校園資訊入口網之規劃與建置 – 以臺灣大學為例

邱淑美
臺灣大學計算機及資訊網路中心
Taipei, Taiwan, ROC
smchiou@ntu.edu.tw

摘要

為整合臺灣大學各種校務 e 化資訊服務，提供全校教職員工生單一入口，透過單一認證依個別權限提供個人化的服務，臺灣大學計資中心於 2008 年 7 月完成臺大校園資訊入口網站 (Enterprise Information Portal, EIP) 之規劃與建置，做為各處室資訊服務的平台，並讓使用者可以迅速找到需要的服務。現有採用計資中心帳號認證的 web-based 應用系統或新開發的，都能利用同一權限管理機制進行登記與設定，使上百個資訊系統連結可以分門別類地呈現，使用者經過單一認證後，便可以同時看到該使用者有權限執行的服務。

此單一入口網提供一致的系統操作模式，可降低使用者學習門檻與教育訓練成本。而其權限管理系統可提供系統管理者與業務負責人維護角色定義以及使用者權限之管控。

各大專院校於建置入口網有各自不同的考量與規劃重點，本文主要是分享臺灣大學在 EIP 建置過程中，有關設計單一認證機制與權限管理的一些經驗，並討論未來推動線上簽核、憑證及授權設計，期以打造一個兼具便利與安全的入口網站時的一些考量。

關鍵字: 入口網, EIP, 單一簽入, 權限管理

ABSTRACT

Computer and Information Networking Center, National Taiwan University completed an enterprise information portal in July of 2008 to integrate various e-services across campus, provide faculty and students with a single entry portal while maintaining personalized service at different levels of authorizations. Each user can now see all services available to them in one comprehensive interface with more than a hundred systems displayed in an organized manner. Current and future web-based systems may utilize a unified authorization management mechanism for registering and setting up.

This portal provides a comprehensive system operational module, reduces the learning curve, and the costs for personnel training. Moreover, this authorization management mechanism can provide administrative personnel with better control over character definitions and user privileges.

This article discusses NTU's transition to a comprehensive EIP in hopes to aid other campuses in their creation. Bedsides sharing experiences in designing single sign-in session service and authorization management, some considerations over future development of online signature and electrical certification are also discussed.

Keywords: portal, EIP, single Sign-on, authorization management

I. 前言

臺灣大學自 1996 開始由 client-server 模式改用 web browser 提供資訊服務，利用網際網路技術以 HTML, Visual Basic, IDC (Internet Database Connector), CGI (Common Gateway Interface), Java Script, ASP 等語言，陸續開發課程查詢系統等教務相關的資訊服務；於 1997 將各項 web-based 資訊系統依類別整理於 info 網站，正式進入 internet 的世代。從草創時期的 12 個 web-based APs 持續成長，至 2008 年 info 網站 [1] 上已有超過一百個應用系統，其間並經過多次改版，以期使用者能於最少的時間內找到所需的服務。但因全校各單位長期依各自的需求所各自發展的應用系統，有各別的登入頁與帳號密碼，造成使用者需要反覆登入的困擾。而系統之間缺乏整合，也造成資料不一致、或要求使用者重複輸入同樣資料的困擾與不便。

為了有效運用既有的系統及解決前述長期累積的問題，並積極因應不斷成長的校務行政 e 化需求，以提供全校師生、業務單位最好的資訊服務，計資中心自 2006 起進行校務系統的轉型及改造。在核心資料方面，透過人事相關資料庫的整併與共享，消除資料不一致或重複的問題；在系統結構方面，統一採用以服務導向架構 SOA (Service Oriented Architecture) [2] 建構整合性的平台，運用元件組合應用系統，提昇開發效率並降低維護的負擔。並於 2007 年開始進行臺大校園新一代的資訊入口網站 (Enterprise Information Portal, EIP) [3] 規劃，運用蓬勃發展的 web 環境與新技術來進行資訊整合。

2008 年 7 月成功推出了臺大人入口網 - myNTU，成為校內資訊單一簽入 (Single Sign-on) [4] 入口，提供新資訊系統有關身份辨識與權限控管一個共通的開發與管理平台，有效利用現有資源，將過去不同單位所開發的資訊系統，依據使用者的身份與角色進行不同授權，使正確的資訊在適當的時機傳達給需要的人。

II. MyNTU 資訊平台簡介

A. *友善且跨平台的入口網*

臺灣大學校風一向自由又多元，為了使入口網能夠跨瀏覽器，myNTU 之前端採用 Ext JS 進行使用者介面開發，Ext JS [5] 乃擴展自 Yahoo!UI (Yahoo! User Interface Library) 做整合性包裝所延伸出來的架構 (framework) [6]。後端則使用 Microsoft .NET 來連結 MS SQL 資料庫擷取資料給前端使用；對於前後端之間的資料傳輸使用 AJAX (Asynchronous JavaScript and XML) [7] 非同步技術，包括 Ext JS 的 Ajax 功能、AjaxPro 與及 Microsoft 泛型處理常式 (Generic Handler .ashx) [8]，只需傳遞少量資料回 Server 處理，可減少 PostBack 造成的延遲和畫面閃動，提供使用者良好的使用經驗。

myNTU 以簡潔好記的網址 https://my.ntu.edu.tw 提供服務，在臺大首頁上也有提供 myNTU 連結。進入此平台前，使用者必須過通過身份認證，單一簽入頁面如圖 1。

圖 1.　　myNTU 單一簽入頁面

B. *個人化的使用者介面設計*

使用者通過身份認證後，進入 myNTU 後的首頁右資訊框是每日焦點，乃結合『臺大校園公佈欄』動態產生的最新公告；視窗左框為系統清單，有兩個頁籤分別是『個人』及『業務』，其中『個人』頁籤目前分全校性、學生專區、教職員專區、非 NTU 帳號服務等群組（圖 2）；目前學生的服務都集中在『個人』頁籤，而教職員工則可依業務需要去點選『業務』頁籤取得與自己業務有關的其他服務。『業務』頁籤目前分課程/教務、學生事務、研發國際事務、帳務/財物、人事、活動/場地、其他等群組，都是以使用者的角度來進行分類。

透過 myNTU 所提供的權限管理機制，各群組下的系統清單可依登入者之身份（帳號別）、所設定的系統權限資料，將符合條件的資訊系統，以動態方式產生在所屬群組裡（圖 2），如此一來就可避免使用者資訊超載，自動隱藏與自己無關的服務。

圖 2. 左框動態產生之群組與系統清單

點選左框任一系統後，該系統首頁便會呈現在右資訊框的『我的結果』頁籤，並將頁籤標題以系統名稱取代；而為了運用有限的視窗空間，左框在被點選了某一服務後，會自動縮到最左只顯示一直行文字『系統清單』（圖 3），當滑鼠移到該行，系統清單會再自動彈出來。

除了系統選單可依 myNTU 的權限管理系統動態產生，個別系統的功能選單亦可以透過同樣的機制動態產生，使單一系統的功能可依不同使用者或角色區隔，提供不同的功能選單（圖 3）。

圖 3. 右資訊框內單一系統依據使用者角色動態產生之系統功能選單

III. MyNTU 之單一認證機制

A. *使用者帳號管理*

臺大校園資訊入口網站之單一認證乃採用計資中心所發放的 NTU email 帳號，因計資中心帳號室有最嚴謹的帳號發放與檢核機制，結合該帳號不但對使用者是一大便利，也免除各系統各自設置帳密的設計負擔、及管理者必須處理使用者忘記密碼時的麻煩。可用來登入入口網站的使用者帳號分為個人帳號與單位公務帳號兩種。個人帳號的發放機制，若是學生，是於新生入學時自動發放，而教職員工則必須透過申請程序取得，申請者必須已有一校內員工編號，然後依身分給予不同帳號別、享有不同的權限。學生畢業後成為校友，或編制內教職員退休，其帳號

皆可沿用，繼續取得該有的服務。若為離職員工，帳號即會被停用。

個人帳號管理所需的人員資料檔包含人員基本資料及在學/在職狀態，來自由教務系統及人事系統維護的學籍檔及教職員工檔，每日同步提供帳號系統使用。其中教職員工人員資料的整合最具挑戰性，因為除人事室管轄的教職員工外，還有研發處所管轄、流動性極高的計畫人員。本校因為組織龐大、校區分散、需求各異，無法引進坊間 LDAP [9] 產品來進行人事與帳號的管理，故完全由計資中心程式組內部開發人事相關之管理系統。雖然在整合過程中，費了相當大的努力在單位間進行協調與溝通，但由計資中心集中開發與管理，在整合上還是有較高的效益與彈性。

除了個人帳號外，對於開放給單位使用的服務，如張貼公告、發行電子報、活動報名管理等，則以單位公務帳號進行登入。帳號管理乃依人事室所維護的組織表，核准單位之公務帳號申請，若申請人退休或離職，必須有其他承辦人登記，方能繼續使用。

表 1. 帳號別與人員資料關係表

帳號別	人員檔	人員類別	資料來源	維護單位
學生	學籍檔	大學部、碩、博士生、進修推廣部學生	學籍檔	教務處
教師	教職員工檔	專兼任教師、研究人員	人事檔	人事室
職員		編制內職員/技工友、約用人員、專任計畫人員	人事檔 計畫人員檔	人事室 研發處
		單位自聘、全職工讀生	單位自聘人員檔	各單位
短期	線上輸入	臨時人員	來文申請	各單位
單位公務	單位檔	單位公務承辦人	組織表	人事室
校友	校友檔	已畢業學生	校友檔	秘書室

B. 身份認證模組 Session Service

由計資中心自行開發之身份認證模組 Session service，除進行驗證登入之帳號密碼是否存在外，並以 Web service 將使用者個人資料，包括學號/教職員編號、中文姓名、所屬單位、帳號狀態與帳號類別等，傳回給應用系統，以便系統進一步判斷，決定是否有權限使用。

資訊系統申請使用 Session service 時，為避免資料外洩，須全程使用 SSL (Secure Sockets Layer)，故必須確認所在 web server 有支援 SSL 連線，也就是 https 連線，並必須採用計資中心所簽發之電子憑證。

原則上 Session service 所提供的服務為帳號密碼之認證 Authentication，至於授權 Authorization 的部分則必須由個別資訊系統處理。雖然使用者可以享受到單一簽入的便利，但隨著使用者角色變化的客製化系統選單，系統開發者仍然需要各自處理系統內部功能的授權，造成系統開發的沈重負擔。因此目前新開發或具有較複雜權限控管的系統，皆已改採用 myNTU 所提供透過認證代理模組的權限查詢來處理有關權限的問題。

C. 認證代理模組 Session Service Proxy

過去 myNTU 入口網尚未建置前，應用系統必須逐一提供系統名稱、系統內容、作業系統版本、程式開發平台與環境、系統網址、主機位址、管理者姓名與聯絡方式等申請資料，登記存入 Session Service 資料庫，以便取得單一認證服務，無形中也增加 Session service 管理者的負擔。為了使同一伺服器下不同資訊系統，只需申請一次便可共享同一 Session service，於是有了 Session Service Proxy 的產生，現在系統只要加入 myNTU 後，便可經由 Session Service Proxy 直接取得服務。

應用程式可使用 NtuSessionKit 函式庫，透過 Session Service Proxy 建立 SessionKit 物件後，使用 SessionKit 所提供的屬性，讀取從 Session Service 取回的資料存入 Local Session 中。瀏覽器、應用程式、Proxy、Session Service、資料庫間所所執行的動作與發生的訊息交換等處理邏輯，依時間序以 UML (Unified Modeling Language) 呈現的循序圖 (Sequence Diagram) [10] 如圖 4。

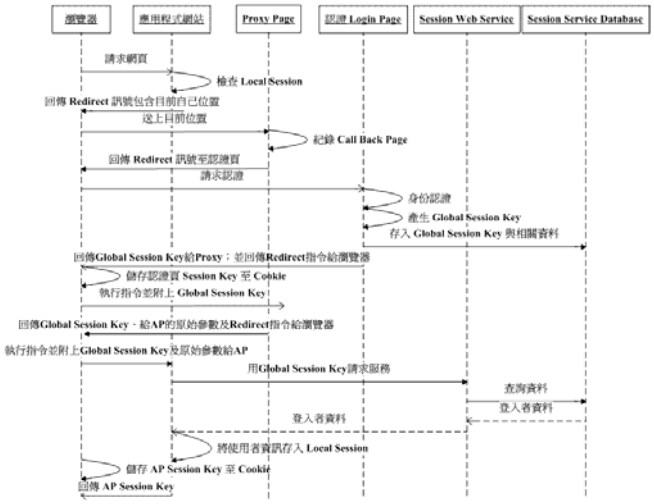

圖 4. Session Service Proxy 循序圖

Session Service Proxy 除提供同一台主機上 Session 交換之認證代理服務外，其最重要的功能為提供包括權限查詢、自然人憑證查詢、組織與人員查詢、E-Mail 寄件等介面之 Web Service，使系統共用之元件模組化，以重複利用、節省系統開發的人力與時程。其中權限查詢資料以權限管理資料庫為主，並具備 Cache 機制。Cache 資料每小時更新一次，因此於權限管理系統修改之權限資料，最長會有一小時的差異，其關係架構如圖 5。

權限查詢模組函式庫有三個主要的函式 GetInstance、GetFunctionList 與 GetPrivilege 分別掌管 Session Service 透通、取得系統列表與取得功能列表三種功能。myNTU 平台在使用者成功登入後，利用上述函式從權限資料庫取得權限資料之傳回值，將符合條件的資訊系統，動態產生可

執行之系統選單在群組裡，並進而動態產生所執行系統之功能選項。目前權限管理查詢模組可支援以 Visual Studio 2005 (Microsoft.NET 2.0 Framework) 所開發之 ASP.NET (Web Form) 程式。

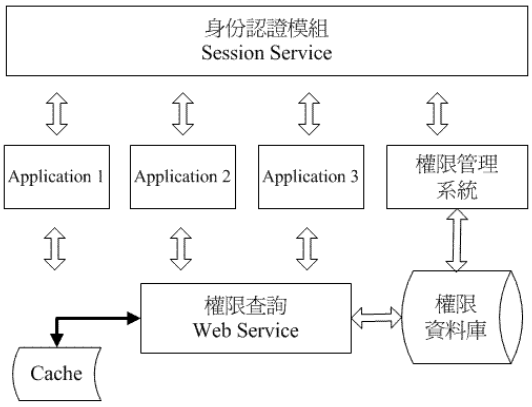

圖 5.身份認證與權限管理架構圖

IV. MYNTU 權限管理機制與設計

解決使用者單一簽入的問題後，如何打造一個個人化的入口網呢？這便屬於授權 Authorization 的課題。myNTU 的另一核心規劃，便是在解決如何依照個人的權限來呈現使用者可以享有哪些服務。

A. 權限管理系統需求概述

提供『權限系統管理者』可進行業務群組代碼維護與系統業務群組設定。業務群組是用來區隔資訊服務類別之用，再透過系統業務群組設定，使資訊系統可依個人或業務之群組別，被分門別類地呈現出來。

每一新加入 myNTU 之資訊系統，由『權限系統管理者』授權給該『資訊系統管理者』進入權限管理系統，去進行系統代碼維護與功能代碼維護。『資訊系統管理者』可指派業務單位負責授權的人為『業務管理者』，使其亦可自行增修角色代碼、角色功能設定與使用者權限設定。

權限管理系統除能為個人量身定作外，對於不是開放個人使用的一些公務系統，也可以用『單位權限設定』指定單位公務帳號在系統中所擁有的角色及功能。

B. 參數管理設計

1) 系統代碼維護

用以記錄某系統之相關資訊（系統名稱、正式/測試平台網址）、開放範圍（由該系統自管權限、是否 NTU 帳號全部開放、是否單位帳號全部開放、人員分類）及使用圖案（新上線系統、使用電子憑證）等設定參數（如圖 6），以便動態呈現系統清單。

舊有系統可經由此功能之『由該系統自管權限』設定，沿用原先設計的權限管控，而只需以帳號別（即人員別）設定來判斷是否顯示該系統。

而使用對象屬大眾的系統，可直接以『是否 NTU 帳號全部開放』或以『人員類別』參數來判斷是否顯示該系統。至於使用對象為少眾的管理系統，則需進一步靠『使用者權限設定』針對個人帳號以指派角色方式進行。

圖 6. 系統代碼維護畫面

2) 功能代碼維護

用以記錄某系統有哪些功能、及功能選單階層、排序關係功能路徑、是否全部開放等設定參數，再搭配『角色功能設定』及『使用者權限設定』功能，便可動態呈現屬於某角色的使用者可以看到的功能選單。

3) 群組代碼維護

用以記錄 myNTU 左視框系統清單之頁籤名稱（目前設定為『個人』及『業務』）、群組名稱、排序、及分類辨識用圖檔名稱，以便區隔系統清單要呈現哪些區塊。再搭配『系統群組設定』功能，便可使應用系統一一落在適當的區塊裡。

4) 系統群組設定

用以設定某系統編號所屬之分類、群組，及其序號，便於使用者直覺、快速地找到需要的服務。

5) 角色代碼維護

用以記錄某系統使用者可以有哪些角色代碼、名稱，再搭配『角色功能設定』及『使用者權限設定』功能，便可動態呈現屬於某一角色可以看到的功能選單。

圖 7. 角色功能設定畫面

6) 角色功能設定

用以設定某系統各角色可以執行哪些功能代碼（如圖 7），再搭配『使用者權限設定』功能，便可動態呈現屬於該角色可以看到的功能選單。

C. 使用者管理設計

1) 使用者權限設定

與業務有關的管理系統須要個別管控少數承辦人才能使用時，可利用此功能進行。以單位、職稱或姓名查詢到某人員，並從系統清單下拉選擇某系統後會自動列出已定義的角色，即可勾選該員所屬的角色（如圖 8）。

圖 8. 使用者權限設定畫面

2) 單位權限設定

提供一、二級單位下拉選單選定單位、並選擇某系統進行設定該單位公務帳號在某系統可以具備哪些角色。

V. 成效與未來發展

myNTU 入口網於 2008 年 7 月推出時，成功地整合了 72 個校務系統在同一平台上；經過 97 學年度的兩個學期後，提供服務的對象由原先全校 30812 在校生與 5821 位專兼任教師、職工，擴展到包含 2766 位專任計畫人員，且截至目前又增加了 30 項資訊服務。人事資料有效地整合，是促使單一入口成功的關鍵，而平台式、模組化的建構方式，則使系統開發的人力成本降低、也更有效率了。

從 myNTU 伺服器 web log 取得過去一年之每日成功登入 myNTU 的人數進行分析，發現週末 (星期六、日) 登入人數明顯低於上班日，並且在過去一年中沒有變化，將週末資料排除後，以僅包含上班日的 31 日移動平均觀察登入人數的趨勢變化，結果顯示：(1) 在每一新學期開始時都會有高峰期，(2) 下學期比上學期有明顯的成長。其登入人數分佈圖及上班日移動平均線如圖 9。

若取非高峰期上班日的登入人數來進行比較，去年十一月與今年六月的日平均登入人數，已由 1776 成長為 2800（數字本身看起來不大是因一旦登入成功，透過 session service 便可以取得其他資訊服務，不用重新登入），其使用率之成長幅度高達 58%。

此入口網除提供臺大教職員工生便捷與多元服務的資訊平台外，接下來要推展的工作尚有線上簽核、憑證推動及授權機制的建立。

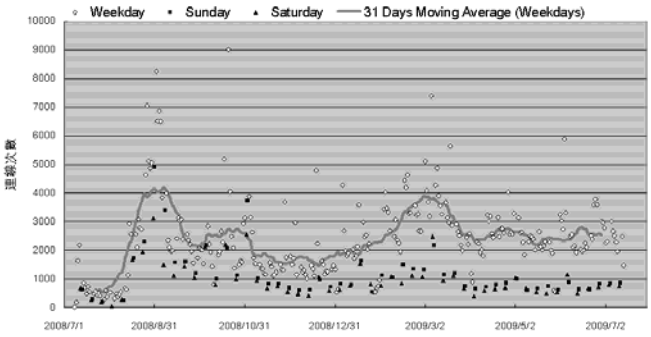

圖 9. myNTU 每日連線數量的分佈圖

A. 線上簽核與憑證推動

因應無紙化時代的來臨，下一波要推展的重要資訊服務是以電子簽章 [11] 進行線上簽核。為了使教職員能習慣使用自然人憑證進行簽核，逐步以推出部分電子表單，可用憑證刷卡進行線上申請，並於 2009/1/1 新差勤簽到退系統上線時，強制職員以憑證刷卡、進行線上簽到退。

目前進行中之國內外差假系統，將一改過去將假單列印出來蓋章的行政流程為線上簽核，各級行政主管將率先強制以自然人憑證進行假單簽核，作為將來公文線上簽核的試金石。

線上簽核最大的課題在簽核流程之設計，而系統預設簽核流程則必須建立在明確的組織架構與主管層級。面對複雜而又可能改變的人事規定，假單線上簽核作業經過一再地測試與單位、主管資料的檢核，及業務單位多次提出流程修改，最後才告底定，交叉分析結果顯示主要的流程在橫向有假別（未滿六日/六日以上差假/公傷假）、加班別（申請加班費/補休）、忘刷申請，而縱向則以人員類別（主管/副主管/非主管、計畫人員）來進行簽核流程之邏輯整理，盡可能使簽核流程之程式可以模組化，將來其他應用系統或電子表單也可以運用，朝建立共通的簽核平台而努力。

B. 授權機制的建立

過去為了讓各系所可以線上進行課程維護、導生資訊申報、公告張貼或其他業務，由計資中心提供各單位公務帳號，以登入應用系統執行與單位有關的資料維護與管理。隨著 e 化服務逐年新增，讓同一單位不同業務承辦人共用同一單位公務帳號進行登入，的確不易釐清資料維護的權責，而有資訊安全的潛在風險。單位帳號宜回歸由單位主管或其指派的人員進行管控，然後以單位帳號進行與單位業相關系統的授權，授權對象必須是持有 NTU 帳號之教職員工，有助於資訊安全的稽核。

至於個人業務代理的部分，目前計畫相關系統已有一套讓計畫主持人可以授權助理或學生幫忙處理線上聘僱申

請或報帳業務，差勤系統亦有主管授權秘書進行線上簽核的功能，為節省各應用系統各自開發授權頁面，擬將授權的機制也模組化，讓使用者有較便捷的管理授權的介面，也讓系統便於存取、共享授權資料庫。以既有 myNTU 權限管理系統的架構，進行擴充授權的管理，應是指日可待。

VI. 結論

臺大計資中心自行研發的單一入口網，不但造福了全校使用者不必在反覆登入，並減輕應用系統各自管理帳號密碼的負擔，認證之代理服務也大大降低了過去帳密大量在網路傳輸過程中被竊取的風險，對資訊安全來說是很大的助益。除提供新系統開發的共用模組，及身份辨識與權限控管，也能有效利用現有資源，將過去不同單位所開發的資訊系統一併融入，成為學術單位、研究單位完善的行政支援共通平台。

將來仍要繼續努力於線上簽核平台及授權機制的設計工作，以因應不斷成長的電子表單開發需求，提供全校師生更多元、更便利的服務。

參考文獻

[1] 臺大校園資訊網，http://info.ntu.edu.tw

[2] 陳啟煌，“服務導向架構 (SOA) 之校園全方位收費平台” TANET 2008 台灣網際網路研討會論文。

[3] The IBM Enterprise Information Portal: A Practical Approach, November 2000/10, http://www.redbooks.ibm.com/redbooks/pdfs/sg246101.pdf

[4] Single Sign-On, http://www.opengroup.org/security/sso/

[5] Ext JS: Cross-Browser Rich Internet Application Framework http://extjs.com/products/extjs/

[6] 劉建宏，“程式開發的利器 EXT (YUI-Ext)”, 2007/6/20, http://www.cc.ntu.edu.tw/chinese/epaper/20070620_1010.htm

[7] 吳江華，“微軟 ASP.NET 2.0 的 AJAX 利劍～ ASP.NET AJAX”, http://epaper.gotop.com.tw/pdf/ACL021700.pdf

[8] HTTP 處理常式和 HTTP 模組概觀 http://msdn.microsoft.com/zh-tw/library/bb398986.aspx

[9] 李維修、莊順清、劉見來、游文豪，“大學校園單一簽入機制之規劃與建置—以新竹教育大學為例.” TANET 2008 台灣網際網路研討會論文。

[10] Scott W. Ambler, “UML 循序圖的簡介”, 2001/1/11, http://tzuchieh.miroko.tw/Jyemii/umlcolumn/articles/umlwriting/tipuml03.htm

[11] 陳振寰，“電子簽章程式設計”, 2007/6/20, http://www.cc.ntu.edu.tw/chinese/epaper/20070620_1011.htm