，提高系统的可用性，满足企业级用户的需求。并为将来系统的扩展做好充分的准备。
7. **多种后台用户数据库支持：**系统支持LDAP、MySQL、Oracle、MS-SQLServer、Radius等。可以无缝集成现有的用户数据库作为系统的用户数据库。
8. **全面的日志审计：**精确地记录用户的日志，可按日期、IP、用户、应用等信息对日志进行查询、统计和分析。审计结果通过Web界面以图表的形式展现给管理员。
9. **只有用户对自己的信息具有所有权：**用户信息数据库中的信息只有用户自己具有所有权，只有在用户授权的情况下，应用程序才能使用，如授权应用程序使用用户的ID、头像等。



第 2 章 如何工作

2.1. 模块组成

整个系统由以下模块组成：

1. 授权模块：

授权模块是整个UIP系统的技术核心部分，授权模块的功能如下：

- a. **应用授权：**接受来自应用的授权，并对应用进行验证，甄别非法的应用并拒绝其接入；
- b. **用户授权：**提示用户对应用进行授权访问，如果需要登录，则将用户导向认证模块；
- c. **发放授权码：**在应用和用户授权通过后，发放授权码给应用，提示应用该用户认证通过。

2. 资源模块：

资源模块是存储用户信息的地方，例如：用户的ID、密码、头像及工号等信息。我们可以理解为用户信息数据库。在默认情况下，UIP使用LDAP（OpenLDAP）或MySQL做为资源模块。此模块扩展容易，也很容易使用其他的数据库，如Radius、Oracle、MS-SQL等。

3. 系统管理模块：

这个模块主要是对系统中的一些配置选项进行管理，主要功能如下：

- a. **应用管理：**主要管理应用的相关属性。应用的属性主要有ID，名称，LOGO，URI，类型等。管理员能对应用进行添加，修改和删除；
- b. **认证管理：**对认证接口的管理，如果选择LDAP认证，则管理LDAP服务器的地址，用户和密码；
- c. **资源管理：**对资源接口的管理，如果选择数据库，则管理数据库的地址，用户，密码；

d. **用户管理**：管理能对本模块进行操作的用户。

4. 日志管理模块：

这个模块主要是对系统中产生的日志进行记录，并通过SYSLOG接口发送到制定的syslog服务器中。主要记录的日志类型如下：

- a. **应用授权日志**：记录每个应用接入授权模块的时间，接入IP地址；
- b. **用户日志**：记录用户在何时，何地，访问了何种应用的日志；
- c. **资源日志**：记录每个应用访问资源的时间，访问了何种资源。

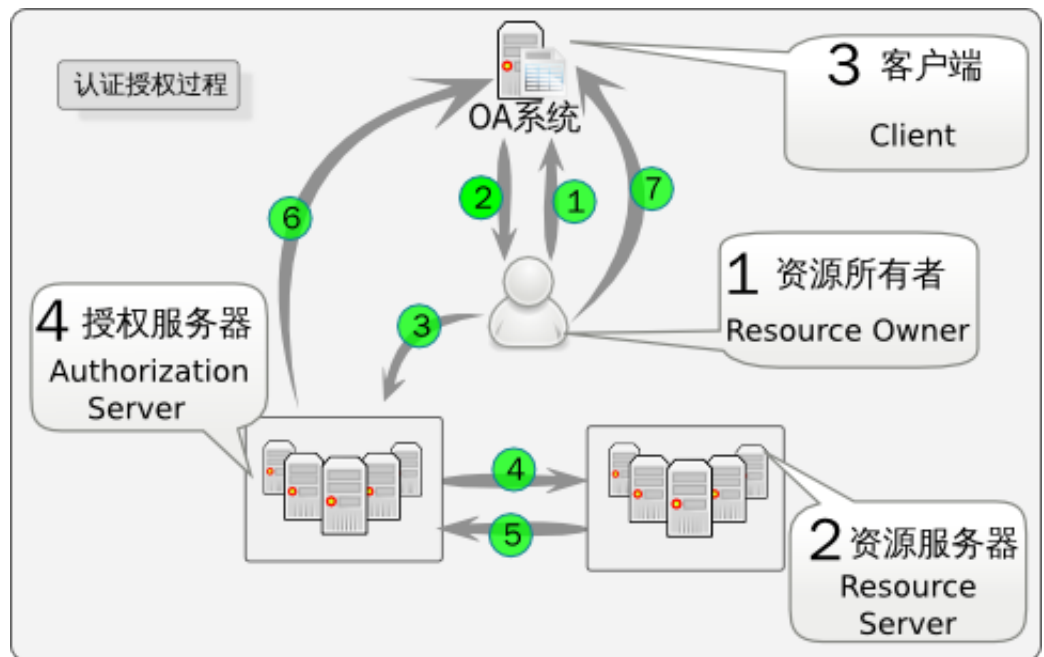
2.2. 工作流程

一个完整的流程是从一个应用在网络中注册开始的，开发人员首先需要获得管理人员的授权，并为其应用颁发一个唯一的密钥，开发人员的应用使用该密钥与UIP系统通信。应用可以是桌面应用、手机App、及其他智能设备。应用开发完成后便进入系统，投入使用。

UIP是一套功能完备的用户授权系统，采用了业界广泛使用的OAuth2.0协议、session共享机制、集群机制等先进的技术和标准的产品。它不仅在功能上可以完全满足用户的需求，而且在安全性、稳定性及可扩容性方面都做好了充分的准备。

整个系统一个简明的的工作过程如下：

图 2.1. 系统工作过程



1. 用户访问应用（OA系统），在浏览器中输入OA的地址，在OA系统的页面上会出现一个需要授权的图标

图 2.2. 用户在浏览器中输入OA的URL



2. OA系统告诉用户先到UIP系统进行认证，当用户点击授权的图标，就会被重新定向到UIP的授权页面

图 2.3. UIP的授权页面



上图中的url解释如下:

图 2.4. UIP认证授权的URL说明



3. 用户到UIP系统进行认证, 输入自己的帐号和密码
4. UIP接收到用户的请求, 将用户信息提交到“用户信息系统”进行验证
5. 在用户信息正确的情况下, “用户信息系统”告诉UIP, 用户合法
6. UIP系统将这一信息通知OA系统

7. 用户开始使用OA系统



第 3 章 系统技术功能

龙盟科技的统一身份平台是一套功能完备，具有很强扩充能力的系统。她的主要功能和优点如下：

1. 软件能够跨平台实施，在windows，linux和Unix都能实施；
2. 使用OAuth2.0技术标准；
3. 单点身份认证接口采用URL参数传递方式；
4. 在认证通过后采用JSON文本将用户资源传递给接入应用；
5. 支持TLS/SSL加密传输；
6. 支持设置授权过期时间；
7. 设置详细的排错参数，以便能够调试接口；
8. 授权接口的授权码采用数字加密方式，这种方式很难被非法用户猜测；
9. 认证接口支持基于LDAP，数据库的认证；
10. 资源接口能够支持LDAP，数据库资源的分发；
11. 软件平台采用PHP，Apache/Nginx, Mysql的平台，这个平台比较流行，部署方便、简单；
12. B/S设计方式，无须客户端，使用浏览器即可管理和使用整个系统；
13. 支持多种日志记录，能完全把握用户的访问趋势，日志支持syslog；
14. 统一的应用管理模块，能够方便的接入应用；
15. 完备的文档系统，系统首页显著位置放有我们的API文档和各类技术说明文章，方便接入应用的开发；
16. 支持WEB应用、Javascript应用、桌面应用的接入、手机APP，涵盖了主流的应用；
17. 支持用户信息安全保护，保护用户信息不会被非法的应用和用户窃取。

第 4 章 特点和优势

4.1. 集群化的设计

UIP本身采用了集群化的设计，无论是在一个简单的网络中做单台的部署，还是在大规模的网络中的做集群式的部署，UIP都能够应对自如。

1. 高可用机制

UIP的底层自带了一套完善的集群机制，在小规模的网络中可以单台部署，在大规模的网络中也可以集群式部署。由多台UIP组成的集群可以更稳定、更高效的为网络用户服务。

用户使用统一的域名或IP地址访问整个集群，整个集群在外面看来就是一台机器，只有一个访问的入口。当集群中的某台机器出现宕机或服务不可用的状态，其他的服务器会自动接管其服务，从而使整个集群保持稳定；在流量高的情况下，集群中的每台服务器会均衡的处理流量，让服务更加的高效。

2. 先进的current session remains（当前会话保持）机制

在用户的访问被定向到集群中的某台机器时，用户的会话（Session）就会被保存在这台机器上，记录下用户当前的状态，如果这时这台服务器突然宕机，用户就会出现“掉线”的现象，UIP采用了会话保持机制，避免了这种情况的发生。在用户使用UIP时，他的会话会被系统写到集群中的每台服务器上，如果有某台在线的服务器出现宕机，接管其服务的机器会正确的识别用户的状态，让用户毫无察觉的、平滑的使用系统。

保存Session的区域称为Session Pool，Session Pool是独立的，以Socket端口的形式提供Session的保存服务，很容易将这部分安装在独立的机器上，如存储系统中。从而使整个系统更加的健壮。

4.2. 标准化的接口

UIP严格的遵循了Oauth2等相关的RFC标准，为开发人员提供了完善的、标准的、有限的接口，容易使用，而且学习成本极低。

1. 请求授权接口： `authorize`，通过这个接口应用程序向UIP发起授权的请求；
2. 获取授权接口： `token`，通过这个接口应用程序向UIP获取使用用户信息的权利及权利的大小；

3. 读取用户接口: `resource`, 应用程序获取授权后通过UIP读取用户的相关信息;
4. 帐号登出接口: `logout`, 登出应用程序的接口。

4.3. 丰富的SDK和丰富的User-Agent

UIP已经为应用系统开发人员准备好了丰富的SDK, 这些SDK只需要稍微的修改下与自己系统相配的配置文件, 就可以直接使用, 目前已经包含了如下的开发语言: PHP、Java、.Net、ASP等。

UIP系统主要支持三种应用的授权接入, 这三种应用也是当前主流的应用类型。

1. WEB应用

WEB应用的特点是有WEB服务器端, 有固定的URI地址。

2. Javascript应用

Javascript应用没有WEB服务器, 运行在浏览器端。

3. 桌面应用

桌面应用是运行在pc或移动终端中的桌面客户端。

4. 手机App






支持各种手机应用的开发包括Apple和Android。

4.4. 详细的日志记录

UIP提供了功能完备的日志记录功能, 能够详细的记录用户的登录信息, 主要包括: 用户登录的时间、应用、用户IP地址、使用的操作系统、浏览器等。

图 4.1. 日志信息

用户登录信息日志报表					
登录时间	应用名称	帐号	用户IP	操作系统	浏览器
2012-11-19 17:26:24	管理客户端	Admin	192.168.3.95	Linux	Chrome
2012-11-05 10:46:10	信息门户	Admin	192.168.4.129	Linux	Mozilla
2012-11-05 10:44:35	信息门户	Admin	192.168.4.129	Linux	Firefox
2012-11-05 10:38:58	信息门户	Admin	192.168.4.129	Windows XP	Firefox
2012-11-05 10:37:19	信息门户	Admin	192.168.4.129	Windows XP	Mozilla
2012-11-05 10:36:51	信息门户	Admin	192.168.4.129	Windows XP	Opera
2012-11-05 10:33:53	信息门户	Admin	192.168.4.129	Windows XP	unknown

 15    Page 1 of 6  显示 1 ~ 15 共83

4.5. 高度的兼容性

UIP可以与现有的多种用户信息数据库对接，包括Radius、LDAP等认证数据库及Oracle、MySQL、PostgreSQL、SQL-Server等传统的关系型数据库。这一特点极大的方便和简化了UIP的部署，使其使用成本和部署成本大大的降低，并且保护了原来的投资。

4.6. 科学的管理

UIP采用了一种安全的、科学的管理机制，保证所有接入UIP系统的应用都是可信的。一个应用系统在加入到UIP之前首先要经过开发人员的申请并且要通过管理人员的审核。管理人员会为每个应用系统分配一个唯一的ID、一个随机生成的密钥。这种机制既要经过人工的特定流程，又在UIP和应用系统之间加入了密钥安全机制，保障了整个系统的安全和管理的方便性。

图 4.2. 添加应用

客户端标识符	<input type="text" value="OA"/>	32字符以内
客户端密钥	<input type="button" value="随机生成"/>	
客户端名称	<input type="text" value="OA"/>	50字符以内
客户端类型	<input type="text" value="WEB应用"/>	
客户端描述	<input type="text" value="办公自动化系统"/>	1000字符以内
重定向地址	<input type="text" value="oa.dcux.com"/>	255字符以内
资源访问域	<input type="text" value="uid"/>	255字符以内
客户端地址	<input type="text" value="http://oa.dcux.com"/>	255字符以内
客户端LOGO路径	<input type="text" value="http://oa.dcux.com/oa_logo.png"/>	255字符以内
在首页显示	<input type="text" value="否"/>	

[创建](#) [返回](#)

第 5 章 系统配置

综合考虑整个系统的成本、安全、易扩容及兼容性，建议底层的操作系统和一些基础软件采用开源的系统，一个建议的配置如下：

1. 操作系统: Debian Linux 8.0
2. 资源服务器: MySQL 5.7
3. Web服务器: Nginx 1.9.X (with PHP 5.6.X)
4. UIP: 龙盟UIP 2.0

