doi: 10.3969/j.issn.1006-1576.2011.08.014

企业信息门户单点登录和信息集成

董新风[1,2]，李保国[2]
（1. 沈阳理工大学，沈阳 110168；2. 西安北方光电科技防务有限公司，西安 710043）

摘要：针对企业用户登录不同应用系统时操作处理不便的问题，介绍了一种基于统一认证、单点登录和信息集成的企业信息门户的设计方法。经过企业信息门户的统一用户认证和 SSO 登录后，通过基于用户映射的认证方式，在不同登录方式的应用系统中实现了单点登录。并利用 Ajax 技术、Web 动态语言技术实现了跨域和非跨域的信息集成。在北方光电公司的系统中应用结果表明：该方案能实现多系统的单点登录和跨域信息集成与整合，大大提高操作的方便性。

关键词：企业信息门户；统一认证；单点登录；信息集成；Ajax；用户映射
中图分类号：TP393.02 **文献标志码**：A

Single Sign On and Information Integration of Enterprise Information Portal

Dong Xinfeng[1,2], Li Baoguo[2]
(1. Shenyang Ligong University, Shenyang 110168, China;
2. Xi'an North Opto-Electronic Science & Technology Defence Co., Ltd., Xi'an 710043, China)

Abstract: Log in various applications for business users deal with the inconvenience of operating system problems, a novel based on a unified authentication, single sign-on and integration of information enterprise information portal design. After the unified enterprise information portal user authentication and single sign on (SSO) login, map-based user authentication, application in different login system to achieve a single sign. The use of Ajax technology and Web technology achieve cross-domain dynamic languages and non-cross-domain information integration. The application system of north opto-electronic Co., Ltd. shows that the scheme can realize multi-system and cross-domain single sign information integration and integration, greatly improving the convenience of operation.

Keywords: enterprise information portal; unified authentication; SSO; information integration; Ajax; user mapping

0 引言

现代企业内部建立很多应用系统，如电子邮件、办公 OA、ERP、PDM、档案系统等。这些系统往往有着独立的用户认证模块和机制，用户需要分别登录每一个系统。且用户要处理的业务信息分散在各应用系统中，需要来回切换系统才能进行查阅和办理，给用户的使用造成诸多不便。目前，基于单点登录（single sign on，SSO）和信息集成的企业信息门户（enterprise information portal，EIP）成为最终解决方案。用户只需登录一次信息门户，就能自动完成对各个应用系统的单点登录，而且该用户在各应用系统中的待处理事务和所关注的信，用户可以直观地看到需要处理的全部信息，并根据事务的轻重缓急直接进行处理。

要建立一个这样的企业信息门户，需要解决 2 个关键问题：一是实现单点登陆；二是实现信息集成。目前有很多企业信息门户的实现方案，其中常见的单点登录认证机制有：Kerberos、PKI、KryptoKnight 等，常用的技术有：Web Service、Cookie 等。在单点登录系统的实现过程中，往往会碰到如下问题：1) 企业现有的各个应用系统间相互独立或者通信状况混乱，对外接口也不同，给应用系统的集成带来了极大困难；2) 同一个用户，拥有多个应用系统的访问帐号，使用户信息难以统一管理；3) Cookie 不能跨域的限制也使实现各个应用系统之间 Cookie 共享成为一个难题。信息集成是在实现 SSO 的前提条件下进行的，主要的问题是访问权限和跨域信息集成问题。目前，大多数门户系统仅仅实现了单点登录，对于信息集成仅仅做到对公用信息的集成。因此，笔者介绍了基于 Ajax 和 Web 应用原理，绕过 Cookie 跨域的限制，采用用户映射机制设计的单点登录和对跨域信息集成的方案，以解决上述问题。

1 设计方案

企业信息门户主要包含统一认证、单点登录和信息集成 3 部分。统一认证系统主要功能是：用户访问 EIP，首先要进行系统登录，统一认证系统根据用户提供的登录信息，进行身份验证，如果通过验证，返回给用户一个认证的 EIP 凭据；然后系统对通过认证的 EIP 用户进行单点登录操作。单点登

收稿日期：2011-05-16；修回日期：2011-06-07
作者简介：董新风（1976—），男，陕西人，硕士研究生，工程师，从事决策支持应用研究。

录的主要功能是：根据门户系统用户映射表中维护的 EIP 用户在各应用系统的用户名及密码，自动在系统底层完成对各应用系统的登录，由各应用系统分别进行授权并向客户端浏览器发送允许票据 Cookie。信息集成部分的主要功能是：将用户在各应用系统中的待处理事务和用户所关注的公共或私有的信息经过提取和格式化处理后，集中显示在用户的门户页面上，提供给用户进行快速查阅和办理。上述过程对用户是透明的，用户看到的是登录了企业信息门户，自己在各系统中需要办理和关注的信息便集中显示在门户页面中了。整个企业门户系统的结构如图 1。

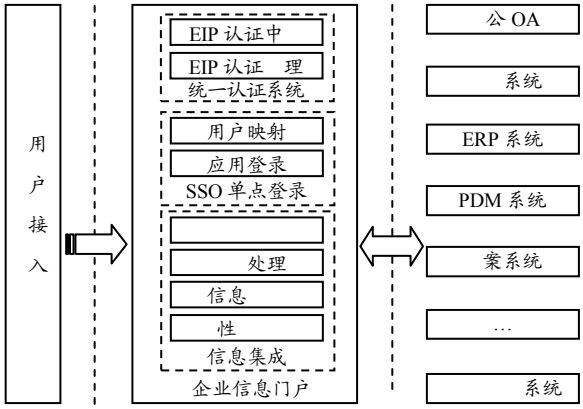

图 1　企业信息门户结构图

1.1　统一认证

统一认证中心提供系统的认证服务和用户管理，但并不包括集中的授权和会话的管理，授权和会话的管理依赖于各应用系统本身。其主要功能是：向所有应用系统提供认证服务和入口，提供用户调用接口和用户基本信息服务，同时提供对认证系统管理功能。EIP 认证中心的用户包含全部应用系统的用户，是所有应用系统用户的并集。每个应用系统的登录认证机制可能各不相同，要根据具体情况而定。对于已经上线运行的应用系统，由于这些系统往往有着独立的认证机制，而且有很多业务流程涉及到用户信息，单点登录的实现应尽量不影响这些应用系统的原认证模块；对于新的应用系统，则可以完全由信息门户来接管用户身份的认证。总的来说，在信息门户中，单点登录只负责决定用户能否进入某个应用系统，而用户对应用系统资源的访问权限则由各应用系统独立控制。

1.2　单点登录

用户登录信息门户经过统一认证中心认证通过后，系统就进行 SSO 单点登录。SSO 模块包含用户映射和单点登录 2 部分。

1.2.1　用户映射

将用户在各应用系统的用户名和密码经过加密后保存在 EIP 系统用户映射表中，如表 1。该部分包含一个应用系统注册模块和一个应用用户注册模块。对于加入单点登录的每一个应用系统，系统管理员会为其注册一个全局唯一的应用 ID 并设置对应的认证接口，然后初始化用户映射表。初始化的主要工作是导入各应用系统与认证相关的主要信息（如用户名、密码等），并与 EIP 用户 ID、应用 ID 进行关联，以后新增的用户可以通过用户注册模块进行注册。

表 1　用户映射表

EIP 用户 ID	应用 ID	用户		
dongxinfeng	OA 系统	dxfeng	******	90ac7cd9ad2d0e
dongxinfeng	系统	dxf	*********	null
dongxinfeng	ERP 系统	dongxf	*****	23e3a76cd8a0ea
dongxinfeng	PDM 系统	xinfengdong	*******	null
dongxinfeng	案系统	dxf	********	null

1.2.2　Form 表单的单点登录

这种登录机制是针对那些基于浏览器的 Form 表单方式的 Web 应用系统设计的，不需要对应用系统的原有认证模块作任何修改。在用户通过 EIP 认证中心登录认证通过后，系统根据用户映射表中对应的应用 ID、用户名和密码，自动向用户浏览器生成 Ajax 程序代码，在客户端由 Ajax 通过底层模拟 form 表单向应用系统登录模块提交登录请求，应用系统登录模块根据提交的用户名和密码进行登录校验，若用户名和密码正确，返回登录成功的信息包，并向客户端浏览器写入允许票据 Cookie，建立会话；否则返回登录失败的信息包。Ajax 程序根据返回信息包中的 URL 或 Html 信息判断是否登录成功。

1.2.3　非 Form 表单的单点登录

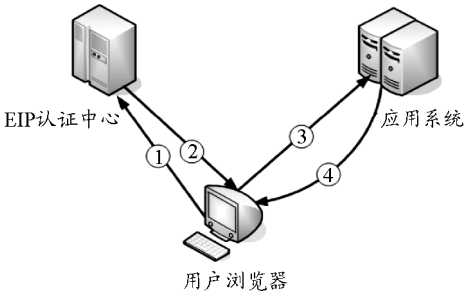

图 2　常规单点登录图

这种登录方式如 Domino 应用系统、ftp 应用等比较常见，它没有 form 登录页面，不能运用模拟表单提交的方式登录。因此，需要运用 Xmlhttp 模拟浏览器提交访问请求，通过 Xmlhttp.Open 携带用户

名和密码向目标应用系统发送访问请求，并通过 Xmlhttp.Status 来获得返回状态，如果状态等于 200，表示用户名和密码正确，登录成功，应用系统会向客户端浏览器写入允许票据 Cookie，建立会话。以上 2 种登录均属于常规单点登录，如图 2。

1.2.4 对单点登录的改造

对某些应用安全性要求比较高，不希望用户帐号密码在外部服务器上存放或在网络上传输，要实现这些应用的单点登录，可以对应用系统的认证模块进行少量改造。使应用系统能够访问认证中心用户密钥来验证用户真实身份，以此作为安全凭证为用户授权访问系统资源。

具体过程是：1) 用户登录信息门户，由 EIP 认证中心随机生成 32 位的一次性密钥，并保存在数据库映射表中；2) 系统携带该密钥向应用系统改造过的认证模块发送登录请求；3) 应用系统认证模块接收用户密钥后连接 EIP 系统数据库与映射表中存储的用户密钥进行核对，如果密钥正确，则表明该用户是登录 EIP 成功的合法用户；4) 清除映射表中该用户的密钥，应用系统开始进行授权，向用户客户端浏览器生成允许票据 Cookie，建立会话。改造后的单点登录如图 3。

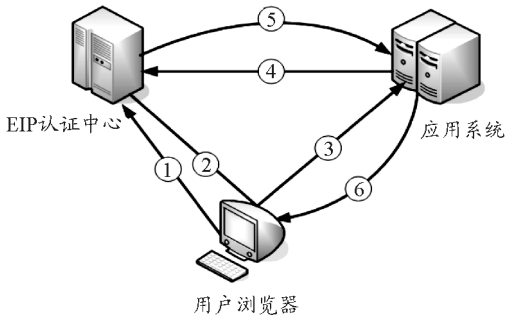

图 3 改造后的单点登录图

1.2.5 单点登录注销

由于实现单点登录的系统比较多并且登录方式多样，有基于 Form 认证的应用系统、也有基于非 Form 认证的应用系统等，为了便于企业信息门户的快速部署和实现及简化操作起见，笔者建议对各应用系统不做逐一注销，用户只需关闭全部浏览器窗口即可完成所有应用系统的注销。

1.3 信息集成

信息集成主要包含对各应用系统的公共信息和个人待办事务、待审批流程、邮件、消息等私有信息的集成。公共信息是与用户无关联性的、允许所有用户浏览的公共性信息，而待办事务、待审批流程、邮件、消息等属于用户私有信息，与用户有关联性。信息集成一般有 2 种方式：第 1 种是数据库级集成，就是通过门户服务器端直接访问应用系统的数据库来获取需要集成的数据，这种方式的优点是不受用户客户端浏览器环境的限制，但缺点是需要单独开发业务处理逻辑，而且门户服务器直接操作应用系统的数据库，存在很大的安全风险；第 2 种方法是应用级集成，就是通过调用应用系统已有模块功能进行信息集成，这种方式的最大优点是不需要开发业务逻辑，直接利用应用系统的功能模块，且不直接访问应用系统的数据库，不存在安全性问题。缺点就是此方式需要先实现单点登录，若解决了单点登录的问题，信息的集成就能够快速实现。根据前文单点登录结论，笔者采取第 2 种信息集成方式即应用级集成，来实现信息的集成。

企业中各应用系统的访问域名各不相同，有些还是通过 IP 地址或端口号来访问。因此，信息集成一般都存在跨域的集成问题。对于跨域信息集成的问题可以通过 2 种方式解决：一是对于公共类信息的集成，可以是动态程序语言(如 java、.net 等)通过服务器端进行数据集成；二是对于用户私有类信息，因为需要用户会话票据才能访问，因此需要使用 Ajax 通过客户端进行信息集成。具体实现的过程是：根据集成的业务需要，使用 java 等动态 Web 技术或 Ajax 技术为每个应用系统开发出多个 webapp 模块，将这些模块集成在信息门户中，分别用来提取用户的待办事务、邮件、订单等私有信息和用户关注的公共资讯类信息。用户可根据自己在信息门户中的角色权限进行个性化定制，选择不同的 webapp 模块，将自己需要的或关注的信息集中显示在信息门户中，方便自己进行查阅和直接办理。

2 系统实现

根据上述设计方案，笔者通过 Tomcat6.0 + JSP + Mysql5.1 对内部 Domino 的 OA 系统、邮件系统、Oracle 的 ERP 系统、PDM 系统、档案系统等描述实现过程。

2.1 准备工作

搭建 Tomcat 的 Web 服务器和 Mysql 数据库，创建 EIP 用户表 EIPUser 和用户在各应用系统的映射表 UserMap，并初始化用户数据，将用户在各应用系统中的用户名和密码导入到映射表中。

2.2 SSO 的实现

编写 Ajax 的客户端单点登录函数 SSOLogin，JSP 程序根据 EIP 用户 ID 从映射表中取出该用户的

全部记录，将应用 ID、用户名和密码传递给 SSOLogin 函数，并向客户端浏览器生成 Ajax 代码，由客户端执行该代码。以下是其中实现 SSOLogin 的部分代码：

```
function SSOLogin(app,user,password){
//登录各应用系统，成功返回 true,否则返回 false //
//app 是应用系统标识 ID。如 oa erp pdm bbs 等 //
//user, password 是用户在应用系统的用户和密码//
switch (app){
  case "oa":  //非 form 表单单点登录
  requrl="http://oa.abc.com";  //目标应用地址
  xmlHttp.open("GET", appurl, false, user, password);  //向目标应用发送用户名和密码
  xmlHttp.send();  //发送请求
  if(xmlHttp.status==200)  //判断返回状态
    return(true);  //登录成功
  else
    return(false);  //登录失败
  break;
  case "erp":  //form 表单单点登录
  requrl="http://erp.abc.com/login.jsp?u="+user+"&p="+password;
  xmlHttp.open("GET", appurl, false);
  xmlHttp.send();
  var rtxt=xmlHttp.responseText; //接收返回内容
  if(rtxt.search("<!--OK-->")!=-1) //判断返回内容中是否是登录成功页面
    return(true);  //登录成功
  else
    return(false);  //登录失败
  break;
  }
}
```

2.3　信息集成的实现

在实现 SSO 登录后，由于各应用系统已经向用户的客户端浏览器写入允许票据 Cookie，用户再次访问这些应用系统时，就不会弹出用户名密码了。因此，针对要集成的各应用系统，开发不同的 webapp 应用包，并将其添加在用户的信息门户中。用户的浏览器通过执行这些应用包程序就可以提取出相应的信息，经格式化后显示在信息门户页面的指定区域。另外，信息门户支持用户个性化设置功能，用户可以根据系统权限自由选择 webapp 应用包，按照自己的需要定制要集成的内容。其中的一个应用包的部分代码为：

```
function webapp(){
//集成办公 OA 公文信息，提取需要的数据 //
  var str,infourl
  infourl="http://oa.abc.com/info.nsf/msg?OpenView&Start=1&Count=5&end"  //要提取内容的 url 地址
  xmlhttp.open("GET",infourl,false)
  xmlhttp.send()  //发送请求
  str=xmlhttp.ResponseText
  str=str.substring(str.indexOf('<!--Start-->'), str.indexOf('<!--End-->'))  //截取有用的数据部分
  document.write(str)
}
```

如图 4，该方案已在北方光电公司企业信息门户中被成功应用。该信息门户实现对企业内部办公 OA、ERP、PDM、档案等应用系统单点登录，并将当前用户在各系统中的待办事务及邮件、公告公文、资讯等信息分类显示在门户中。

图 4　企业信息门户

3　结束语

该方案不需对应用系统做任何改造或只做少量改造，即可实现对不同登录方式的应用系统的单点登录及信息集成。该方案对于快速实现多系统单点登录与信息集成，整合企业资源、建立企业信息门户系统有一定的参考价值。

参考文献：

[1] The Open Group Single Sign-On [EB/OL] [2008-07-21]. http://www.opengroup.org/security/sso/

[2] , , , . 中实现 认证的单点登录[J]. 计 与 , 2008, 36(2): 85-87.

[3] , . 基于用户映射 CAS 单点登录系统设计与实现[J]. : 理 大 2009, 04.

[4] , , , . 技术中的通信[J]. , 2010, 31(8): 97.

[5] , , , . 一 Web 单点登录系统的 与实现[J]. : 大 信息 , 2007, 18(102).

[6] . 单点登录系统的 与 [D]. : 技大 , 2007.