Software Engineering and Applications 软件工程与应用, 2013, 2, 109-117
http://dx.doi.org/10.12677/sea.2013.25020 Published Online October 2013 (http://www.hanspub.org/journal/sea.html)

The Practice of Academic Administration Information Portal and Single Sign-On Design Integration

Mingtzau Lin, Chungkai Liu

Computer Center, Taipei National University of the Arts, Taipei
Email: mtlin@tnua.edu.tw, chongkai@tnua.edu.tw

Received: Aug. 13th, 2013; revised: Aug. 19th, 2013; accepted: Sep. 10th, 2013

Abstract: This paper mainly introduces the self-development of the integration of Single sign-on (SSO) and Enterprise Information Portal (EIP) for academic administration information system of Taipei National University of the Arts (TNUA). The purposes are to share the practical systems experience regarding EIP and email SSO, improve the convenience for using academic administration information systems including academic information system, student affairs system, human resource information system, email, information inquiry, etc. Besides, it could substantially reduce the development cost by applying the Open Lightweight Directory Access Protocol (OpenLDAP) theory and the developing system language could also support LDAP Application interface to efficiently revise system recognition mechanism to reach the SSO development. The key processes for this whole design include account management, data design and construction for Lightweight Directory Access Protocol and LDAP, application program interface (API) for LDAP, account opening system, and account integration design.

Keywords: Single Sign-On (SSO); Enterprise Information Portal (EIP); Lightweight Directory Access Protocol (LDAP)

校务行政资讯系统单一签入与帐号整合之实作

林明灶，刘仲凯

国立台北艺术大学电子计算机中心，台北
Email: mtlin@tnua.edu.tw, chongkai@tnua.edu.tw

收稿日期：2013 年 8 月 13 日；修回日期：2013 年 8 月 19 日；录用日期：2013 年 9 月 10 日

摘　要：本文主要描述国立台北艺术大学(Taipei National University of the Arts, TNUA)，在自主开发建置单一帐号签入统整各校务行政资讯系统的过程架构及方法。以分享系统实务流程经验，建构整合校园行政系统资讯入口(Enterprise Information Portal, EIP)，及学校 e-mail 单一帐号登入(Single sign-on, SSO)，便利使用教务系统、学务系统、人事系统、电子邮件、资讯查询等各项校园资讯系统，提供实务开发经验分享应用。开发流程重点于帐号管理设定、轻量级目录存取协定(Lightweight Directory Access Protocol, LDAP)资料架构设计及建置、LDAP 应用程序接口、帐号开启系统及帐号整合机制规划。运用 OpenLDAP 原理延伸目录服务管理大幅降低软体建置成本，且资讯系统的程序开发语言皆有支持 LDAP API，迅速修改系统认证机制，达成单一登入之开发。

关键词：单一帐号登入；校园行政系统资讯入口；轻量级目录存取协定

1. 引言

大学校务系统的开发管理与经营控管，对于大学行政绩效的提升，具有关键性的影响。数位化校园建设中行政系统资讯化，不同时期陆续开发完成教务资

讯系统、学务资讯系统、人事资讯系统、总务资讯系统与招生试务系统及其它相关子系统等建置更新作业，以提升教务处、人事室、学务处、推广教育、总务等行政效率与服务品质，及资料库整合之即时及一致性作业，提供各项资讯自动化作业、管理报表及报部报表。校务行政资讯系统均需要使用者键入帐号密码进行认证，认证通过后，各系统针对登入的帐号进行授权，取得相对应的功能与权限[1]。但开发过程中，各系统的帐号因无相互整合，使用者就需要针对每个系统去进行帐号的建立(如以身份证字号、email 帐号、学生学号或个别帐号等)，密码的设定。系统增加，相对需记忆之帐号密码亦增加。因此对使用者帐号密码管理是困扰的。当人员资料异动时，需以非资讯化机制如书面或定时管理帐号资料。可能面临的困难点，于各系统帐号的不同、资讯系统上线而无法全面修改帐号、开发程序语言不同及委外系统厂商的经验与配合度。因此统整各应用系统的帐号，使用单一组帐号密码登入如图 1 于各应用系统是必需的。

企业入口网站(EIP)及单一帐号签入之开发，以目前学校校园及企业界为例，多以厂商外包方式协助开发，在系统整合过程中厂商虽有标准化作业流程，与充足之经验，但开发费用接近 10 万美金以上之要求，每年至少需 10%以上之维护费用，且委托单位面临程序无法自主及核心技术无法获得，新系统开发之介接仍需依赖于厂商，厂商之资讯人员异动频繁常造成技术衔接有代沟，时效管理都有所延迟。自主开发除了能节省开发费用，效能与功能符合业务单位需求，且能精进各系统开发人员之技术能力，亦能熟稔系统之实质架构。需挑战的是系统与 EIP 整合之协调沟通，及资讯安全之设计。

EIP 及 SSO 之发展已近十余年，相关论文着重于单一学术主题讨论，帐号管理关键技术在于使用轻量级目录存取协定 LDAP[2-5]，经研究厂商使用之 LDAP 技术，区分为 AD (Windows)、eDirectory (Novell)、Directory Server (IBM)及 OpenLDAP，经由评估其优缺后选用 OpenLDAP，因为免授权费用与开放式源始码(Open Source)及效能可以应付教职员生共约 3000 人，与功能符合需求。目前 SSO 之 LDAP 技术及应用程序技术(Application program interface, API)多为开发厂商之核心技术，而无法取得相关开发之报告，本论文在

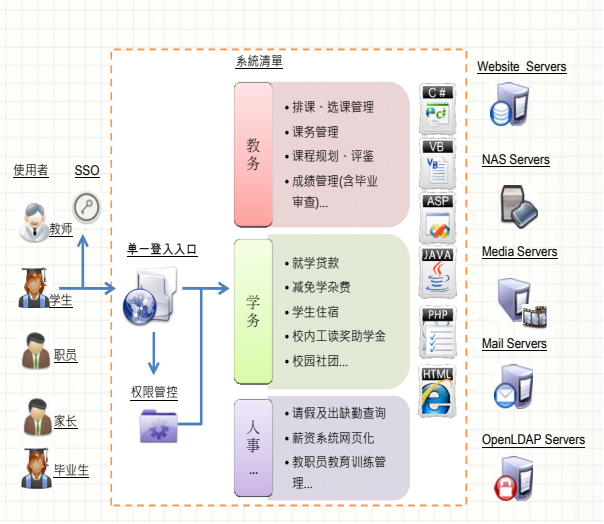

Figure 1. The architecture diagram of academic administration system and SSO
图 1. 校务系统单一签入架构规划图

于本校全面性自行开发与研究 EIP 与 SSO，得就开发之成果得以呈现与揭露核心技术于论文，并广为推广学校与企业应用。

本论文主要三大工作为目录服务、单一登入(SSO)服务及个人化入口网站(Portal)：

1) 目录服务：建立与教务与人事资料同步的身份识别资料，整合现有资讯系统帐号，提供以 LDAP 或 Web Service API 服务。

2) 单一登入(SSO)服务：以帐号、密码同步或至目录服务服务器作认证进行单一签入，存取所有系统。

3) 个人化入口网站(Portal)：将所有系统的讯息统一集中到 Portal，并建立各系统子选单(Portlet)，用户只须登入到 Portal，便可存取内部被授权的各类资源。

2. SSO 帐户资讯管理机制

目前于各资讯系统的帐号大致可以区分为 Email、学生学号、身份证字号、个别帐号如表 1 所列，为达成单一签入式登入帐号，因考虑外籍人士无法取得身身份证字号，规划以 Email 帐号为统一的帐号。

综合 SSO 业界整合技术分为 2 种及共同合并使用，其运作模式如图 2 所示：

1) 使用者帐号资讯存放于目录服务系统如 LDAP、AD (Active Directory)，目前业界厂商如 Direk Tech Inc.、Novell、IBM 大都以目录服务系统来开发 SSO 相关产品。

2) 使用者帐号资讯存放于资料库(DB)系统如

Table 1. Login account information system with the use of classification
表 1. 资讯系统与使用登入帐号分类表

登入帐号	资讯系统
Email 帐号	无线网路、webmail、数位学习、总务系统……
教职员身分证、学生学号	教务系统、学务系统、挂失系统、图书馆系统……
教职员身分证	出纳系统、招生系统、人事系统……
个别帐号	官网、电子公文、数位典藏……

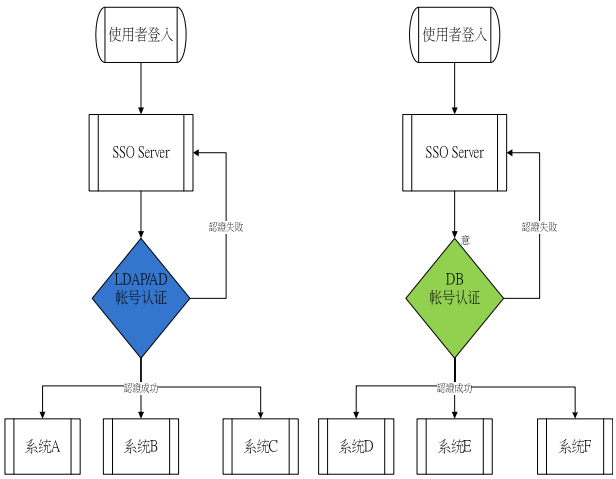

Figure 2. The account authenticate methods of SSO information system
图 2. SSO 帐户资讯管理认证方式

MSSQL、Oracle、MySQL，目前业界厂商如状态网际网路大都以资料库系统来开发 SSO 相关产品。

比较分析学校各资讯系统的属性后，使用者帐号资讯存放于 LDAP 及 DB 共同合并使用，若系统无法以 LDAP 进行帐号认证时，则将采取使用帐号资讯存放于 DB，其中 DB 俱有之优点：DB 容易与各资讯系统进行资料交换与资料同步。帐号资讯存放于 DB 容易被各系统的开发语言所使用，资料的备份与备援机制健全。使用资料库存放使用者资讯可自由快速的附加其它栏位属性，无需重新启动服务，扩充性与便利性较高，更新资料速度快，写入资料的比例比读取资料的比例还高，允许多个连线同时更新同一笔资料。使用帐号资讯存放于 DB 相对存放于 LDAP，俱有以下缺点：存取控制(Access Control List, ACL)较不安全，LDAP 的 ACL 较 DB 完整，DB 的存取技术难度虽相较 LDAP 简单，LDAP 通讯协定是属于 protocol，支援的异质平台较多，但 DB 通讯协定不属于 protocol，所以支持的异质平台较少。所以本系统在资料安全性维护上，有规划相对应的配套(资讯安全规划)如后说明。

EIP SSO 流程说明

SSO[6]运作原理分为以下四个步骤如图 3：

1) 使用者所有登入都连到 SSO Server 进行。

2) 未经登入无法存取 Web Application。

3) 登入之后，SSO Server 给予使用者凭证，证明已经通过身分认证。

4) 使用者取得凭证后，就可以存取 Web Application，并由 SSO Server 告知 Web Application 使用者的身分。

若资讯系统已有 LDAP 认证机制，不以上述 SSO 认证方式，Web service 直接认证 LDAP。

3. 系统开发流程

系统开发主要核心于帐号管理同步程序开发、OpenLDAP 资料架构设计及建置、修改资讯系统至 LDAP 认证关键程序、及资讯安全规划。

3.1. 帐号管理同步程序开发

帐号管理平台引进了标准的 LDAP 服务，LDAP 全名为 Lightweight Directory Access Protocol 为一种目录服务，可以使用 LDAP 来记录各种人员资讯。由于 LDAP 是一种标准的通讯协定，故不同的应用系统只要遵守此一共通的通讯协定，即可与 LDAP 服务进行沟通，取得其内的资料如帐号基本资料、权限资料等。此一目录服务已被各界广泛运用于帐号管理，认证、授权等机制。故由于它的标准性及普遍性，故采用其相关产品来作为我们帐号管理平台。经由评估测试，采用的是 OpenLDAP 软体与资料同步软体。

目前 LDAP 的资料架构在整合每一个资讯系统的不尽相同过程中，整合的方式分为：

1) 原系统帐号与 LDAP 帐号一致：资讯系统由于帐号与 LDAP 帐号一致，只有密码可能不一样，故整合的方式只需要将原认证的方式改由向 LDAP 服务器进行认证即可如图 4，现在开发之程序语言都有内建与 LDAP 服务器沟通的函示库提供整合。即认证帐号与 LDAP 一致时，同步认证帐号 Attribute 到 LDAP Attribute。

2) 原系统帐号与 LDAP 帐号不一致：资讯系统由于原使用的帐号和 LDAP 帐号不一致，整合的方式就是原帐号资料中，属性值是 LDAP 帐号基本资料中

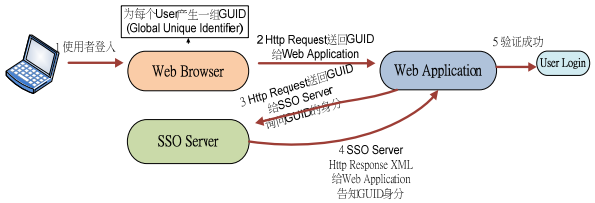

Figure 3. The operation principle of SSO
图 3. SSO 运作原理

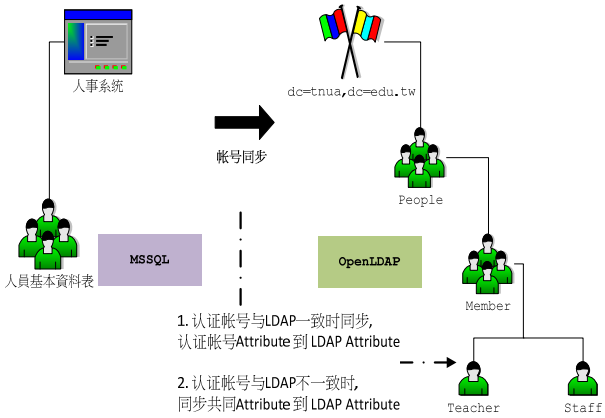

Figure 4. The synchronization manager of the teacher and staff member accounts for human resource system
图 4. 人事系统教师职员帐号同步管理

也同时具有的，通常为身份证号码。修改原认证的机制改由 LDAP 帐号完成认证后，再透过额外的函示库取得该帐号所对应的属性资料，如前所述的身份证号码，透过此属性资料对应到原系统帐号。简单说同步共同 Attribute 到 LDAP Attribute。

LDAP 相关名词 DC (Domain Component)、CN (Common Name)、OU (Organizational Unit)。学校的使用者分为教师、职员、学生。教师、职员的基本资料来自于人事系统；学生的基本资料来自于教务系统，故此帐号管理同步程序(图 5)每日至人事系统同步教师、职员的基本资料到 ou = member，ou = people，dc = tnua，dc = edu.tw 如图 4；帐号管理同步程序每日至教务系统同步学生的基本资料到 ou = member，ou = people，dc = tnua，dc = edu.tw 如图 6。

3.2. OpenLDAP 资料架构设计及建置

LDAP 模型是以项目(entry)为基础。项目是一个称为 objectclass 之属性的集合。每一个项目都有一个识别名称(DN)，它可用来清楚参照(项目)。在 LDAP，项目是以阶层式结构排列的，如图 7 之阶层图，为本校之 LDAP 结构。代表学校的项目位在树状结构的顶

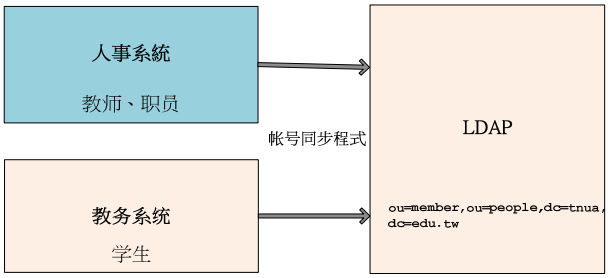

Figure 5. The synchronization manager of the accounts for academic information system and human resource system
图 5. 教务系统人事系统帐号同步管理

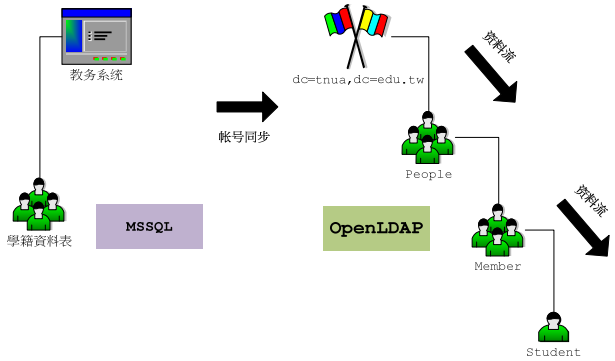

Figure 6. The synchronization manager of the student accounts for educational System
图 6. 教务系统学生帐号同步管理

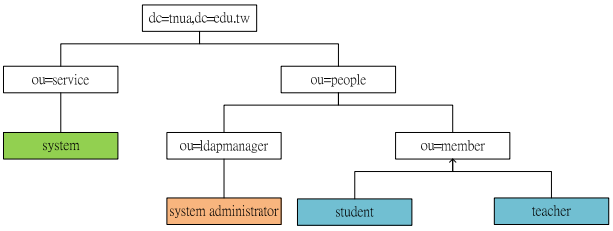

Figure 7. Hierarchy diagram of LDAP
图 7. LDAP 阶层图

端也就是(dc = tnua, dc = edu.tw)，学校底下有组织，分别为(系统使用群组(ou = service, dc = tnua, dc = edu.tw))和(国立台北艺术大学群组(ou = people, dc = tnua, dc = edu.tw))，学校底下有组织，分别为(系统使用群组(ou = service, dc = tnua, dc = edu.tw))和(国立台北艺术大学群组(ou = people, dc = tnua, dc = edu.tw))，最后在树状最末端的项目一般是代表人员(person)，每一个树状最末端的项目都有一个相对的识别名称，它在树状结构分枝的其它同层对象中必须是唯一的。例如：

Cn = xxx@tnua.edu.tw, ou = member, ou = people, dc = tnua, dc = edu.tw

目前在 LDAP(教职员生群组(ou = member, ou = people, dc = tnua, dc = edu.tw))内存放教职员生的资料架构， 每个人员资料内有数个属性，其中 LDAP 个人员资料属性比较重要的如表 2 所列。

3.3. LDAP 关键应用程序撰写

现有各资讯系统的使用者资讯，记录在各资讯系统的资料库里，且各系统自行认证。为统一各资讯系统帐号与密码，若资讯系统可以 LDAP 进行帐号进码认证，则需修改原本的认证机制，改到 LDAP 进行认证如图 8。

OpenLDAP 为 Linux 之应用软体，LDAP 关键应用程序撰写，以属性主要设定档中，include/inetorgperson.schema 结构为例，进行 LDAP 个人员资料属性表设定，执行步骤为 1) 定义新的属性 inetorgperson.schema、栏位名称、资料型态、物件栏位编号。2) 修改 inetorgPerson ObjectClass 必填/非必填栏位，3) 进行 OpenLDAP 重新启动 ReStart。部份设定简述如下：

步骤 1：OpenLDAP 为 Linux 应用软体，Attribute 主要设定档为/etc/openldap/slapd.conf，其中部分可应用之 LDAP include schema 为

include/etc/openldap/schema/core.schema
include/etc/openldap/schema/cosine.schema
include/etc/openldap/schema/inetorgperson.schema
include/etc/openldap/schema/nis.schema
include/etc/openldap/schema/misc.schema
include/etc/openldap/schema/FreeRadius.schema

以 include /etc/openldap/schema/inetorgperson.schema 为例有 idNumber 可用

attributetype (2.16.840.1.113730.3.1.219#资料型态
NAME \'idNumber\' #栏位名称
DESC \'for tnua.edu.tw id number\' #描述
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{20})# 物 件 栏 位编号

步骤 2：依据表 2 LDAP 个人员资料属性表，新增 inetorgperson ObjectClass 必填/非必填栏位

#inetOrgPerson
#The inetOrgPerson represents people who are associated with
#an organization in some way. It is a structural class and is
#derived from the organizationalPerson which is defined in
#X.521 [X521].
objectclass (2.16.840.1.113730.3.2.2 #物件编号
NAME\'inetOrgPerson\'#物件名称
DESC\'RFC2798: Internet Organizational Person\'#对象描述
SUP organizationalPerson
STRUCTURAL
MAY (#对象所有可用栏位
audio $ businessCategory $ carLicense $ departmentNumber $
displayName $ employeeNumber $ employeeType $

Table 2. LDAP personnel data attribute table
表 2. LDAP 人员资料属性表

Attribute	Value	属性说明
Gid Number	10000	群组识别码
Object Class	inetOrgPerson	LDAP 物件
Object Class	posixAccount	LDAP 物件
Object Class	inetLocalMailRecipient	LDAP 物件
Mail	xxx@tnua.edu.tw	电子邮件
Uid	xxx@tnua.edu.tw	LDAP 帐号
Uid Number	2001	单位识别码
Cn	xxx@tnua.edu.tw	使用者帐号
Home Directory	/home/xxx@tnua.edu.tw	Samba 私人目录
Hr student	1	是否在人事系统有帐号
Id Number	xxxxxxxx	身份证
Given Name	xxx	姓名
Mobile	xxxxxxxxxx	行动电话
Birthday	1980xxxx	出生年月日
Status	1	是否在职/学
Sn	B0804	人事代码/学号
Title	tea	身份群组(教职员/学生)
Card No.	02xxxxxx	教职员证、学生证芯片序号
Mail Host	mymail.tnua.edu.tw	Mail Server
User Password	{CRYPT}FQIVLBeqPEQgI	使用者密码
Postal Address	xxx	通讯地址
Postal Code	xxx	邮递区号
Ou	1201	单位代码
Description	E01	身份别

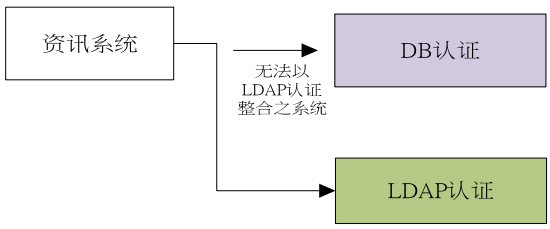

Figure 8. The LDAP authenticate mode of information system
图 8. 资讯系统改 LDAP 进行认证

givenName $
homePhone $ homePostalAddress $ initials $ jpegPhoto $ labeledURI $ mail $ manager $ mobile $ o $ pager $ photo $ roomNumber $ secretary $ uid $ userCertificate $ x500uniqueIdentifier $ preferredLanguage $ userSMIMECertificate $ userSecondPassword $ secondMail $ idNumber $ status $ birthday $ userPKCS12))

步骤 3：重新启动 OpenLDAP ReStart。

3.4. SSO 认证关键程式

如前说明 SSO 业界整合技术分为使用者帐号资讯存放于目录服务系统 LDAP 及存放于资料库 DB 共同合并使用，若系统无法以 LDAP 进行帐号认证时，则将采取使用帐号资讯存放于 DB，采取 DBSSO 认证之关键程式。1) SSO Server 认证完毕回传所产生 XML 的主要程式码，2) Client 端解析(Parsing)上段 server xml 之认证结果之关键程式码。

以下为 SSO Server 认证完毕回传所产生 XML 的主要程式码，SSO Server 是以 Microsoft Visual Studio 2010[7]为开发工具，以 C#为程式开发语言之 XML 如下所示：

```
1.  public string sessionStatusXML
2.              {
3.                  get
4.   {    //宣告XML物件
5.  XmlDocument xmldoc = new XmlDocument();
    XmlDeclaration node_dec =
    xmldoc.CreateXmlDeclaration ("1.0", "utf-8",
    "yes");
6.  xmldoc.AppendChild (node_dec);
7.  SessionUser = xmldoc.CreateElement ("Ses-
    sionUser");
8.  //如果找不到GUID相对应的User
9.    if (id == 0)
10.       {
11.           user = xmldoc.CreateElement ("mem-
    ber");
12.               user.InnerText = "null";
13.   SessionUser.AppendChild (user);
14.   xmldoc.AppendChild (SessionUser);
15.       }
16.       else
17.    {
18. //如果User已离职或离校
19.         if (disabled == true)
20.             {
21.       user = xmldoc.CreateElement("member");
22.               user.InnerText = "null";
23.  SessionUser.AppendChild (user);
24.  xmldoc.AppendChild (SessionUser);
25.              }
26.   //GUID对应到User且User身分是在职或在学
27.         else
28.           {
29.      //产出member属性栏位
30. user = xmldoc.CreateElement ("member");
31. user.InnerText = member.id;
32. SessionUser.AppendChild (user);
33.        //产出其他栏位
34.               username[姓名]、type [身分]、
35. staffId [人事代码/学号]、idNo [身分证]、
36. guid [User登入时的GUID]、userIP [登入IP]、
37. logDate [登入时间]、disabled [帐号是否停用]、
38. inutesDiff [有效时间]、unit [User单位代码]
39.                         }
40.                     }
41. //产出结果XML回传给Client
42.  return xmldoc.OuterXml;
43.                 }
44.           }
```

Client 端解析(Parsing)上段 server xml 之认证结果之关键程式码，Client 依据 Web Application 本身撰写的语言来解析 SSO Server 回传的 XML 档，进一步得知使用者的身分。以下是以 C#为例 Parsing SSO Server 回传的 XML。

```
1.  protected void Page_Load(object sender, Even-
    tArgs e)
2.  {
3.    //取得User登入EIP的GUID
4.    string guid= Request["guid"];
5.    //宣告XML物件
6.    XmlDocument doc = new XmlDocument();
```

```
7.      //指定到SSO Server取得XML档
8.     doc.Load(
9.      //询问SSO Server该GUID是哪一个User
10.  "http://eip.tnua.edu.tw/Portal/CheckGUID?member
     Log.guid = "+guid
11.           );
       //Parsing XML member attribute栏位资料
12.    string mail =
     doc.SelectNodes("//member").Item(0).InnerText;
13.    //Parsing XML ip attribute栏位资料
14.    //接续Web Application本身的登入验证模式
15.  }
```

使用者帐号资讯整合存放于 LDAP 目录服务系统，原系统程式可直接进行 LDAP 认证，直接修改资讯系统至新 LDAP 认证，关键程式为：

```
1.   string path =
         "LDAP://cldapc.tnua.edu.tw/ou=member,ou=pe
         ople,dc=tnua,dc=edu.tw";
2.   DirectoryEntry de = new DirectoryEntry(path);
3.   bool result;
4.   try
5.   {
6.   de.Username = String.Format("uid={0},ou =
         member,ou = people,dc = tnua,dc = edu.tw",
         account);
7.   de.Password = psd;
8.   de.AuthenticationType = Authentication-
         Types.None;
9.   string a = de.Name;
10.  System.Diagnostics.Debug.WriteLine("LDAP 验证
         成功!");
11.  }
12.  catch (Exception e)
13.  {
14.  System.Diagnostics.Debug.WriteLine("LDAP 验证
         失败!");
15.  }
16.  finally
17.  {
18.  de.Close();
19.  }
```

3.5. 资讯安全规划

规划之 SSO 系统，必需通过多量使用者同时登入请求之系统压力测试，以负荷伺服器流量之需求。一般方法以压力测试之套装软体进行测试如以 Apache JMeter Java 视窗程式，辅助进行压力测试和性能测量的工具。JMeter 可以执行 Http、FTP、RDBMS(关联式资料库)、LDAP、SOAP 与 WebService 等的负载以及效能测试。但目前压力测试软体如 JMeter 程式，只可当模拟与辅助测试，因受限单一机器及软体使用，仍无法以实际同时间大量产出测试指令，因其是使用单一时间循序发出测试指令，非同时瞬间发出测试指令，但仍可做效能的图形分析或在大量同时发生的负载下测试伺服器与相关应用程式的稳定性。若要辅助此不足之处，可以实际安排多人实机测试，如 10 人以上同时登入功能相同之校务资讯系统，在我们以此方法安排 10 人真人实机同时指示同一运作指令之重复测试，可获得测试出 SSO 系统之稳定性及代为登入之校园资讯系统之程式缺失，以提供各个子系统工程师修正之依据。

图 9 我们应用 JMeter 软体模拟之压力测试，模拟 10 秒内有 1000 个 Users 透过 Web Application 进行 LDAP Query，并将压力测试以 DB 格式储存，检查其执行结果如图 10，含 LDAP Query 开始时间、LDAP Query 结束时间及耗时毫秒，验证压测结果获得平均存取本开发系统 2 毫秒，最大为 16 毫秒，最小 0 毫秒。

资讯安全规划使用帐号资讯存放于 DB 相对或 LDAP，必须考虑存取控制不安全疑虑之因应作法[8]，除网路防火墙协助外，另增实际的辅助维护资料安全做法有非法登入通知、不允许多重登入、存取控制表(Access Control List, ACL)、敏感资料加密、LOG 记录…等。叙述如下说明：

1) 非法登入通知：一小时内超过 3 次登入失败，即会透过 Email、简讯。如图 11 所示：

2) 不准许多重登入：同一时间只能准许同一个帐号进行登入 EIP 系统、如果多重登入最先登入的用户，会被登出。如图 12：

3) 存取控制表(Access Control List, ACL):启动 IP Tables 只准许合法的 IP 进行 GUID 的 Query。

4) 敏感资料加密:使用者密码采用 Base64 进行加

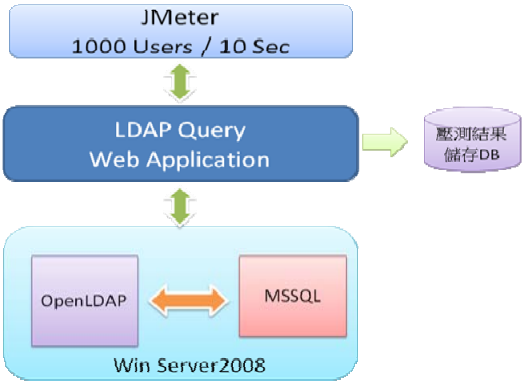

Figure 9. The stress test by JMeter Software simulation
图 9. JMeter 软体模拟之压力测试

id	beginTime	endTime	result	diff
2241	2012-07-10 14:56:27.963	2012-07-10 14:56:27.980	1	16
2247	2012-07-10 14:56:28.027	2012-07-10 14:56:28.043	1	16
2290	2012-07-10 14:56:28.510	2012-07-10 14:56:28.527	1	16
2291	2012-07-10 14:56:28.510	2012-07-10 14:56:28.527	1	16
2292	2012-07-10 14:56:28.510	2012-07-10 14:56:28.527	1	16

Figure 10. The stress test results by JMeter Software simulation
图 10. JMeter 软体模拟之压力测试结果

Figure 11. Illegally logged notice
图 11. 非法登入通知

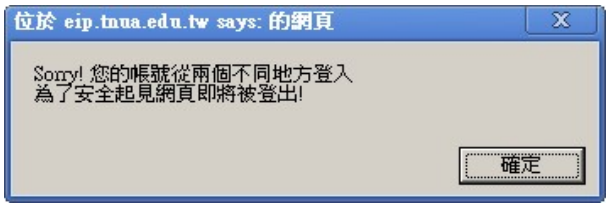

Figure12. Multiple logins notice
图 12. 多重登入通知

密。

5) LOG 记录:使用者登入留有 LOG 记录及 SSO 登入不同资讯系统留有 LOG 记录。

4. 开发成果

校务行政资讯系统单一签入，与帐号功能整合个人化入口网站开发之过程，EIP 资料来源的确认与人事资料较正，教师身分(专任教师、兼任教师)、职员身分(人事系统职员身分、教师兼一、二级主管)、学生身分；SSO 的安全登入机制、帐号密码管理(密码强度、密码时效性、忘记密码处理流程、修改密码机制)、与新旧 LDAP 资料同步、原有系统使用 LDAP 认证转移至 EIP LDAP、EIP 的版型架构、EIP 提供 Portlet 的服务、美术编辑及系统推广教育训练…等，是单一签入与帐号功能整合所需规划之开发细节，每一步骤确认才能完整整合校务行政资讯系统单一签入。

校务行政资讯系统单一签入，与帐号功能整合个人化入口网站(Portal)，于本校建立之校园资讯入口网(Information Portal of Taipei National University of the Arts, 簡稱 iTNUA)，iTNUA 单一签入入口网自行开发建置(校园资讯入口网站 http://eip.tnua.edu.tw/)，于 2012 年 7 月开始进行开发研究，完成单一签入入口网已建置完成，并自 2013 年 6 月开始上线启用。

帐号密码登入、密码查询及及 EIP 操作页面如图 13~15，并将所有系统的讯息统一集中到入口网，用户只须登入到入口网，便可存取内部被授权的各类资源，并设计于 EIP 页面框架与显示分割功能页面(Portlet)[9]。目前已经成功整合的校务行政资讯系统如下：

1) 教务系统：含开课查询、学籍、研究生学位考、成绩查询、毕业审查及离校系统等。

2) 学务系统：学生奖惩、请假、兵役、奖学金、操行、宿舍管理系统等。

3) 总务系统：薪俸查询、停车证申请、场地租借、悠游卡挂失系统等。

4) 资讯相关系统：电子邮件信箱、电子报系统、简讯发送系统、校园无线网路系统等。

5) 人事相关系统：人事系统、差勤系统等。

6) NAS、卡务系统、门禁系统、图书馆自动化系统、教师自我评鉴系统、数位学习平台人事相关系统等。

5. 结论

iTNUA 单一签入入口网自行开发建置，运用 OpenLDAP 原理延伸出的目录服务管理可以大幅降低软体建置成本，并将资源集中，各资讯系统的程式开发语言皆有支援 LDAP API，可快速的修改系统认证

Figure 13. The EIP home of system login
图 13. 系统登入首页

Figure 14. The queries of forgot account or password
图 14. 忘记帐号密码查询

Figure 15. EIP operation page
图 15. EIP 操作页面

机制，进一步达到单一登入(Single sign-on)的运用。另达成主要目的与效益为：

1) 以OpenLDAP目录服务为主要存取认证中心，来达成使用者单一签入(SSO, Single Sign On)的目标。简单的来说，使用者仅需一组帐号与密码，即可进入已整合之各系统网站。

2) 不需要以不同的帐号密码，重复登入各系统网站，解决教职员及学生记忆多组帐号及密码的困扰，减少忘记密码情况之发生。

3) 登入 iTNUA 单一签入资讯入口网后，每位使用者轻易快速的开启校内提供各系统网站之服务，获得个人及各相关单位所发布之资讯，有效提升学校所提供 e 化服务之使用率。更重要的自主开发除了能节省开发费用，效能与功能符合业务单位需求，且能精进各系统开发人员之技术能力，亦能熟稔系统之实质架构。

导入后之实质效益提供所有教职员生零时差的使用或管理校园资讯服务、简化帐号与权限管理、减少作业错误、强化资讯安全认证功能、确保身份资料一致的安全性，避免非学校人员可存取学校资源、协同作业平台提供讯息完整即时的传递、重大政策有效地宣导及工作项目清单一览无遗。并且以此本校全面性自行开发与研究 EIP 与 SSO，得就开发之成果得以呈现与揭露核心技术于论文，可广为推广学校与企业应用及合作。

参考文献 (References)

[1] 周盟渊. 校务行政系统帐号整合[R]. 台北: 国立台湾师范大学电子计算机中心, 2011.
[2] T. Jackiewicz. Deploying openLDAP. New York: Apress, 2004.
[3] 蒋大伟. LDAP 系統管理[M]. Taiwan Branch: O'Reilly, 2003.
[4] LDAP 入门[URL]. 2008. http://www.l-penguin.idv.tw/article/ldap-1.htm
[5] OpenLDAP Foundation. OpenLDAP Software 2.3 Administrator's Guide [URL]. 2008/2012. http://www.openldap.org/ doc/admin23/index.html
[6] 廖文渊. Single Sign-On(SSO)的优越融合－以IBM WebSphere Application Server V. 5和Lotus Notes/Domino 6为例[R]. 台北: 资策会数位教育研究所, 2004/2012.
[7] Microsoft Developer Network. 实作企业单一登入[URL]. 2009/2012. http://msdn.microsoft.com/zh-tw/library/aa558712(v=bts.10).aspx
[8] Microsoft Developer Network. SSO 安全性建议[URL]. 2009/2012. http://msdn.microsoft.com/zh-tw/library/aa560954(v=BTS.10).aspx
[9] Portals and Portlets: The Basics [URL]. 2006/2012. http://editorial.mcpressonline.com/web/mcpdf.nsf/wdocs/5232/$FILE/5232_EXP.pdf

