行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※

※　　　　　　　　　　　　　　　　　　　　　　　※

※　　　　　　電子化公文管理系統　　　　　　　　※

※　　　　　　　　　　　　　　　　　　　　　　　※

※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：■個別型計畫　　□整合型計畫

計畫編號：NSC 90-2213-E-009-080

執行期間：90 年 08 月 01 日 至 91 年 07 月 31 日

計畫主持人：葉義雄教授　　　　　國立交通大學資訊工程學系

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學資訊工程學系

中　華　民　國 91 年 08 月 02 日

行政院國家科學委員會專題研究計畫成果報告

計畫編號：NSC 90-2213-E-009-080
執行期限：90 年 08 月 01 日 至 91 年 07 月 31 日
主持人：葉義雄
計畫參與人員：林俊宇、李練君
執行機構及單位名稱：國立交通大學資訊工程學系

一、中文摘要

隨著資訊科技與網路科技的進步，政府所規劃的電子化政府政策，是針對組整層級的再造、組織人事的精簡與決策層級的縮短而制訂，如此不僅可以加快政府決策制訂的速度帶領國家向上提升的速度，更可讓電子化的過程讓國家邁向依法制化的自由國家體制。然而電子化政府必須具備的電子化公文系統，將決策與政策傳遞電子化，在藉由 NII 所搭建的網路基礎建設，構建政府內部的數位神經系統，期使各部會機關所扮演的功能透過政府內部所構建之數位神經系統的連結達到統合的效果，而各機關所接受到的整體大環境改變的刺激快速回應到中央決策機制，如此未來政府所構建的電子化政府可隨著環境而衍生進化。

本計畫所規劃的電子化公文系統，將根據密碼學的理論基礎、網路安全機制與資料庫管理系統，來建立一適合電子化政府使用的電子化公文管理系統，如此才藉由將公文的電子化管理，進而達到電子化政府所欲達成的快速決策機制與組織再造的目的。

關鍵詞：電子化公文，網路身份憑證，安全存取機制，X.509

Abstract

With the rapid growing of information and network techniques the government deals with all the documentation should be changed from papers to electronic-line. This can efficiently short time to finish the documentation and the transaction. Also it can promote all the decisions. To reform as e-government it is necessary to have e-document system. All decision and policy-make should through electronic by NII network infrastructure. It must construct the government's digital neuro system. It can integrate all the divisions through this system.

This project will plan an e-document system based on cryptographic theory, network security mechanism, and database management system to construct an e-document system for government use. This will reach our goal to have the fast decision make and simplified the organization.

Keywords：e-Document, Authentication, Network Security Mechanism, X.509

二、緣由與目的

自從 HTML 語言與 HTTP 通訊協定的誕生，網際網路(Internet)的使用人數與資源以指數級數呈爆炸性成長，網際網路所帶來的便利性使得知識與資訊得以迅速傳遞，這改變了二十一世紀人類生活與教育的模式，傳統文件的傳遞方式與處理模式都相繼的以電子化的方式來處理，以使得文件可以藉由網際網路得以傳遞。

以電子化方式處理文件時，必須考慮到以下幾點：

1. **確認性**(authentication)—驗證通訊者的身份。在傳統的公文處理模式是以橡皮圖章來確認公文已經過相關人士的處理，並藉由對圖章的確認達到身份的驗證，然而在 Internet 上，我們更需要具備相關的身份確認功能，以避免可能的身份冒用、誤用，而根據 X.509 v3 標準所設計的網路身份證是目前被廣為採用來達到身份確認要求的機制。
2. **存取控制**（access control）—根據使用者的身份來管理存取的權限。根據所確認的使用者身份與使用者權限來管理存取文件或相關資源的權力，以便控制文件或相關資源的存取政策。
3. **完整性**（integrity）—確保資料未被竄

改或傳遞時未發生錯誤。
檢查資料是否被人竄改或在傳遞的過程中是否有錯誤，以保證資料的完整性。文件的可能因為傳遞過程中硬體的錯誤而產生文件被破壞或因為人為因素的介入竄改文件，因此為了確保文件的完整性，MAC（message authentication code）是一個常常被用來驗證與保護資料的完整性。

4. **機密性（confidentiality）**—確保資料得以機密的、安全的保存或傳遞。

在 Internet 上傳送的資料時，TCP/IP 通訊協定是採用 IP v4 通訊協定來協助通訊雙方進行通訊，然而在 IP v4 所設計的協定，並未考慮到資訊安全的問題，所以資料是以明文的方式傳遞，因此 Internet 上傳遞文件，就猶如以明信片傳遞訊息一樣，所傳遞的內容是公開的、未加以保護的，所以確保資料的機密性是相當重要的。通常可採用對稱型加密系統與非對稱型加密系統搭配來保護資料的機密性。公文的電子化，所牽扯的問題包括上述四點問題外，文件傳遞所採用的通訊協定以及文件歸檔所涉及的管理問題，都是電子化公文所必須考量的問題，另外傳統公文的處理流程與公文分類、各類公文的效力、公文的機密等級以及公文保密的時限都是本計畫所必須涉及與考量的課題，唯有適當與適合的設計才可能建構一妥當與人性化的電子化公文系統，以達成政府實現電子化政府的目標。

經由本計畫落實政府所提倡的電子化政府的理念，以利提升政府效能進而增加國家的競爭力與產業發展的潛力，本計畫將針對公文的電子化需求做相關研究與設計，以期能建立一電子化公文系統，以便達成政府實現電子化政府的目標。本計畫的實施過程可為國家培養資訊安全的人才，以便能有足夠的人力加強本國網路安全與資訊安全防護的能力。藉由本計畫的執行，能讓本實驗室的研究生能落實平日所研究的密碼學理論於電子化公文系統中，加強與達成文件傳遞時的保密性、完整性、身份確認性與存取控制。並藉由搭配政府所建立的 GCA（government certificate authority）的網路身份憑證，使本系統所建立的安全控制機制可以以最小的成本來達成，並使本計畫所建立的建立的電子公文系統可以確實的應用於電子化政府政策中。

本計畫將針對 Microsoft Office 系統做改良，並結合數位簽章、檔案加密、數位信封與身份確認等技術，以節省並配合政府相關機關的現行運作環境，如此可節省系統導入所需的教育成本與適應時間。

三、結果與討論

本計畫利用密碼學系統中的三大領域，對稱型加密系統、非對稱型加密系與雜湊函數，達成公文在網際網路上傳遞的安全要求，其方法說明如下：

1. **對稱型加密系統：**
   對稱型加密系統，速度快可以用來將公文加密，以便保護公文傳遞與保存時的機密性，本計畫所規劃的電子公文系統，會結合對稱型加密系統與非對稱型加密系統以電子信封的方式保護公文傳遞的安全性，另外會設計相關金鑰管理的方式來加強公文保存的機密性。
2. **非對稱型加密系統：**
   非對稱性加密系統用於 X.509 v3 網路身份憑證的驗證與製作電子信封。以達成本計畫對身份確認的需求與資訊傳遞的機密性。另外可以實現數位簽章以取代傳統印章的功能。
3. **雜湊函數：**
   雜湊函數可用於產生 MAC 以保護及驗證資料的完整性，當然所產生的 MAC 可以配合非對稱型加密系統以產生數位簽章以達到不可否認性。
4. **X.509 網路身份憑證：**
   本計畫將採用被廣泛使用的網路身份憑證的規格 X.509 v3 來當作電子公文確認身份的機制，如此才可以確認收、發雙方的身份。
5. **搭配政府所建立的 GCA：**
   本計畫是為了電子化政府之電子化公文

系統而設計，為了解決身份確認的問題將採行 X.509 v3 的網路身份憑證規格，政府已建立 GCA 來發行網路身份憑證，因此本計畫將搭配 GCA 來完成身份驗證的機制。

6. 金鑰管理：

本計畫會牽涉到電子公文保存的安全控制問題，我們將以對稱型加密系統來保密歸檔的公文於系統中，而金鑰部分將根據相關策略以不同的方式來保管，以達到公文保密的需求。

四、計劃成果自評

電子化政府是邁向二十一世紀政府再造與政府轉型的做主要課題，本計畫所規劃的電子公文系統，不僅可以達成培養國家對於資訊安全人才的需求，亦可讓學術研究能貼近日常生活的應用，其完成之功能說明如下：

1. 結合 Microsoft Office 辦公室文書處理系統，以建立一具備數位簽章、密碼技術、網路安全與存取控制的電子化公文處理系統。
2. 根據網路身份憑證所具備的身份確認特性，並根據本電子化公文系統所建立的組織結構圖與公文存取策略，來控管公文的調閱與批閱的權限，並根據這些管理與安全控管機制，將文件利用資料庫系統管理。
3. 透過 ODBC（Object Data Base Connection）存取相關的資料庫管理系統，以便實現本系統所設計的安全機制與管理機制。
4. 以 SSL proxy 的方式，建裡 Intranet 的安全傳遞機制。
5. 建立的電子化公文系統可以加速政府所正在推動的電子化政府之政策，本系統可以透過電子化的方式輔以資訊科技，以達到增加每一位管理者的管理跨幅（management span），以達到扁平化組織的目的，如此不僅可以藉由縮短管理的層級以加快政府決策的速度，更可以藉由資訊截取的科技的加快管理者決策時資料彙整與蒐集的速度。

7. 發表論文

國外期刊

[1] Yi-Shiung Yeh, C. H. Lin, and Wei-Shen Lai: “Construct Message Authentication Code with SHA and AEA,” Journal of Discrete Mathematical Sciences & Cryptography (EI, Accepted)

[2] Chu-Hsin Lin, Yi-Shiung Yeh, Wei-Shen Lai, and Cheng-Long Lee: “A Software Anti-Paravy System Using Undeniable Signature and Smart cards,” JASS (Accepted, paper #: JASS-03-04-2002)

五、參考文獻

1. R.L. Rivest, A. Shamir, and L.M.Adleman,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystem," Communications of the ACM, v. 21, n. 1, Feb 1978, pp. 120-126.
2. R.L. Rivest, A. Shamir, and L.M. Adleman, "On Digital Signatures and Public-Key Cryptosystems," MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979.
3. N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, v. 48, n. 177, 1987, pp. 203-209.
4. V.S. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, 218(1986), Springer-Verlag, pp. 417-426.

5. ANSI X9.17 (Revised), American National Standard for Financial Institution Key Management (Wholesale)," American Bankers Association, 1985.
6. ISO DIS 8732, "Banking-Key Management (Wholesale)," Association for Payment Clearing Services, London, Dec 1987.
7. W. Tuchman, "Hellman Presents No Shortcut Solutions to DES," IEEE Spectrum, v. 16, n. 7, July 1979, pp. 40-41.
8. R.L. Rivest, "The RC4 Encryption Algorithm," RSA Data Security , Inc., Mar 1992.
9. http://www. nist. gov/aes
10. R.L. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, Apr 1992.
11. "Proposed Revision of Federal Information Processing Standard (FIPS) 180, Secure Hash Standard," Federal Register, v. 59, n. 131, 11 Jul 1994, pp. 35317-35318.
12. Research and Development in Advanced Communication Technologies in Europe, RIPE Integrity Primitives: Final Report of RACE Integrity Primitives Evaluation (R1040), RACE, June 1992.
13. M.J.B. Robshaw, "The Final Report of RACE 1040: A Technical Summary," Technical Report TR-9001, Version 1.0, RSA Laboratories, Jul 1993.
14. J. Postel and J.Reynolds: Telnet Protocol specification, RFC 854, May 1983.
15. J. Postel and J.Reynolds: Telnet option specifications, RFC 855, May 1983.
16. Alan O. Freier, Philip Karlton, and Paul C. Kocher: The SSL Protocol, Netscape Communication Corp, ver 3.0, Mar. 1996.
17. T. Dierks, C. Allen: The TLS Protocol Version 1.0, RFC 2246, Jan 1999.
18. B. Schneier: Applied Cryptography, 2nd Ed. John Wiley & Sons, 1996.
19. T. ElGamal, "A PublieKey Cryptosystem and a Signature Scheme Based on Discrete Logarithms," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 10-18.
20. X. Lai and J. Massey, "A Proposal for a New Block Encryption Standard," Advances in Cryptology - EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 389-404.
21. R.L. Rivest, "The MD4 Message Digest Algorithm," Advances in Cryptology - CRYPTO '90: Proceedings, Springer-Verlag, 1991, pp. 303-311.
22. R. Srinivansan, Sun Microsystems, RFC-1832: XDR External Data Representation Standard, August 1995.
23. Y.S. Yeh, C.C. Wang, "Construct Message Authentication Code with One-Way Hash Functions and Block Ciphers", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, v. E82-A, No. 2, Feb. 1999, pp. 390-393.