利用自然人憑證整合校園資訊系統身分認證之規劃與實作

黃錦法　　李志朗
國立雲林科技大學 資訊管理系　　國立彰化師範大學 電子計算機中心
huangcf@mis.yuntech.edu.tw　　bob@cc.ncue.edu.tw

摘要

一般基於安全性考量，網路上的身分認證方式，大多會結合公開金鑰基礎建設（Public Key Infrastructure, PKI）認證機制。然而企業為了實現PKI機制，往往因此而自行建置憑證管理中心(Certificate Authority，CA)，自行發放及管理憑證。但因為建置上複雜度高、成本花費大且有許多技術上的問題需克服，實行上往往不是很順利，且企業自建 CA 所發放之憑證僅可應用於企業內部，在應用上缺乏彈性。

目前各大專院校之校園資訊系統大部分仍採用帳號密碼做為使用者身分認證方式，本研究最主要目的在於結合內政部憑證管理中心所簽發之自然人憑證，提出一個資訊系統開發架構，並將此一架構應用在校園資訊系統的開發上，以最經濟有效的方式將校園內部的資訊系統整合在一起。同時並根據此一架構進行系統實作，以初步驗證此一系統架構的可行性。

關鍵詞：公開金鑰基礎建設、數位簽章、自然人憑證、認證機制

Abstract

Due to the considerations of security, the authentication of information systems in the network always combine with PKI(Public Key Infrastructure) authentication mechanism. In order to realize PKI mechanism,enterprises often contruct CA(Certificate Authority) to grant and manage Certificates by oneself . But because of high complexity and costs and having a lot of technology problems need to overcome, it always fill of challenges, and the self-built CA of enterprise can only be applied within enterprises, lack flexibility in using.

Most of the information systems in campus are still adopt the account and password for user's identity authentication way. The main purpose of this research lies in combining Citizen Digital Certificate, propose an information system development structure, and apply this structure to campus,integrate the information systems within the campus in a most economic and effective way. In order to proof the feasibility of the architecture, a sample was implemented in the final.

Keywords: PKI、Citizen Digital Certificate, Digital Signatre、Authentication

1. 前言

傳統資訊系統在使用者身分認證上，大多是採用帳號密碼做為使用者認證方式，然而由於資訊系統不斷擴增，為登入不同的系統必須經常將帳號密碼等重要資訊暴露於網路之中，對系統的安全性是一大隱憂；對系統管理者而言，要管理這些使用者的帳號密碼更是一大負擔[3]。基於安全性考量，網路上的身分認證方式，大多會結合公開金鑰基礎建設（Public Key Infrastructure, PKI）認證機制。然而企業為了實現PKI機制，往往因此而自行建置憑證管理中心(Certificate Authority，CA)，自行發放及管理憑證。但因為建置上複雜度高、成本花費大且有許多技術上的問題需克服，實行上往往不是很順利，且企業自建 CA 所發放之憑證僅可應用於企業內部，在應用上缺乏彈性。

政府近來積極鼓勵民眾申辦由內政部憑證管理中心所負責簽發的自然人憑證，並推動各項自然人憑證之相關應用。自然人憑證的應用範圍廣泛且具有彈性，除了可應用於電子化政府之各項政府業務線上申辦外，亦可應用於企業之資訊系統開發上，企業應用自然人憑證，無需自行建置CA，可節省建置及維護管理成本，且政府亦提供相關的技術支援，讓政府機關學校及民間企業在應用自然人憑證的過程能更順利。[2]。

因應網路時代的來臨，各大學院校為提升行政效能、加快校園資訊流通速度，都致力於將現有資訊應用網路化，以提供更有效、更方便的資訊服務，校園資訊系統的規劃開發成為校務發展的重點工作項目之一。目前各大專院校之校園資訊系統大部分仍採用帳號密碼做為使用者身分認證方式，本研究最主要目的在於結合內政部憑證管理中心所簽發之自然人憑證，提出一個資訊系統開發架構，並將此一架構應用在校園資訊系統的開發上，以最經濟有效的方式將校園內部的資訊系統整合在一起。

2. 文獻探討

2.1 企業推動 PKI 遭遇到的問題

由於PKI對於目前的網路環境可以提供完整的安全保護機制，因此各企業無不積極的推動 PKI，

以強化網路環境的安全控管機制。然而根據相關研究[12]指出，一般在推動 PKI 的過程中常會遭遇到許多問題，使得在 PKI 的推動及應用上並不是非常順利。而在推動 PKI 所遭遇到的主要問題，前幾名分別為應用軟體不支援、成本太高、對 PKI 的認知不足及太強調技術層面等。

許多企業在推動 PKI 的過程中都會面臨一個問題，即是否需要自己建置 CA？企業內部自行建置 CA 最主要的好處在於企業可以自行簽發及管理憑證，不須透過公正第三者就可取得憑證，程序簡單快速且管理方便，且憑證的查詢及驗證更為快速。但其缺點為必須花費大量的成本，如購買硬體及軟體設備的費用、日後維護管理的費用等等，且憑證的維護管理較為複雜，技術層面較高，若管理人員技術能力不足或人員異動都可能會影響 PKI 機制的正常運作。因此企業在決定是否要自行建置 CA 之前，應先充分考量企業本身的條件再做最適當的選擇[5][12]。

2.2 我國 GPKI 與自然人憑證

為了實現電子化政府之目標，我國政府正積極的推動 PKI 之發展，以健全電子化政府基礎環境建設，並建立行政機關電子認證及安全制度。我國之政府公開金鑰基礎建設(Government Public Key Infrastructure，GPKI）架構如圖 1[4]所示，為一階層式的憑證管理架構，最上層為政府憑證總管理中心(Government Root Certification Authority, GRCA)，GRCA 下有許多的憑證管理中心，例如內政部憑證管理中心(MOICA)、工商憑證管理中心(MOEACA)、組織及團體憑證管理中心(XCA)、政府憑證管理中心(GCA)等，各自依照其不同的用途及對象來簽發及管理憑證。[1][4]其中內政部憑證管理中心負責自然人憑證的簽發作業，主要針對我國設籍登記滿 18 歲以上國民之自然人的公鑰憑證進行簽發及管理。

圖 1 政府公開金鑰基礎建設架構圖

自然人憑證是一張具有 PKI 機制之 IC 智慧卡，因此具有身分識別性、機密性、完整性、不可否認性的四大功能特性，利用此一機制可驗證使用者的身分，進而直接透過網際網路來進行各種相關的應用。

自然人憑證可應用的業務相當多，除了提供民眾電子認證與保護資料安全的功能外，自然人憑證也可應用在電子郵件加密安全簽章的應用上，可讓民眾收發電子郵件可以更安全，同時也可應用於政府機關及各企業內部之安全控管，透過自然人憑證來控管內部系統等。

目前自然人憑證發卡總數已超過 80 萬張，而利用自然人憑證開發的資訊應用目前已有電子公路監理、網路報稅、地政、戶政…等多項應用。由於政府的積極推動，未來利用自然人憑證的應用將會越來越普遍[1]。

2.3 數位簽章

數位簽章是以密碼學上的公開金鑰密碼系統（Public Key Cryptosystem)，又稱「非對稱密碼系統（Asymmetric Cryptosystem)」為基礎，每一位使用者擁有一對金鑰：一把密鑰（Secret Key）與一把公鑰（Public Key)。其中公鑰公佈於網路中，密鑰則由使用者自己保存。使用者可以利用自己的密鑰對文件進行簽署；而數位簽章的接收者可以利用該簽署者的公鑰來驗證數位簽章的有效性。數位簽章與電子文件的內容息息相關，亦即，同一位簽署者所產生的數位簽章，會隨著電子文件內容不同而有所不同[6][8]。

一個安全且有效的數位簽章，除了簽署者必須要以正確且有效的方法來對電子文件進行簽署外，其所產生的數位簽章之有效性亦需要一個合適的驗證方法來驗證。數位簽章機制（Digital Signature Mechanism）便是以密碼學（Cryptography）為基礎來定義安全的簽章產生與簽章驗證方法，此機制包括：簽章產生機制（Signature Generation Mechanism）與簽章驗證機制（Signature Verification Mechanism)。

「簽章產生機制」是指簽署者產生數位簽章的方法或程序，而此機制可視為一個數學演算法。若簽署者要進行簽署時，他可以將欲簽署的電子文件與自己所擁有的密鑰當作該演算的輸入值，經過該演算法的計算後便能得到電子文件的數位簽章。數位簽章產生過程如圖 2[8]所示。

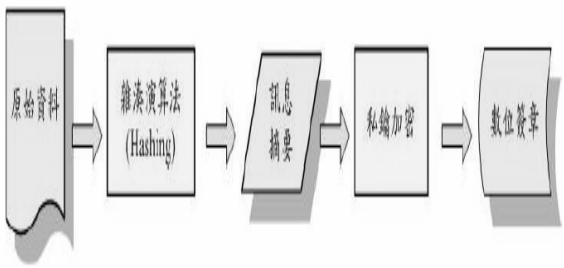

圖 2 數位簽章產生過程

「簽章驗證機制」是指驗證者用來驗證數位簽章之有效性的方法或程序。若是驗證者收到簽署者的電子文件與數位簽章時，他必須使用電子文件、數位簽章以及簽署者的公鑰，並且透過此機制來驗證此數位簽章的有效性。驗證數位簽章的過程如圖3[8]所示。

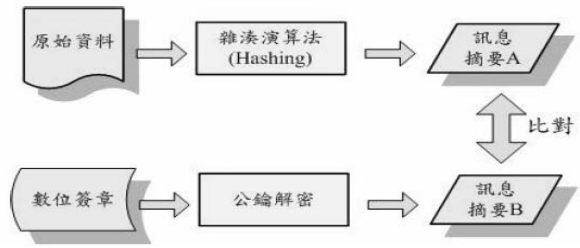

圖 3 數位簽章驗證過程

3. 系統開發架構

3.1 系統架構及組成元件

本研究主要提出一個以自然人憑證為認證基礎之校園資訊系統開發架構，此一系統架構結合內政部憑證管理中心所簽發之自然人憑證，整個系統架構如圖 4 所示。

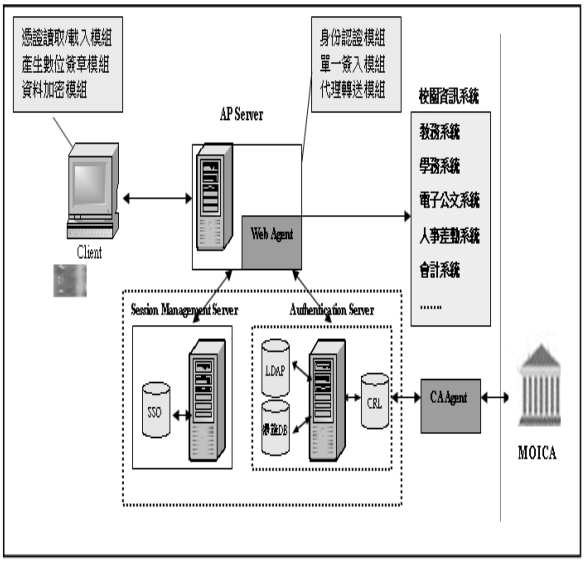

圖 4 系統架構

本研究所提出的系統架構主要由以下 6 個部分所組成：

1. Client 端：使用者利用瀏覽器提出資訊系統的服務請求，透過網頁自動部署 ActiveX COM 元件，執行以下模組功能：
   (1)憑證讀取/載入模組：執行自然人憑證安全性檢查、讀取使用者憑證資料(包括使用者姓名、身分證後四碼及憑證序號等資料)，並將個人憑證存檔後載入至憑證資料庫。
   (2)產生數位簽章模組：利用自然人憑證簽章金鑰產生數位簽章。
   (3)資料加密模組：負責使用者簽章及認證資訊的加密工作。
2. AP Server：所有資訊系統的控制中樞，除了負責接收及回覆使用者的服務請求外，同時透過 Web Agent 執行使用者認證工作，並將經認證成功後的使用者導向至所要求的應用服務。其中 Web Agent 為 AP Server 的一模組化元件，執行以下模組功能：
   (1)身分確認模組：透過認證伺服器驗證使用者簽章並確認使用者身分。
   (2)單一簽入模組：透過連線管理伺服器執行使用者單一簽入任務。
   (3)代理轉送模組：認證成功後，將使用者導向至所提出之應用服務。
3. 校園資訊系統：負責提供使用者各種不同的校園資訊系統應用服務，如教務系統、學務系統、電子公文系統、人事差勤系統…等。
4. 連線管理伺服器(Session Management Server，SMS)：負責管理維護使用者的 Session 連線資訊，接受 Web Agent 的單一簽入連線請求，並將結果傳回給 Web Agent。
5. 認證伺服器(Authentication Server，AS)：主要負責使用者個人身分認證工作，驗證使用者簽章並傳回認證結果。認證過程需要使用者的相關資料，包括使用者基本資料、個人權限(Authorization)資料、個人憑證及憑證廢止清冊等。
6. CA Agent：負責連線至內政部憑證管理中心，執行自然人憑證廢止清單的更新工作。第一次建置時下載完整的廢止清單，建置完成後則為每天自動下載廢止憑證的異動清單，並更新至內部資料庫。

3.2 簽章產生及驗證方式

利用數位簽章做簽章驗證的詳細運作方式如圖 5 所示，主要由客戶端產生數位簽章，並由認證伺服器端執行數位簽章的驗證工作。

使用者輸入正確的自然人憑證 IC 卡 PIN 碼後，透過客戶端的模組元件取得自然人憑證簽章用私密金鑰的控制指標並產生數位簽章，將簽章及認證資訊加密後透過 SSL 加密連線傳送至伺服器端；伺服器端則將認證資訊解密後，並以使用者的公開金鑰對簽章做驗證，以確認使用者簽章的正確性及使用者的身分。

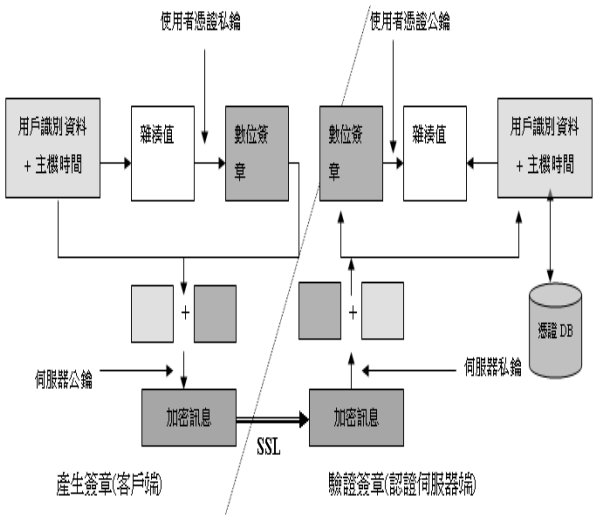

圖 5 數位簽章驗證過程

客戶端所傳送至認證伺服器端的訊息內容為：

$$MSG = E_{Pus.}[\ CONT + SIGN\ ]$$

$$CONT = [\ USRname + USRid + TIMEs\ ]$$

$$SIGN = E_{Prc.}[\ H(\ USRname + USRid + TIMEs\ )\ ]$$

MSG：客戶端傳送至認證伺服器端的加密訊息。

$E_{Pus.}$：利用認證伺服器之公開金鑰做資料加密。

CONT：客戶端的個人識別資料。

SIGN：自然人憑證之私密金鑰產生之數位簽章。

USRname：自然人憑證 IC 卡讀出之用戶姓名。

USRid：自然人憑證 IC 卡之用戶身分證後四碼。

TIMEs：認證伺服器主機時間。

$E_{Prc.}$：用戶自然人憑證之私密金鑰。

H：雜湊函式。

使用雜湊及數位簽章可確認使用者身分並確保資料未被篡改之完整性。而為確保傳送的訊息不會遭到他人竊取或冒名重送，在簽章的訊息內容部分，除了個人識別資料以外，並加上認證伺服器之主機時間做為簽章的訊息內容，以確保傳送的訊息是在有效期限內；同時以認證伺服器之公開金鑰對訊息做加密，以確保只有認證伺服器才可以收到此一加密訊息。

伺服器端利用使用者憑證中之公開金鑰來驗證使用者數位簽章之正確性，而自然人憑證 IC 卡中內含兩張個人憑證，一為數位簽章用，一為資料加解密用。每張憑證的大小約為 1.1K Bytes。基於傳輸速度及安全上考量，本研究以自然人憑證中用戶姓名及身分證後四碼(約 10Bytes)當做個人識別資料，而不傳送整個憑證至伺服器。而用戶的自然人憑證公開金鑰則事先儲存於伺服器中，可利用個人識別資料自憑證資料庫中取得。

4. 系統實作與實例展示

為驗證本研究所提出系統架構的可行性，我們依據此一系統架構建置了一個可以實際運作的系統環境。

4.1 系統實作

在自然人憑證相關功能的實作上主要包括 IC 卡憑證資料的讀取及載入、產生數位簽章、驗證數位簽章、憑證廢止清冊解析、資料加解密等部分，主要採用 C++程式語言，透過內政部自然人憑證管理中心所提供的 HiSECURE API 來撰寫相關應用程式。採用 HiSECURE API 最主要的原因在於 HiSECURE API 為政府委託中華電信數據分公司開發之自然人憑證 IC 卡應用程式 API 介面，開發上較為快速方便。

為提供在 Web 上執行自然人憑證相關程式功能，我們採用 ActiveX 技術，將 C++程式編譯成可在瀏覽器上運作的 ActiveX COM 元件，供客戶端自動下載執行。同時我們也採用動態連結函式庫(Dynamic Link Library,DLL)技術，將 C++程式編譯成 DLL 檔，以提供不同程式語言所開發的應用系統一個共同的存取介面。

使用者簽章驗證的方式，主要為安裝 Apache HTTP Server 2.0，將自然人憑證簽章驗證功能之 C++程式編譯成執行檔，並利用 PHP 開發相關模組功能程式，以執行簽章驗證功能。相關的資料庫元件，如憑證 DB、CRL 及 LDAP 部分，實作上皆以 Oracle 資料庫來儲存相關資料。

憑證廢止清冊的處理，主要係利用 VB 開發憑證廢止清冊自動下載程式，並以 C++語言透過 HiSECURE API 實作自然人憑證廢止清冊解析功能。

在使用者介面方面，為整合所有校園資訊系統，本研究採用 JWS(JAVA Web Start)技術，建立 Web 化的系統整合入口，讓使用者可於 Web 網頁環境下執行。因此，客戶端除了要有瀏覽器及安裝執行 C/S 架構資訊系統所需的應用程式外，還必須安裝 JRE(Java Runtime Environment)，以透過 JWS 執行系統整合入口的 JAVA 程式。

AP Server 與客戶端及不同的網站伺服器(PHP、JSP 或 ASP…)間的運作方式如圖 6 所示，執行自然人憑證功能之 ActiveX COM 元件存放至同一 AP Server，以提供客戶端瀏覽時自動佈署執行，且不同的網站伺服器在運作時皆透過同一 AP Server 代理轉送，共用同一 AP Server 所有的功能及元件。因此實作時網站應用程式幾乎可不需做修改即可正常運作。

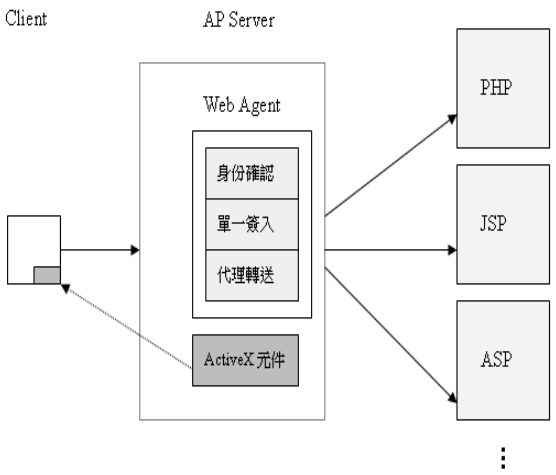

圖 6 AP Server 與客戶端元件運作方式

4.2 實例展示

本研究實作之雛型系統主要包括系統管理程式、校園資訊系統及登出等三個選單(圖 7)。

系統管理程式的功能選單主要有二個功能，分別為系統使用者管理與憑證廢止清冊(CRL)處理作業，其中系統使用者管理作業主要提供使用者個人基本資料建檔及使用權限設定等功能，使用者插入自然人憑證 IC 卡後，選擇新增使用者功能，系統將自動從自然人憑證 IC 卡中取出個人憑證基本資料，包括憑證序號、姓名、身分證後四碼等資料，並將個人憑證存成憑證檔，設定個人基本資料及系統存取權限後，利用存檔功能可將個人資料及個人憑證檔儲存於伺服器端，並出現作業執行成功的畫面。

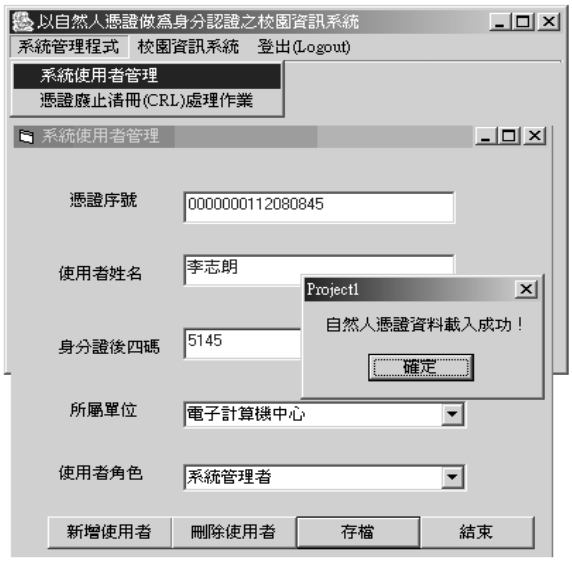

圖 7 系統使用者管理畫面

憑證廢止清冊處理功能(圖 8)最主要為連線至內政部憑證管理中心下載憑證廢止清冊，並更新內部資料庫。此一處理作業可利用排程於每天固定時間自動執行。

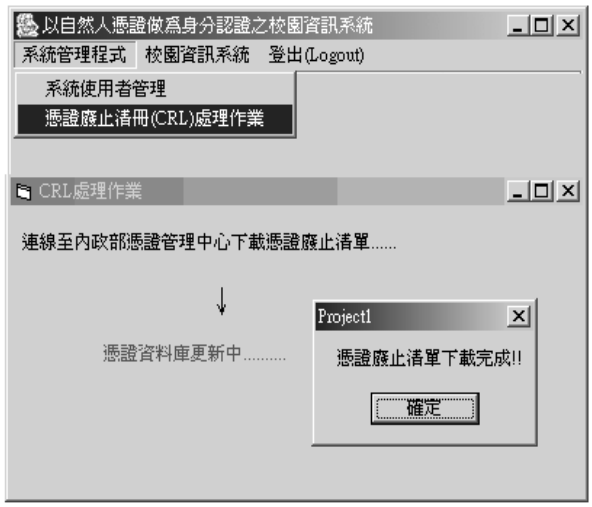

圖 8 憑證廢止清冊處理畫面

校園資訊系統主要提供二個系統，分別是 Web 公文製作系統及公文管理系統。

圖 9 為當使用者選擇任一資訊系統時，如本實例選擇的是 Web 公文製作系統，會先連線至 AP Server 的校園資訊系統單一簽入畫面(圖 9)，若使用者電腦尚未安裝具有自然人憑證功能之 Activex COM 元件，則會要求使用者自動下載安裝此一元件，透過 Activex COM 元件執行自然人憑證相關功能，一開始會先讀取 IC 卡憑證資料以確認使用者的簽入狀態；若使用者尚未成功簽入，則會要求使用者輸入自然人憑證的 PIN 碼產生簽章，並將簽章資訊送至伺服器端。

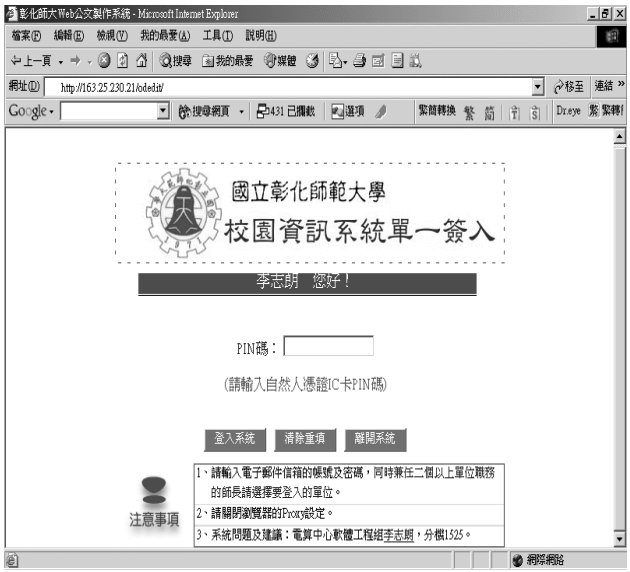

圖 9 校園資訊系統單一簽入畫面

AP Server 接收使用者的認證資訊後，會將認證資訊透過 Web Agent 傳送至認證伺服器驗證，認

證伺服器會檢查使用者權限及驗證使用者所送過來的簽章是否正確，並將認證結果傳回 AP Server，若使用者成功通過認證，則將使用者導向至所要求之資訊應用服務(圖 10)。

圖 10 成功登入系統畫面

5. 結論與未來工作

本研究主要提出一個結合自然人憑證認證方式的校園資訊系統開發架構，自然人憑證除了可應用於校園內部資訊系統外，亦可應用於其他的資訊服務，應用範圍廣泛且無須額外的建置費用。

本研究所建構的系統運作架構主要以模組元件的方式來開發，可減少開發時間及增加服務元件的重覆使用，加速校園資訊系統的開發及整合，讓校園的資訊應用能達到最大的成效。

不同的校園組織規模及資訊系統特性可能會有不同的複雜度及問題。未來將針對以下幾點做進一步的探討：

1. 在多使用者同時上線的環境下，對資訊系統整體效能(Performance)的影響，是否會造成瓶頸或是效能的下降？
2. 受限於開發環境及使用的開發工具，本研究的實作系統在客戶端部分主要針對 Windows 作業系統環境來開發。未來的研究可針對如何提供一個跨平台的系統做更進一步的探討。

參考文獻

[1] 內政部憑證管理中心網站，2004，*http://moica.nat.gov.tw*。

[2]王國榮，”VB5 & ActiveX 程式設計”，旗標出版社。

[3]朱建達，2001，”建立於公開金鑰基礎建設的單一簽入系統”，國立交通大學，碩士論文。

[4] 政府憑證總管理中心網站，2004，http://grca.nat.gov.tw/cindex.htm。

[5]林誠，2004，”E化宜蘭縣府公文整合與線上簽核的平台”，2004台灣網際網路研討會。

[6]周伯錕，2003，”利用智慧卡之遠端身份認證之研究”，國立中興大學資訊科學系，碩士論文。

[7]蔡明志，”Visual C++ 6 教學手冊”，碁峰資訊。

[8]劉廷楷，2003，”電子病歷分享系統中安全技術之設計與實作”，私立東海大學資訊工程與科學系，碩士論文。

[9]顏志臻，2002，”運用公開金鑰基礎建設 生物認證技術及Kerberos 建構一個應用於分散式系統之安全認證機制”，國立清華大學電機工程學系，碩士論文。

[10] Satoh, F. and Itoh, T. ,2004,”Single Sign On architecture with dynamic tokens”,Applications and the Internet, 2004. Proceedings. 2004 International Symposium on,197 – 200.

[11]Liang, S., The Java Native Interface Programmer's Guide and Specification, Addison-Wesley, 1999.

[12]Peter Doyle and Steve Hanna,2003,”Survey on Obstacles to PKI Deployment and Usage”,Prepared and Published by the OASIS Public Key Infrastructure Technical Committee.

[13]Peter Kohler,2004,”Simple Single Sign-On Solution for Web Applications”,SANS Institute.

[14]Vipin Samar,1999,”Single sign-on using cookies for Web applications”,In Proceedings of the 8th IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises,158--163.