分散式智慧財產權管理系統之電子檔案儲存機制

黃明祥[1]、李正吉[2]、孫耀國[1]、關華蓉[1]、江岡旻[1]、黎凡煒[1]、陳志維[1]

朝陽科技大學資管系[1]
台中縣霧峰鄉吉峰東路 168 號
Email: mshwang@cyut.edu.tw

交通大學資科所[2]
新竹市大學路 1001 號

摘要

目前政府正積極地進行電子檔案管理的籌設工作，以有效地管理並儲存各類型的檔案資料，並提供使用者快速便捷的線上調閱服務，讓使用者清楚的瞭解政府的施政措施。由於在電子化的環境中，因檔案資料以數位的方式儲存，使得檔案容易被複製、偽造甚至竄改。此外本文亦將著重於電子檔案儲存安全認證機制，內容將包含電子檔案的加解密、數位簽章機制、浮水印技術，並透過加密技術來確保機密檔案的私密性。

關鍵詞：電子檔案、電子公文、加解密、數位簽章、浮水印

壹、前言

早期，檔案資料均以紙張之方式儲存，不僅使用者調閱不便，頻繁的調閱頻率亦造成紙張的損壞，使得檔案紀錄的不易保存。現今，電腦科技技術之發達，文件掃描及光碟技術的成熟，以電子化方式儲存的檔案資料，經過適當的整合管理，不但經濟、環保也更有利於提供線上調閱服務，世界上許多先進國家已採用電子設備處理檔案，並以數位化的方式儲存。

為因應此一趨勢，目前政府正積極地進行電子檔案管理的籌設工作，以有效地管理並儲存各類型的檔案資料，並提供使用者快速便捷的線上調閱服務，讓使用者得以清楚的瞭解政府的施政措施。但仍有二個問題存在，第一個，雖然政府欲成立檔案管理局來有效管理並儲存各類的檔案資料，但這些檔案僅限於各地方機關認為須典藏的檔案，因此若民眾想查詢非典藏的檔案，就必須至發文機關的網頁中查詢，這對民眾十分不便。另外，資訊系統的安全問題也是我們所不能忽視的問題，在電子化的環境中，檔案資料以數位的方式儲存，使得檔案的複製、偽造及竄改變的極為容易，非法者可以輕易的偽造、竄改檔案之內容，其影響將更為深遠，因此如何防止機密資料的外洩，以及確保檔案資料的完整性，已是目前刻不容緩的議題。

基於以上所述，本篇論文將朝此方向來進行研究，期望利用電子檔案的特性，為檔案局的檔案管理作業，開發出一套安全又實用之系統，以及利用一個有效且安全的分散式電子檔案作業架構，提供相關應用服務給使用者來查詢使用。此外，為了達到分散式電子檔案交換之安全機制，我們也期盼透過一些分散式、密碼學及資訊安全技術之運用，來提出一個可行的方案，能夠應用到全國檔案資訊系統，推動本國電子化政府的目標。因此，使用者或各機關便可以透過網際網路交換電子檔案，以達到政府單一窗口的政策，不僅可以提高政府行政效率，又可以便利使用者。

本論文著重的目標在於電子檔案安全性的維護上，故舉凡檔案透過網路傳輸所可能遭遇的安全威脅，乃至檔案如何有效的保存並管理，都將是我們所需要克服及考量的問題。因此本系統必須利用數位簽章技術，來確保檔案資料的完整性及來源性，並利用加解密技術，來達到私密性的要求，以防止機密資料的外洩。如此一來便可大量提升網路傳輸與檔案儲存

安全的部份。所以在安全性維護上，就必須達成下列這幾點的要求：

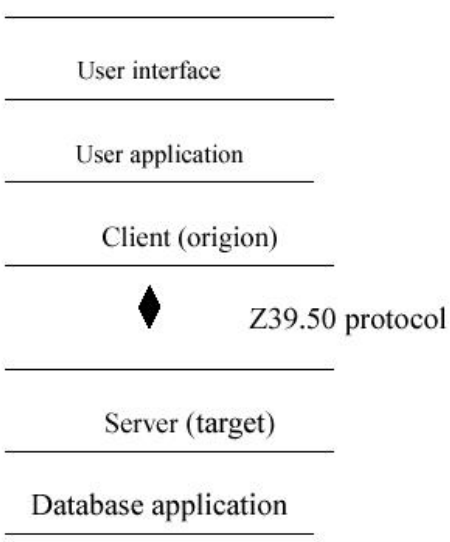
- 私密性：非合法授權者無法讀取機密的檔案資料；
- 可驗證性：使用者可確定檔案來源的合法性；
- 完整性：使用者可確保檔案沒有被有意或無意的竄改。

貳、分散式資料處理之方式

目前各地方機關的公文，皆自行發佈並且保存，民眾在查詢資料時可能需要到各個地方政府之網站做查詢，才能夠滿足需求，十分不便。所以，提供一個分散式電子公文整合檢索的環境，是非常必要，也是電子化政府必須的責任。

目前有五種分散式檢索相關標準可幫助分散式電子資源的組織與查詢，包括：Z39.50 標準、ZLite、史丹佛網際網路檢索與查詢協定 STARTS（Standard Protocol for Internet Retrieval and Search）、DAP/LDAP（X.500 Directory Access Protocol）及 CORBA（OMG's Common Object Request Broker Architecture）等。而其中 Z39.50 標準，目前正被廣泛的應用在國內圖書館自動化的建設，底下我們將簡略介紹此標準之相關作業。

Z39.50 是以主從模式（Client/Server Model）為架構。它定義伺服器（server）與使用者端（client）兩者間資料的傳輸方式，如下圖一。



圖一、Z39.50 系統示意圖

●Z39.50 提供的服務協定

使用者以 Z39.50 協定作資料檢索時，事實上是由客戶端之電腦經由網路發出各項符合 Z39.50 協定的服務請求，由伺服器端電腦依照此標準一一回應。其規範的服務項目在第三版中有下列十一項：

一、啟始（Initialization）：定義客戶端連上伺服器，及伺服器回應的訊息與過程。

二、存取控制（Access Control）：連上伺服器時，對客戶端所做的身份、密碼確認。

三、解釋（Explain）：客戶端可發出請求，請伺服器解釋其可供利用之資料庫及相關訊息，如資料庫名稱與使用說明、支援的資料格式與屬性及關於資料庫的 metadata。

四、瀏覽/掃瞄（Browse/Scan）：客戶端可請求伺服器列出可供檢索的詞彙，如人名、題名等，據以瞭解資料庫中的索引詞彙或控制詞彙。

五、查詢（Search）：使用者的查詢條件，經客戶端軟體處理包裝後提出查詢，伺服器回應查詢摘要（所得筆數）與部份結果，並保留此結果供後續的請求利用。使用者可就某一查詢結果予以命名，便於和後續的查詢作交集或聯集的運用。

六、會計/資源控制（Accounting/Resource Control）：客戶端中斷伺服器的處理、或要求回應檢索計費狀況等服務，讓使用者在計費的檢索服務系統內，瞭解其資源使用狀況。

七、排序（Sort）：客戶端可請求伺服器就某欄位（如題名、年代）或某條件將查詢結果排序，以便於檢視。

八、擷取（Retrieve）：此部份包含展現（present）與分段（segment）服務。客戶端可就某些記錄以特定範圍、欄位或格式請求展現資料，當回應的資料非常大時（如圖形檔案），可請求以分段方式傳回。

九、延伸服務(Extended Services)：使用者可由此項目，利用沒有正式規範在 Z39.50 協定內的其他服務，如館際互借、定期查詢、資料庫更新等功能。

十、結果集刪除（Result-Set Delete）：用以刪除伺服器儲存的查詢結果，降低伺服器的負擔。

十一、結束（Termination）：兩端電腦結束查詢會期，斷線離開的服務。

由於檢索 Z39.50 Server 的資料，必須使用到 Z39.50 Client 軟體，然而 Z39.50 Client 軟體並沒有像 WWW 的瀏覽器那樣普及，因此，其 Client 軟體可以採用與 CGI 或其他的方式結合設計，以求與 WWW 整合，提供使用者以 WWW 界面進行檢索及顯示，此 Client 須能將 HTML 格式之檢索需求，轉換為 Z39.50 標準與 Server 溝通，並將 Server 傳送之結果，轉換為 HTML 格式給 WWW Server，供使用者瀏覽。

其作業方式說明如下：

1. 將讀者在 WWW 所輸入查詢條件，透過 CGI 程式傳送至「Z39.50 Client 軟體」。
2. 「Z39.50 Client 軟體」將所接收到之 HTML 格式之查詢條件，轉換成 Z39.50 檢索指令，傳送至「Z39.50 Server」，開始檢索分散式電子資料。
3. 「Z39.50 Server」將檢索到之結果傳送至「Z39.50 Client 軟體」。
4. 「Z39.50 Client 軟體」再依讀者之顯示需求，透過 CGI 轉為 HTML 格式於 WWW 上顯示。

各地方政府可以不用自行開發檢索功能，只要其資料庫採用 Z39.50 標準，由檔案管理中心來維護檢索系統，那麼，一般民眾即可將檔案管理中心當作統一的服務窗口，透過檔案管理中心即可查詢各地方政府的電子

化資料，例如施政措施、公告事項以及往來公文等等，除了可以提供民眾快速便捷的線上調閱服務，更可以減輕檢索系統的維護成本。

叁、憑證管理中心之建置規劃

為確保電子檔案儲存的機密性(Confidentiality)、可鑑別性(Authentication)、完整性(Integrity)及不可否認性(Non-repudiation)，建立一可信賴的電子憑證管理機制是推動電子檔案儲存安全認證機制中非常重要的一環。此認證機制的主要設置目的，在提供電子化檔案儲存時所需的公開金匙安全機制及數位浮水印安全認證機制，透過一公正的憑證管理中心(Certification Authority, CA)來扮演具有公信力的認證中心，對個人及機關團體進行憑證的簽發及管理作業，以利各種相關安全認證技術的推動。

我們對於公開金匙的憑證管理機制，我們建議採行政府所提供的政府憑證管理中心(GCA)，而不自行建立憑證管理中心，主要基於以下四個原因：

(1) GCA 轉置成本較低：由於 GCA 提供使用者免費申請，且目前政府單位均採用此一機制來做公開金匙的簽發及認證工作，並有許多政府機關與民眾的相關應用已開始實施。未來國家檔案局正式成立後，若使用 GCA，則使用者可立即使用原來向 GCA 所申請的憑證，就可進行相關的業務服務，而不需另外申請電子憑證。

(2) 相容性高：政府憑證管理中心所採用的系統機制均符合國際標準，因此其相容性高，更有利於國際間之電子檔案的儲存。

(3) 完善的憑證管理：憑證的簽發、展期、註銷及稽核等措施均已設置完善，政府機關及個人透過網路便可便利地進行各項服務。

(4) 減少建置成本：若採用 GCA，則可省去大量的建置費用及日後維護系統所需的人力及經費。

此外，我們將使用數位浮水印的技術，用一把機密金匙藏入浮水印，來保護電子檔案的著作權，在數位浮水印的認證機制方面，我們規劃認證中心所採行的措施如下：

(1) 著作的機關或個人將著作的電子檔案及所要藏入的浮水印送交認證中心審核。

(2) 認證中心查詢是否有相同或類似的電子檔案，若無則簽發數位浮水印憑證。數位浮水印憑證包含下列資訊：
   a. 持有者的認證資訊：如姓名、地址等。
   b. 原始的電子檔案：如著作的影像文件(已藏入浮水印)。
   c. 欲藏入的數位浮水印。
   d. 簽發單位的數位簽章。
   e. 簽發單位的名稱 。
   f. 數位憑證的有效期限。
   g. 數位憑證的序號。

   此憑證的格式亦採用 ITU-T(CCITT)所定義的 X.509 國際標準格式，使其具有較高的相容性。

(3) 要證明自己擁有某一電子檔案的著作權時，便利用自己所持有的機密金匙取出所藏入的浮水印，再與數位浮水印憑證中的原圖與浮水印作一比對，來進行判別。

利用以上的機制我們可以成功的讓擁有者證明其為合法的所有者，並使電子安全檔案儲存機制更加完善。

肆、電子公文交換安全認證之機制

電子公文交換的安全機制是在解決兩個機關之間，如何安全的傳送電子公文到另一個機關，以達到電子公文的來源鑑別、機密性、存取控制及完整性等需求。為此，我們可以利用

一些資訊安全技術及密碼學的原理來達成目標。

首先，雙方都必須由一個公認的認證中心(Certificate Authority，CA)註冊申請得到一對公開、私密金鑰，公開金鑰必須公佈在公開的目錄下，供所有使用者取用，而私密金鑰則自己保存。當發文端及收文端要安全地傳送電子公文時，他們必須先到 CA 取得對方的憑證，並取出對方的公開金鑰，然後依據事先協議出的密碼系統(RSA)，再利用圖二的流程，即可製作出密文及簽章。當要驗證電子公文的完整性及來源鑑別時，利用圖三的流程，即可互相認證對方所傳送的電子公文。

底下我們將分別針對發文端及收文端的處理程序作說明。

(一)發文端的處理程序

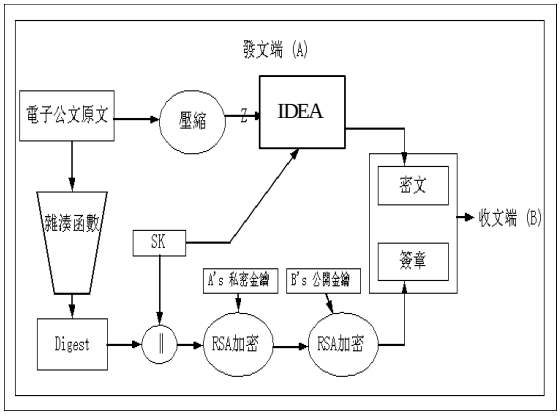
(1) 首先，發文者會先對電子公文原文作壓縮，壓縮後的原文稱為 Z，先作壓縮的原因是可以減少加密的長度，增快加解密的速度。

(2) 亂數產生一個交談金鑰(Session Key, SK)，此交談金鑰每次都不一樣，作為每次加解密電子公文之用。利用對稱型密碼系統(如 IDEA)，用 SK 把 Z 加密成密文。

(3) 把電子公文利用雜湊函數(如MD-5或SHA-1)作成訊息摘要(Digest)，接著利用非對稱型密碼系統(如 RSA)，把 Digest 與 SK 用自己的私密金鑰加密後，再用收文者的公開金鑰加密成簽章。

(4) 最後，把密文及簽章傳遞給收文者。

整個處理過程如圖二所示。



圖二、發文端的安全架構

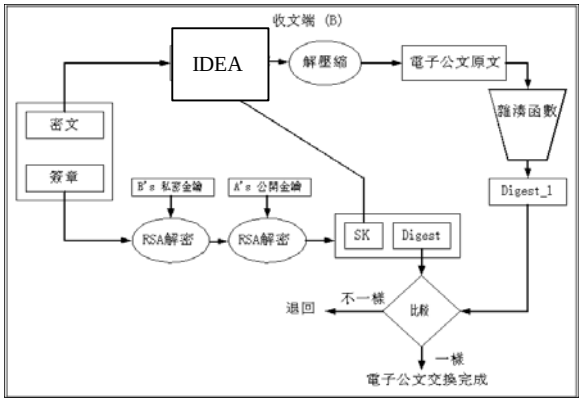
(二)收文端的處理程序

(1) 當收文者收到密文及簽章時，利用非對稱型密碼系統如 RSA，把簽章用自己的私密金鑰解密後，再用發文者的公開金鑰解密成 Digest 與 SK。

(2) 利用對稱型密碼系統如 IDEA，用 SK 把密文解密成 Z，再透過解壓縮的動作，即可還原成電子公文原文。

(3) 把此電子公文原文利用雜湊函數作成訊息摘要(Digest_1)，接著，比對 Digest 與 Digest_1 是否一樣，如果比對結果是正確的，則可以確定電子公文安全交換完成。

整個處理過程如圖三所示。



圖三、收文端的安全架構

由圖二及圖三可以看出，這樣的安全架構可以達到前面所提之電子公文機密性、存取控制、來源鑑別及完整性。在機密性方面，雙方先用非對稱型的密碼系統取得共有的交談金鑰(Session Key)，再透過此交談金鑰使用對稱型密碼系統加解密，即可達到電子公文的機密性，使用對稱型密碼系統作秘密通訊的好處是：它的加解密速度遠快於非對稱型的密碼系統。在存取控制方面，只有合法的收文端才能取得電子公文原文，它的作法是使用收文端的公開金鑰加密交談金鑰給收文端，只有合法擁有私密金鑰的收文端，才能取得此交談金鑰，進而解密出電子公文原文，利用此交談金鑰，除了可以達到機密性外，又可以達到存取控制。

在來源鑑別及完整性方面，使用電子數位簽章的技術，發文端首先會對電子公文作一訊息摘要，再對此訊息摘要作一數位簽章，然後將電子公文及此簽章送給收文端，收文端收到此訊息後，即可用相同方法，先對電子公文作一訊息摘要，再使用發文端的公開金鑰驗證簽章，即可確認此電子公文是由發文端所送出，並確保此公文的完整性。

伍、結論

本研究目前已經完成三個子系統，分別為檔案管理系統、檔案傳輸系統、民眾瀏覽系統。在 Server 端系統中的檔案安全驗證、檔案儲存、事件檔記錄、檔案的傳輸及資料庫的管理等功能都已經完成，另外還有模擬計費功能。Client 端系統則完成了檔案輸傳和數位簽章保護、資料庫管理、權限管理、事件檔記錄，在要傳送機密檔案時也有身份認證的功能。最後完成民眾瀏覽系統，可供使用者線上查詢檔案並下載，身份認證、付費功能等基本功能。

目前完成的系統可以達到檔案在網路傳輸時的安全性，當檔案要傳輸時會經過壓縮和加密，可以讓檔案變小並擁有其機密性，並加上數位簽章達到檔案的來源性和完整性；以足夠確保檔案在網路傳送中的機密性。至於未來需改善的部分為需要在計費方面，考慮一些新的方法，另外需注意 Server 端和 Client 端之間的網路穩定性，否則將會使整個傳輸過程出現問題，這些都是我們未來需要多加注意和改善的地方。

陸、參考文獻

[1] 張真誠，“電腦密碼學與資訊安全”，松崗，1989。

[2] 黃明祥、陳伯岳、林詠章、李正吉，“電子檔案儲存安全之認證研究期末報告”，朝陽科技大學資訊管理系，2001。

[3] 政府憑證管理中心，http://www.pki.gov.tw。

[4] 政府憑證管理中心，“政府憑證管理中心用戶使用說明”，1998。

[5] 政府憑證管理中心，“政府憑證管理中心憑證實做準則”，1998。

[6] 賴國華、江義淵、余丁榮、陳羿逞，“電子文件檔案管理與應用之研究”，元智大學資訊工程研究所，2001。

[7] 趙元甫，“資訊隱藏技術之研究”，國立中央大學資訊管理研究所，碩士論文，1999。

[8] 阮孝緒，“公開金鑰架構系統安全管理認證之設計與研究”，國立成功大學資訊工程研究所，碩士論文，2001。

[9] 高孟甫，“公開金鑰架構中金鑰與憑證相關安全認證之設計與研究”，國立成功大學資訊工程研究所，碩士論文，2001。

[10] 曾元顯，"架構一個 WWW 上的 Z39.50 伺服器"，中國圖書館學會會訊 104 期

[11]公共圖書館資訊網路，"地方文獻數位化之模式與相關標準研究報告"
[12]賴忠勤，"談在全球資訊網（WWW）以Z39.50協定檢索書目資料庫系統之規劃"，書苑季刊34期
[13]曾元顯，"架構在 WWW 與 Z39.50 上的近似自然語言OPAC檢索系統"
[14]Syed, F., “Children of DES：A Look at the Advanced Encryption Standard, ” Network Security, Volume：2000, Issue：9, 2000, pp. 11-12.
[15]Meyer, C., “Fundamental DES Design Concepts,” Computers & Security, Volume：15, Issue：5, 1996, pp. 406.
[16]Chang, C.C., Hwang, S.J., “A simple approach for generating RSA keys,” Information Processing Letters, Volume：63, Issue：1, 1997, pp. 19-21.