以 LAPM 架構整合自然人憑證實務應用之研究

陳奐瑀　　高元宏　　祁苗豐
國立臺中技術學院 資訊管理系
hychen@ntit.edu.tw　kevin@darkblue.idv.tw　chi.clom@msa.hinet.net

摘要

隨著網路資訊的腳步愈來愈快，建立安全及可信賴的電子認證機制，確保資訊在網路傳輸及儲存過程中之安全性，是電子交易能否普及應用的關鍵。本研究以建構一安全的電子商務交易平台為目標，採用 LAPM（Linux OS Server **架設** Apache Web Server、PHP **程式語言、**MySql **資料庫）的程式架構，除了以常見的雙向** SSL **資料加密傳輸外，特別針對近年來政府與業界大力推展的公開金鑰基礎架構（**Public Key Infrastructure**，**PKI**）進行研究。同時為配合「自然人憑證」的推廣，本研究之** PKI **實務應用，採「自然人憑證」驗證使用者身份，以達可認證性與不可否認性，並將研究成果結合電子購物車網站，以完成本研究之目標。**

關鍵詞：公開金鑰基礎架構、自然人憑證、智慧卡、SSL、RSA。

Abstract

With steps of information moving, it is the key of extensive application of electronic transactions that established under security and reliability of electronic identification system and ensured safety of the information in a process of network transfer and storage. The goal of this research is that build a secure platform of commercial electronic transactions. The server program of this research started with construction of LAPM (Apache Web Server established on a Linux OS Server + PHP language + MySql database). In addition to common two-way SSL information of encryption transferred, it is aimed at further research of the Public Key Infrastructure (PKI) popularized by the Government and industry these years. In the meantime, matching up popularized of Nature Person Token, the application of PKI of this research adopt Nature Person Token which to verify users' identification to prove ones' authentication and non-repudiation, and also achieving our goal that combining result of research with website of electronic shopping car.

Keywords : Public Key Infrastructure（PKI）、Natural Person Token、Smart Card、SSL、RSA.

1. 前言

現今網路系統快速發展，進而帶動電子商務的迅速進步，相對的人們對電子商務的需求也是日益倍增，但是隨之而來資安問題卻是不容忽視。為了因應未來網路系統發展趨勢和前景，電子商務系統需具備公平與安全的交易機制，藉以保障消費者與電子商務業者，進而達到消費者買的安心，業者賣的放心的雙贏目的。並期能製造一個安全的網路使用環境，使網路上不安全的議題進而減少，促進一安全、便利的網路使用環境。政府自民國八十九年就開始對電子憑證進行設計與規劃，並委由中華電信數據分公司進行系統建置，同時電子簽章法亦在立法院審議，並於民國九十年十月三十一日完成三讀之立法程序，自此我國的數位簽章有了法律的規範與正式的地位。到了九十二年，內政部已完成電子憑證相關系統建置，並於當年年底開始大力推行自然人憑證的申請，及加速推廣其應用範圍。本研究以現今電子商務的普及化與技術的多元化，本著自由軟體開放的精神，進行以 LAPM **架構整合自然人憑證實務應用之研究。**

2. 文獻探討

2.1 電子商務與資訊安全

依據 CommerceNet [1]**之研究報告，十大電子商務阻礙之首項為「安全」與「加密」。電子商務交易無法保證** 100%**安全，目前資訊在網際網路上傳送，尚有被第三者竊取或變造的可能，特別是敏感的個人及財務重要資訊(如：帳號及密碼、信用卡卡號)；而資料庫或網路資源仍有被駭客侵入，而導致資料被破壞、塗改、洩漏或濫用的可能性。**

為推動電子交易之普及運用，確保網路交易的安全性，促進電子化政府及電子商務的發展，全球各國紛紛立法通過電子簽章法案，確立電子簽章與電子文件的法律效力，並建構公開金鑰基礎建設(Public Key Infrastructure**，**PKI**)，使網路交易達到資料傳輸來源身分辨識、資料隱密性、資料完整性、及不可否認性等安全需求。**

RSA **為目前最著名的公開金鑰密碼系統，是由三位** MIT **的學者** Rivest、Shamir **與** Adleman **於** 1978 **年提出。**RSA **密碼系統可作為加解密、數位簽章、金鑰交換等之用**[2]**，其安全性是建立於因數分解(**factorization**)的困難度。因數分解(**FAC**)問題是指給**

定一合成數 n 為兩個大質數 p 與 q 的乘積，欲分解 n 為計算上不可行，此問題是一個 NP-complete 問題。為了增加安全度，訊息簽署前可以先經過一個單向雜湊函數 h 的轉換再進行簽署，亦即 $s = h(m)^d \bmod n$。RSA 的安全度建立於分解大合成數 n 的困難度。A. Lenstra(1994)已可成功地分解出 RSA 129 位數。為確保至少五年內之安全度需求，建議 RSA 的金鑰長度(亦即模數 n 的大小)要達到 1024 位元以上才算達到安全。

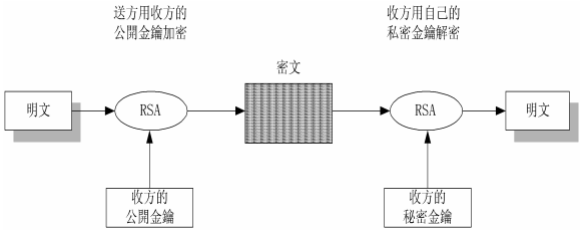

圖 1 RSA 加密解密原理圖示

2.2 SmartCard

一般 IC 晶片卡，根據卡片內部的 IC 線路設計之不同，可劃分為記憶卡（Memory Card）與智慧卡（Smart Card）兩類，前者如預付卡、電話卡，後者如金融卡、GSM 卡等。而由於 IC 卡內本身即已包含了 CPU、ROM、EEPROM、RAM 等元件，所以 SmartCard 就有如一台可隨身攜帶的微型電腦般，可用來儲存及處理重要資料。目前的二代晶片卡可以將金鑰放進上述受到保護的儲存資料區域，於是密碼運算的作業，包含金鑰的選取到使用，就可以完全在卡片內部完成。使用者只需要將資料丟進卡片裡，等它把運算結果傳出來即可。除了傳統的記憶單元外，內建的運算功能(CPU)可以讓加解密的動作在晶片卡內部完成，而不是透過讀卡機或外接裝置運算，也不必將私密金鑰讀出到電腦上執行運算，阻絕了私密金鑰被駭客程式? 用的機會，大幅增加安全性。

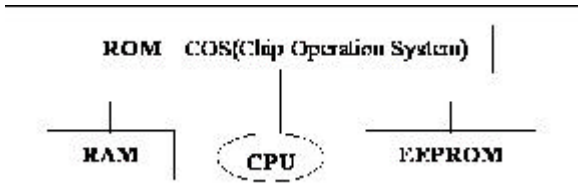

圖 2 晶片卡結構圖

2.3 公開金鑰基礎建設架構

公開金鑰基礎建設(Public Key Infrastructure, PKI)是以公開金鑰密碼學技術為基礎而衍生的架構，在電子訊息傳遞與交換過程中，提供訊息的身分鑑別(Authentication)、資料完整(Integrity)、不可否認性(Non-Repudiation)與隱密性(Confidentiality)等資訊安全四大需求功能。

PKI 基本成員：

2.3.1 CA (Certificate Authority)憑證控管中心：憑證簽核、註銷及 CRL(作廢或失效的憑證資料，如黑名單)產生，提供企業組織內部 PKI Solution，與 AP 整合，強化安全性。例如：身分認證系統、電子公文系統、電子交易系統、電子郵件系統。

2.3.2 RA (Registration Authority)註冊管理中心：憑證申請、撤銷之管理窗口，可連結多憑證控管中心與系統稽核登錄 (Audit Logs)。

2.3.3 DS (Directory Server)目錄伺服器：個人資料及憑證狀態查詢，遵循 LDAP 標準，可進一步整合系統登錄服務(Single Sign-On 整合機制)。

2.4 自然人憑證

自然人憑證就是「電子身分證 IC 卡」，也就是「網路上的身分證」。所以自然人憑證就如同實體世界的印鑑，用以在網路世界中代表持卡者的身分證明，同時也可用以簽署需證明身分之電子文件。國內之自然人憑證是由「內政部憑證管理中心」(MOICA)[3]統籌建置與規劃，自然人憑證係遵循 X.509 v3 的標準格式，包含：基本欄位、擴充欄位與 CA 簽章等三部份（如下表 1）。

表 1 自然人憑證格式欄位內容

基本欄位	憑證格式版本
	憑證序號
	簽章演算法
	簽發者名稱
	憑證有效期限
	主體識別名稱
	持有者公鑰
	簽發者唯一識別碼
	主體唯一識別碼
擴充欄位	金鑰用途
	憑證政策
	金鑰識別碼
	基本限制
	CRL 公佈點
	用戶目錄屬性
	……
	CA 簽章

3. 系統設計與架構

3.1 研究架構

本研究採程式開發與實務測試為主，資料蒐集與理論性研究為輔。先建置一電子商務平台，再逐步對其進行安全性測試與安全機制之建構，藉由不

斷的測試來進行安全機制的研究與建置，以能有實務性的成效，並能確實達到安全的電子交易平台要求。

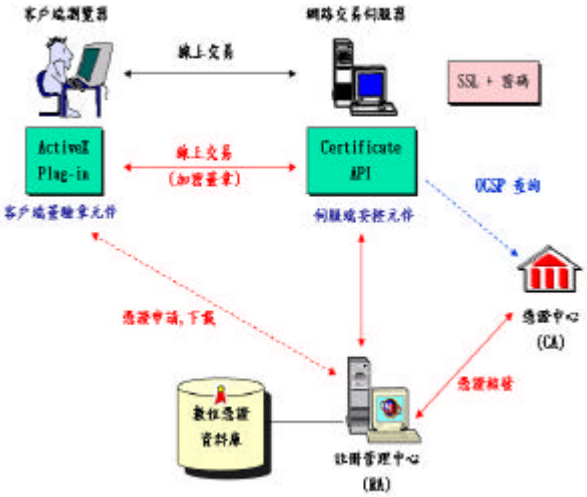

圖 3 本研究架構圖

3.2 系統設計

為了能兼顧快速、穩定及安全性等要求，本研究採用「LAPM」(Linux OS Server 架設 Apache Web Server + PHP 程式語言 + MySql 資料庫)的程式架構開發電子商務平台，同時亦是考量自由軟體推展與技術純熟度。根據 Netcraft[4]的研究指出，目前已經有超過 40%的網站使用 PHP 環境，而且中小企業與大型企業的使用度都有穩定的成長，尤其是該架構的成本最為低廉，其技術性更是經得起考驗，所以本計劃使用「LAPM」的程式架構。同時亦是為了促進自由軟體的開發與發展，藉以加速自然人憑證在實務上的推廣。

在 Client 端的部份，為能快速開發與解決技術限制問題，本研究採用 ActiveX 程式整合有關 API 元件，以能解決網頁瀏覽器驅動讀卡機問題；同時使用 JavaScript 程式語言做為 Client 端使用者網頁操作控制，處理 ActiveX 元件的執行、回應及資料的傳遞（如下圖 4)。唯 ActiveX 僅能在微軟 IE 瀏覽器上執行，是為其不足之部份，後續學者可採用 Java Applet 開發 Client 端程式介面，以能達到跨平台與多種瀏覽器執行。

圖 4 系統設計架構圖

4. 系統實作

4.1 電子商務平台架設

本研究之電子商務平台是使用「LAPM」架構，以 RedHat 9.0 內建的 OpenSSL 函式庫 SSL 加密機制的建立，與 Apache 伺服器中 mod_ssl 安全模組採用模組化程式設計，使程式開發與管理更加方便與容易；網頁安全伺服器使用 Secure Sockets Layer（SSL）通訊協定與來自 Certificate Authority（CA）的數位憑證做結合，本研究採「自我簽署憑證模式」以 OpenSSL 產生 RSA（1024Bits）的金鑰憑證（如下圖 5)，以提供資料加密傳輸之安全性。並且提供各項網頁管理工具，使用者可隨意就其喜好對網頁版面做有限度的變更（如下圖 6)，例如：Logo、顏色、按鈕、廣告連結、商品說明、電子報設定、會員及訂單管理…等等，多樣化的選擇與組合，以滿足電子商務求新、求變之需求。

為達本研究之目的，網站會員身分驗證的部份，以傳統輸入會員帳號、密碼驗證模式和使用自然人憑證輸入 PIN 碼驗證模式一併呈現，除了可讓使用者有便利性的選擇外，亦可充份比較其差異性（如下圖 7)。

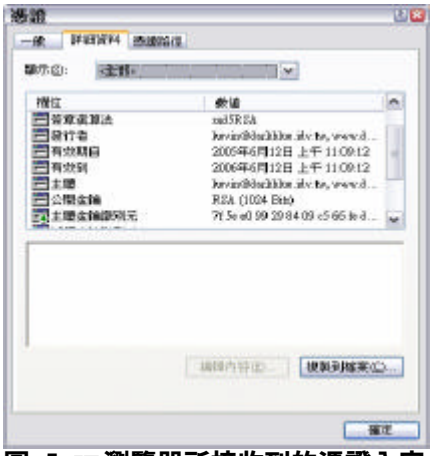

圖 5 IE瀏覽器所接收到的憑證內容

圖 6 網站系統版面設定

圖 7 網站系統登入畫面

4.2 ActiveX元件設計

在 Client 端的 ActiveX 元件設計，主要是將自然人憑證安全保密程式介面（API）[5]所提供之功能加以整合，並以物件導向的程式設計觀念製作出可供 JavaScript 程式呼叫的函式，包含讀卡機的使用判斷、憑證資料的擷取、憑證是否有效及擷取出的憑證資料分析，包含錯誤訊息的回應等（如下圖 8、9、10）。

API 程式介面元件函式架構，主要提供四大功能：資料加解密(對稱與非對稱)、數位簽章與驗證(SHA1 with RSA)、憑證資訊的取得、憑證廢止驗證(CRL 及 OCSP)。其主要函式介面架構如下：1.密碼模組部份：以 PKCS11 為基礎，處理資料加密、簽章的產生及驗證等功能。2.憑證及憑證廢止清單解析部份：取得憑證內部資訊及查詢憑證廢止狀態。3.網路相關部份：目前僅提供 OCSP 函式，供即時的憑證狀態查詢功能。本研究主要以取得憑證內部資訊以進行身分認證之作業，並透過 OCSP 函式查詢使用者憑證狀態。

API 元件函式呼叫流程，1. 密碼模組部份：起始密碼模組 (InitModule)、起始運作環境 (InitSession)、取得金鑰控制指標 (GetKeyObjectHandle)、呼叫密碼相關函式、釋放金鑰資源 (DeleteKeyObject)、結束運作環境 (CloseSession)、結束密碼模組(CloseModule)。2. 憑證解析部份：取得憑證資料、轉為憑證基本結構、取出憑證資訊結構(此時已可取出一些基本資料，但不包含憑證延伸欄位)、取出個別憑證延伸欄位、取出所要資料。3. 憑證狀態查詢部份：取得憑證廢止清單、轉為憑證廢止清單基本結構、呼叫憑證狀態查詢函式、取得憑證狀態。4. OCSP 部份：產生 OCSP 查詢結構、產生 OCSP 查詢封包資料、自行對 OCSP 查詢封包資料簽章(非必要條件)、執行 OCSP 查詢動作。

圖 8 IC卡未插入錯誤訊息

圖 9 IC卡讀取錯誤訊息

圖 10 瀏覽器未啟動 ActiveX 設定錯誤訊息

4.2.1 載入所需的API元件：

包含 BfiveUcs.dll、GPKICardFunction.dll、CHTHiSECUREParsingva.dll、UCSBFive.dll。

4.2.2 自卡片內取出憑證：

```
int iRetValue;
int iCertID = 1 ; // 取出卡片內部第一張憑證
unsigned char *pCertfromICCard = NULL;
int iCertLength = 0 ;
char *sReadName = NULL ;
// 呼叫兩次 GetCertificateFromGPKICard
// 第一次目的為取得憑證的正確長度
iRetValue =
GetCertificateFromGPKICard(iCertID,
pCertfromICCard, &iCertLength, sReadName);
// 宣告足夠大的記憶體空間,此函式才能正確動作
pCertfromICCard = new unsigned
char[iCertLength];
iRetValue = GetCertificateFromGPKICard
(iCertID, pCertfromICCard, &iCertLength,
sReadName);
```

```
FILE *ff;
ff = fopen("user.cer ", "wb");
fwrite(xxx, certlen, 1, ff);
fclose(ff);
if( iRetValue != 0) {
printf("無法取得 IC 卡憑證!\n");
return -1;
printf("取得 IC 卡憑證, 內容如 user.cer 所示
\n");
      }
```

4.2.3 自卡片內取出憑證：

```
int iRetValue;
FILE* pCertFile;
unsigned char* pInData;
int iInDataLength = 0 ;
// 開啟憑證檔案, 檔案須存在
if( (pCertFile = fopen( "user.cer", "r+b" )) ==
NULL ){
printf( "The file was not opened\n" );
return -1;
}
// 計算檔案長度
fseek( pCertFile, 0, SEEK_END); // 先把讀寫
位置移到檔尾
iInDataLength = ftell( pCertFile ); // 再傳回檔
案目前的讀寫位置
// 重新讀取檔案進 pInData
fpos_t pos = 0 ;
fsetpos(pCertFile, &pos);
pInData = new unsigned char[iInDataLength];
fread(pInData,sizeof(unsigned char),
iInDataLength, pCertFile);
// 關閉檔案
if( fclose( pCertFile ) != 0 ){
printf( "The file was not closed\n" );
return -1;
}
CertBasicStruct sCertificate;
char ppchDN[512];
// 開始憑證解析步驟
iRetValue = DecodeCertificate(pInData,
iInDataLength, sCertificate);
// 取出憑證 IssuerDN
iRetValue = GetCertSubjectDN
(sCertificate,ppchDN);
printf("Issuer DN: %s\n",ppchDN);
char c;
scanf("%c",&c);
free(pInData);
CertBasicStructDestructor (sCertificate);
return 0;
```

4.2.4 取得憑證有效期限：

```
int iRetValue;
FILE* pCertFile;
unsigned char* pInData;
int iInDataLength = 0 ;
// 開啟憑證檔案
if( (pCertFile = fopen( "user.cer", "r+b" )) ==
NULL ){
printf( "The file was not opened\n" );
return -1;
}
// 計算檔案長度
fseek( pCertFile, 0, SEEK_END); // 先把讀寫
位置移到檔尾
iInDataLength = ftell( pCertFile ); // 再傳回檔
案目前的讀寫位置
// 重新讀取檔案進 pInData
fpos_t pos = 0 ;
fsetpos(pCertFile, &pos);
pInData = new unsigned char[iInDataLength];
fread(pInData,sizeof(unsigned char),
iInDataLength, pCertFile);
// 關閉檔案
if( fclose( pCertFile ) != 0 ){
printf( "The file was not closed\n" );
return -1;
}
CertBasicStruct sCertificate;
// 開始憑證解析步驟
iRetValue = DecodeCertificate(pInData,
iInDataLength, sCertificate);
struct tm tmBeginDate;
struct tm tmEndDate;
// 單純取出憑證有效期限
iRetValue = GetCertValidity (sCertificate,
tmBeginDate, tmEndDate);
printf("Valid from: %s\n",
asctime( &tmBeginDate ) );
printf("Valid to: %s\n",
asctime( &tmEndDate ) );
char c;
scanf("%c",&c);
free(pInData);
CertBasicStructDestructor (sCertificate);
return 0;
```

5. 結論與建議

經由本研究透過實務的系統程式設計與測試，可將自然人憑證整合電子商務交易平台，以達到安全的電子商務網路交易之要求：隱密性(Confidentiality)、完整性(Integrity)、可認證性(Authentication)及不可否認性(Non-repudiation)。本研究主要成果如下：1.建立模組化之安全電子商務平台：透過模組化的程式設計，提供網路商家多樣化的網頁版面與商務需求組合，並確保使用者之資料安全性。2.以 LAPM 整合自然人憑證驗證作業：使用者可利用自然人憑證取代原先要輸入網站會員帳號與密碼的會員登入認證作業。3.使用雙向 SSL 資料傳輸加解密機制：使伺服器與瀏覽器端之間的資料傳輸獲得保障，避免資料傳輸時輕易被有心入士攔劫與破解，以達到資料的隱密性。

參考文獻

[1] CommerceNet，http://www.commerce.net/

[2] William Stallings, Cryptography and Network Security--Principles and Practices 2rd, 1998.

[3] 內政部，「憑證管理中心」，http://moica.nat.gov.tw/html/

[4] 中文 PHP 資訊站，http://www.unixphp.com/

[5] 中華電信數據分公司，http://www.hinet.net/