iTNUA 校園資訊入口及單一帳號登入整合之實作

林明灶　　劉仲凱
國立臺北藝術大學電子計算機中心
臺北市、臺灣
mtlin@tnua.edu.tw　chongkai@tnua.edu.tw

摘要

本文主要描述國立臺北藝術大學(Taipei National University of the Arts, TNUA)，在自主開發建置單一帳號簽入統整各校務行政資訊系統的過程架構及方法，以分享系統實務流程經驗，於建構整合校園行政系統資訊入口(Enterprise Information Portal, EIP)，及學校 e-mail 單一帳號登入(Single sign-on, SSO)，便利使用教務系統、學務系統、人事系統、電子郵件、資訊查詢…等各項校園資訊系統，提供實務開發經驗分享應用。開發流程重點於帳號管理設定、輕量級目錄存取協定(Lightweight Directory Access Protocol, LDAP)資料架構設計及建置、LDAP 應用程式介面 API、帳號開啟系統及帳號整合機制規劃。運用 OpenLDAP 原理延伸目錄服務管理大幅降低軟體建置成本，且資訊系統的程式開發語言皆有支援 LDAP API，迅速修改系統認證機制，達成單一登入之開發。

關鍵字: 單一帳號登入, 校園行政系統資訊入口, 輕量級目錄存取協定.

ABSTRACT

This paper is mainly introduction 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 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 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

1. 前言

大學校務系統的開發管理與經營控管，對於大學行政績效的提升，具有關鍵性的影響。數位化校園建設中行政系統資訊化，不同時期陸續開發完成教務資訊系統、學務資訊系統、人事資訊系統、總務資訊系統與招生試務系統及其它相關子系統等建置更新作業，以提昇教務處、人事室、學務處、推廣教育、總務...等行政效率與服務品質，及資料庫整合之即時及一致性作業，提供各項資訊自動化作業、管理報表及報部報表[1]。校務行政資訊系統均需要使用者鍵入帳號密碼進行認證，認證通過後，各系統針對登入的帳號進行授權，取得相對應的功能與權限。但開發過程中，各系統的帳號因無相互整合，使用者就需要針對每個系統去進行帳號的建立(如以身份證字號、email帳號、學生學號或個別帳號…等)，密碼的設定。系統增加，相對需記憶之帳號密碼亦增加。因此對使用者帳號密碼管理是困擾的。當人員資料異動時，需以非資訊化機制如書面或定時管理帳號資料。可能面臨的困難點，於各系統帳號的不同、資訊系統上線而無法全面修改帳號、開發程式語言不同及委外系統廠商的經驗與配合度。因此統整各應用系統的帳號，使用單一組帳號密碼登入如圖1於各應用系統是必需的。

企業入口網站(EIP)及單一帳號簽入之開發，以目前學校校園及企業界為例，多以廠商協助開發，在系統整合過程雖有標準化作業流程，與充足之經驗，但開發費用接近10萬美金以上之要求，及每年至少需10%以上之維護費用，且委託單位面臨程式無法自主及核心技術無法獲得，新系統開發之介接仍需依賴於廠商，廠商之資訊人員異動頻繁常造成技術銜接有代溝，時效管理都有所延遲。自主開發除了能節省開發費用，效能與功能符合業務單位需求，且能精進各系統開發人

員之技術能力，亦能熟稔系統之實質架構。需挑戰的是系統與EIP整合之協調溝通，及資訊安全之設計。

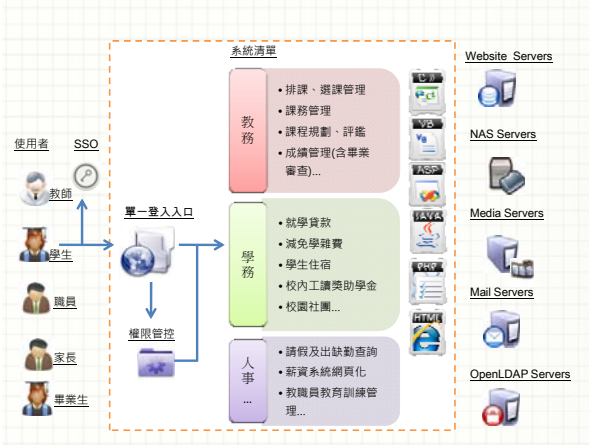

圖 1 校務系統單一簽入架構規劃圖

EIP 及 SSO 之發展已近十餘年，相關論文著重於單一學術主題討論，帳號管理關鍵技術在於使用輕量級目錄存取協定 LDAP，經研究廠商使用之 LDAP 技術，區分為 AD (Windows)、eDirectory(Novell) 、 Directory Server(IBM) 及 OpenLDAP，經由評估其優缺後選用 OpenLDAP，因為免授權費用與開放式源始碼(Open Source)及效能可以應付本校教職員生共約 3,000 人，與功能符合本校需求。目前多為開發廠商之核心技術而無法取得開發之報告，本論文在於本校全面性自行開發與研究 EIP 與 SSO，得就開發之成果得以呈現與揭露核心技術於論文，並廣為推廣學校與企業應用。

目前於各資訊系統的帳號大致可以區分為 Email、學生學號、身份證字號、個別帳號如表 1 所列，為達成單一簽入式登入帳號，因考量外籍人士無法取得身份證字號，規劃以 Email 帳號為統一的帳號。

2. SSO 帳戶資訊管理機制

綜合 SSO 業界整合技術分為 2 種及共同合併使用，其運作模式如下圖所示：

1. 使用者帳號資訊存放於目錄服務系統如 LDAP、AD (Active Directory)，目前業界廠商如 Direk Tech Inc.、Novell、IBM 大都以目錄服務系統來開發 SSO 相關產品。
2. 使用者帳號資訊存放於資料庫系統如 MSSQL、Oracle、MySQL，目前業界廠商如狀態網際網路大都以資料庫系統來開發 SSO 相關產品。

表 1 資訊系統與使用登入帳號分類表

登入帳號	資訊系統
Email 帳號	無線網路、webmail、數位學習、總務系統…
教職員身分證、學生學號	教務系統、學務系統、掛失系統、圖書館系統…
教職員身分證	出納系統、招生系統、人事系統…
個別帳號	官網、電子公文、數位典藏…

比較分析學校各資訊系統的屬性後，使用者帳號資訊存放於 LDAP 及 DB 共同合併使用，若系統無法以 LDAP 進行帳號認證時，則將採取使用帳號資訊存放於 DB，其中 DB 俱有之優點：DB 容易與各資訊系統進行資料交換與資料同步。帳號資訊存放於 DB 容易被各系統的開發語言所使用，資料的備份與備援機制健全。使用資料庫存放使用者資訊可自由快速的附加其他欄位屬性，無需重新啟動服務，擴充性與便利性較高，更新資料速度快，寫入資料的比例比讀取資料的比例還高，允許多個連線同時更新同一筆資料。使用帳號資訊存放於 DB 相對存放於 LDAP，俱有以下缺點：存取控制(Access Control List, ACL)較不安全，LDAP 的 ACL 較 DB 完整，DB 的存取技術難度雖相較 LDAP 簡單，LDAP 通訊協定是屬於 protocol，支援的異質平台較多，但 DB 通訊協定不屬於 protocol，所以支援的異質平台較少。所以本系統在資料安全性維護上，有規劃相對應的配套「資訊安全規劃」如後說明。

2.1 EIP SSO 流程說明

SSO 運作原理分為以下四個步驟如圖 2：

1. 使用者所有登入都連到 SSO Server 進行。
2. 未經登入無法存取 Web Application。
3. 登入之後，SSO Server 給予使用者憑証，證明已經通過身分認證。
4. 使用者取得憑證後，就可以存取 Web Application，並由 SSO Server 告知 Web Application 使用者的身分。

若資訊系統已有 LDAP 認證機制，不以上述 SSO 認證方式，Web service 直接認證 LDAP。

3. 系統開發流程

系統開發主要核心於帳號管理同步程式開發、OpenLDAP 資料架構設計及建置、修改資訊系統至 LDAP 認證關鍵程式、及資訊安全規劃。

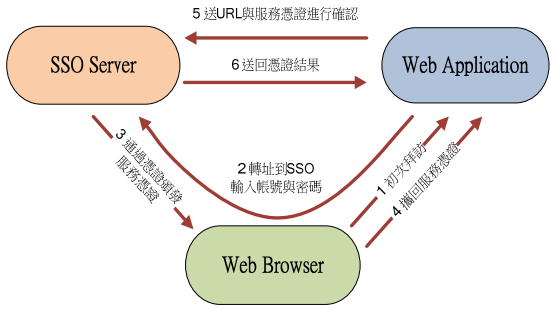

圖 2 SSO 運作原理

3.1 帳號管理同步程式開發

帳號管理平台引進了標準的 LDAP 服務，為一種目錄服務，可以使用 LDAP 來記錄各種人員資訊。由於 LDAP 是一種標準的通訊協定，不同的應用系統只要遵守此一共通的通訊協定，即可與 LDAP 服務進行溝通，取得其內的資料如帳號基本資料、權限資料等。 此一目錄服務已被各界廣泛運用於帳號管理，認證、授權等機制。由於它的標準性及普遍性，故採用其相關產品來作為我們帳號管理平台。經由評估測試，採用的是 OpenLDAP 軟體與資料同步軟體。

目前LDAP的資料架構在整合每一個資訊系統的不盡相同過程中，整合的方式分為:

1. 原系統帳號與LDAP帳號一致：資訊系統由於帳號與LDAP帳號一致，只有密碼可能不一樣，故整合的方式只需要將原認證的方式改由向LDAP伺服器進行認證即可如圖5，現在開發之程式語言都有內建與LDAP伺服器溝通的函示庫提供整合。即認證帳號與LDAP一致時，同步認證帳號 Attribute 到 LDAP Attribute。
2. 原系統帳號與LDAP帳號不一致：資訊系統由於原使用的帳號和LDAP帳號不一致，整合的方式就是原帳號資料中，屬性值是LDAP帳號基本資料中也同時具有的，通常為身份證號碼。修改原認證的機制改由LDAP帳號完成認證後，再透過額外的函示庫取得該帳號所對應的屬性資料，如前所述的身份證號碼，透過此屬性資料對應到原系統帳號。簡單說同步共同Attribute到 LDAP Attribute。

LDAP 相關名詞 DC (Domain Component)、CN (Common Name)、OU (Organizational Unit)。學校的使用者分為教師、職員、學生。教師、職員的基本資料來自於人事系統;學生的基本資料來自於教務系統，故此帳號管理同步程式(圖 3)每日至人事系統同步教師、職員的基本資料到 ou=member, ou=people, dc=tnua, dc=edu.tw 如圖 4; 帳號管理同步程式每日至教務系統同步學生的基本資料到 ou=member, ou=people, dc=tnua, dc=edu.tw 如圖 5。

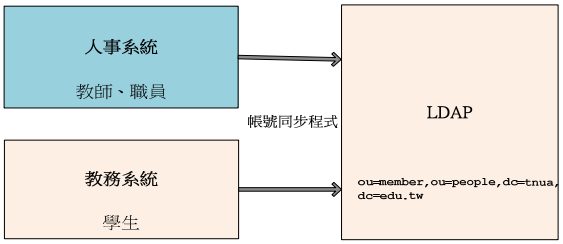

圖3 教務系統人事系統帳號同步管理

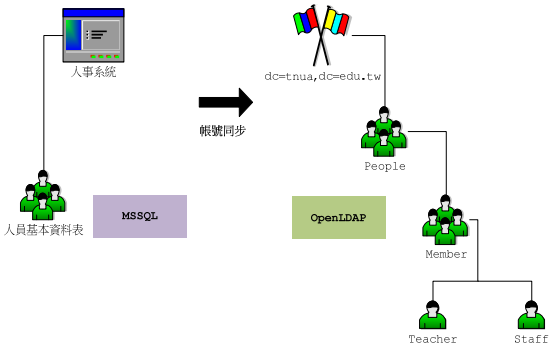

圖 4 人事系統教師職員帳號同步管理

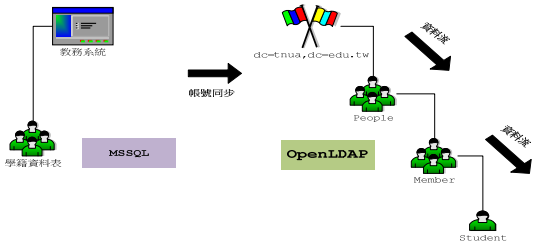

圖 5 教務系統學生帳號同步管理

3.2 OpenLDAP資料架構設計及建置

LDAP 模型以項目(entry)中 objectclass 之屬性的集合[2-6]。每一項目都有一組識別名稱(DN)，用來清楚對照項目。在 LDAP，項目以階層式結構方式排列，如圖 6 之階層圖，為本校之 LDAP 結構。代表學校的項目位在樹狀結構的頂端也就是(dc=tnua, dc=edu.tw)，學校底下有組織，分別為「系統使用群組(ou=service, dc=tnua, dc=edu.tw)」和「國立臺北藝術大學群組(ou=people, dc=tnua, dc=edu.tw)」，國立臺北藝術大學群組底下有「LDAP 管理者群組(ou=ldapmanager, ou=people, dc=tnua, dc=edu.tw)」和「教職員生群組(ou=member, ou=people, dc=tnua, dc=edu.tw)」，最後在樹狀最末端的項目一般是代表人員 (person)，每一個樹狀最末端的項目都有一個相對的識別名稱，它在樹狀結構分枝的其他同層物件中必須是唯一的。

例如：

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

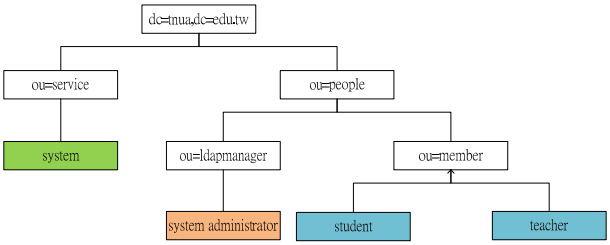

圖 6 LDAP 階層圖

目前在 LDAP「教職員生群組(ou=member, ou=people, dc=tnua, dc=edu.tw)」內存放教職員生的資料架構， 每個人員資料內有數個屬性，其中 LDAP 個人員資料屬性比較重要的如表 2 所列。

3.3 LDAP API程式撰寫

現有各資訊系統的使用者資訊，記錄在各資訊系統的資料庫裡，且各系統自行認證。為統一各資訊系統帳號與密碼，若資訊系統可以LDAP進行帳號進碼認證，則需修改原本的認證機制，改到LDAP進行認證如圖7。

表 2 LDAP 個人員資料屬性表

Attribute	Value	屬性說明
gidNumber	10000	群組識別碼
objectClass	inetOrgPerson	LDAP 物件
objectClass	posixAccount	LDAP 物件
objectClass	inetLocalMailRecipient	LDAP 物件
mail	xxx@tnua.edu.tw	電子郵件
uid	xxx@tnua.edu.tw	LDAP 帳號
uidNumber	2001	單位識別碼
cn	xxx@tnua.edu.tw	使用者帳號
homeDirectory	/home/xxx@tnua.edu.tw	Samba 私人目錄
hrstudent	1	是否在人事系統有帳號
idNumber	xxxxxxxx	身分證
givenName	xxx	姓名
mobile	xxxxxxxxxx	行動電話
birthday	1980xxxx	出生年月日
status	1	是否在職/學
sn	B0804	人事代碼/學號
title	tea	身分群組(教職員/學生)
cardNo	02xxxxxx	教職員證、學生證晶片序號
mailHost	mymail.tnua.edu.tw	Mail Server
userPassword	{CRYPT}FQIVLBeq	使用者密碼
	PEQgI	
postalAddress	xxx	通訊地址
postalCode	xxx	郵遞區號
ou	1201	單位代碼
description	E01	身分別

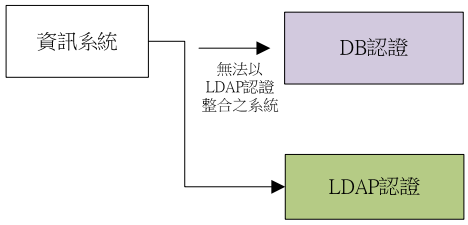

圖7 資訊系統改LDAP進行認證

LDAP認證關鍵程式，是以C#為例至LDAP認證。SSO Server關鍵程式碼[8]，SSO Server 是以 Microsoft Visual Studio 2010為開發工具，以 C# 為程式開發語言，以下為SSO Server產生XML的主要程式碼，XML如下圖所示。

```
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("SessionUser");
8.  //如果找不到GUID相對應的User
9.          if (id == 0)
10.         {
11.           user = xmldoc.CreateElement("member");
12.           user.InnerText = "null";
13.           SessionUser.AppendChild(user);
14.           xmldoc.AppendChild(SessionUser);
15.         }
16.         else
17.         {
18. //如果User已離職或離校
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對應到User且User身分是在職或在學
27.           else
28.           {
29.   //產出member屬性欄位
30.         user = xmldoc.CreateElement("member");
31.           user.InnerText = member.id;
32.           SessionUser.AppendChild(user);
33.     //產出其他欄位
34.           username[姓名]、 type [身分] 、
35.           staffId [人事代碼/學號] 、idNo [身分證] 、
36.           guid [User登入時的GUID] 、userIP [登入IP]、
37.           logDate [登入時間] 、disabled [帳號是否停用]、
38.           minutesDiff [有效時間] 、unit [User單位代碼]
```

```
39.                 }
40.             }
41.             //產出結果XML回傳給Client
42.             return xmldoc.OuterXml;
43.         }
44.     }
```

Client 端關鍵程式碼中，Client 依據 Web Application 本身撰寫的語言來 Parsing(解析) SSO Server 回傳的 XML 檔，進一步得知使用者的身分。以下是以 C#為例 Parsing(解析) SSO Server 回傳的 XML。

```
1.  protected void Page_Load(object sender, EventArgs 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檔
8.   doc.Load(
9.       //詢問SSO Server該GUID是哪一個User
10.  "http://eip.tnua.edu.tw/Portal/CheckGUID?memberLog.guid="+guid
11.      );
         //Parsing XML member attribute欄位資料
12.  string mail = doc.SelectNodes("//member").Item(0).InnerText;
13.  //Parsing XML ip attribute欄位資料
14.  //接續Web Application本身的登入驗證模式
15. }
```

3.4 資訊安全規劃

如第 2 節說明，使用帳號資訊存放於 DB 相對存放於 LDAP，俱有存取控制較不安全缺點 ，所以本系統在維護資料安全性上有規劃，相對應的配套「資訊安全規劃」。設計有

1. 非法登入通知:一小時內超過 3 次登入失敗，即會透過 Email、簡訊。如圖 8 所示：

圖 8 非法登入通知

2. 不准許多重登入:同一時間只能准許同一個帳號進行登入 EIP 系統、如果多重登入最先登入的用戶，會被登出。如圖 9：

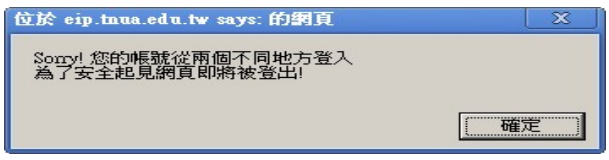

圖 9 多重登入通知

3. Access Control List (ACL):啟動 IP Tables 只准許合法的 IP 進行 GUID 的 Query。
4. 敏感資料加密:使用者密碼採用 Base64 進行加密。
5. LOG 記錄使用者登入留有 LOG 記錄；使用者 SSO 登入不同資訊系統留有 LOG 記錄。

4. 開發成果

校務行政資訊系統單一簽入，與帳號功能整合個人化入口網站開發之過程，EIP 資料來源的確認與人事資料較正，教師身分(專任教師、兼任教師)、職員身分(人事系統職員身分、教師兼一、二級主管)、學生身分；SSO 的安全登入機制、帳號密碼管理(密碼強度、密碼時效性、忘記密碼處理流程、修改密碼機制)、與新舊 LDAP 資料同步、原有系統使用 LDAP 認證轉移至 EIP LDAP、EIP 的版型架構、EIP 提供 Portlet 的服務、美術編輯及系統推廣教育訓練…等，是單一簽入與帳號功能整合所需規劃之開發細節，每一步驟確認才能完整整合校務行政資訊系統單一簽入。

校務行政資訊系統單一簽入，與帳號功能整合個人化入口網站(Portal)，於本校建立之校園資訊入口網(Information Portal of Taipei National University of the Arts, 簡稱 iTNUA)，iTNUA 單一簽入入口網自行開發建置(校園資訊入口網站 http://eip.tnua.edu.tw/)，於 2012 年 7 月開始進行開發研究，完成單一簽入入口網已建置完成，並自 2013 年 6 月開始上線啟用。

帳號密碼登入、密碼查詢及及 EIP 操作頁面如圖 10-圖 12，並將所有系統的訊息統一集中到入口網，用戶只須登入到入口網，便可存取內部被授權的各類資源，並設計於 EIP 頁面框架與顯示分割功能頁面(Portlet)[9]。目前已經成功整合的校務行政資訊系統如下:

1. 教務系統：含開課查詢、學籍、研究生學位考、成績查詢、畢業審查及離校系統…等。
2. 學務系統：學生獎懲、請假、兵役、獎學金、操行、宿舍管理系統…等。
3. 總務系統：薪俸查詢、停車證申請、場地租借、悠遊卡掛失系統…等。
4. 資訊相關系統：電子郵件信箱、電子報系統、簡訊發送系統、校園無線網路系統…等。
5. 人事相關系統：人事系統、差勤系統…等。
6. NAS、卡務系統、門禁系統 、圖書館自動化系統、教師自我評鑑系統、數位學習平台人事相關系統…等。

圖 10 系統登入首頁

圖 11 忘記密碼查詢

圖 12 EIP 操作頁面

5. 結論

iTNUA 單一簽入入口網自行開發建置，運用 OpenLDAP 原理延伸出的目錄服務管理可以大幅降低軟體建置成本，並將資源集中，各資訊系統的程式開發語言皆有支援 LDAP API，可快速的修改系統認證機制，進一步達到單一登入（Single sign-on）的運用。另達成主要目的與效益為:

1. 以 OpenLDAP 目錄服務為主要存取認證中心，來達成使用者單一簽入（SSO, Single Sign On）的目標。簡單的來說，使用者僅需一組帳號與密碼，即可進入已整合之各系統網站。
2. 不需要以不同的帳號密碼，重複登入各系統網站，解決教職員及學生記憶多組帳號及密碼的困擾，減少忘記密碼情況之發生。
3. 登入 iTNUA 單一簽入資訊入口網後，每位使用者輕易快速的開啟校內提供各系統網站之服務，獲得個人及各相關單位所發佈之資訊，有效提升學校所提供 e 化服務之使用率。

更重要的自主開發除了能節省開發費用，效能與功能符合業務單位需求，且能精進各系統開發人員之技術能力，亦能熟稔系統之實質架構。本論文在於本校全面性自行開發與研究 EIP 與 SSO，得就開發之成果得以呈現與揭露核心技術於論文，並廣為推廣學校與企業應用。

參考文獻

[1] 周盟淵, “校務行政系統帳號整合,” 國立師範大學電子計算機中心技術文件，2011年3月25日.
[2] 楊世帆、劉泳霖、方怡雯、蔡旭昇, “結合LDAP之校園電子郵件系統,” 第三屆離島資訊技術與應用研討會，pp. 372-377, 2003年6月.
[3] LDAP 入門, http://www.l-penguin.idv.tw/ article /ldap-1.htm, 查詢時間 2013年6月.
[4] Tom Jackiewicz, “Deploying OpenLDAP,” New York: Apress, 2004.
[5] 蔣大偉, “LDAP系統管理,” Taiwan Branch: O'Reilly, 2003.
[6] LDAP入門, http://www.l-penguin.idv.tw/article/ldap-1.htm, 2008.
[7] OpenLDAP Foundation, OpenLDAP Software 2.3 Administrator's Guide, http://www.openldap.org/ doc/admin23/index.html, 2008/2012.
[8] 廖文淵, “Single Sign-On(SSO)的優越融合－以IBM WebSphere Application Server V. 5和Lotus Notes/Domino 6為例,” 臺北: 資策會數位教育研究所, 2004/2012.
[9] Portals and Portlets: The Basic, http://editorial.mcpressonline.com/web/mcpdf.nsf/ wdocs/5232/$FILE/5232_EXP.pdf, 2006/2012.