行政院國家科學委員會專題研究計畫成果報告

Internet/Intranet 電子文件的來源識別：ITU-T Rec. X.509 公開金鑰電子証書的延伸與應用

Internet/Intranet Document Source Authentication: Extension and Application of the ITU-T X.509 Public-key Certificate

計畫編號：NSC 87-2416-H-009-015-N8
執行期限：86 年 8 月 1 日至 87 年 7 月 31 日
主持人：黃景彰 (JJHwang@cc.nctu.edu.tw)
計畫執行單位：交通大學資訊管理研究所

一、中文摘要

本研究提出了一個管理 EDI 文件授權控制的方法，此方法是基於 ITU-T 所制定的第三版 X.509 公開金鑰證書。除了證書擁有者的個人資訊及公開金鑰值之外，我們還在公開金鑰證書上加入了證書擁有者在企業組織內的職務指派資訊，以及該職務被授權可以處理的 EDI 文件等資訊。這樣的設計，使的公開金鑰證書在使用時，可以同時達到使用者身份識別以及授權控制的目的。

關鍵詞：電子資料交換、X.509 公開金鑰證書、寄方授權確認、電子職務證書

Abstract

We have proposed a method of authorization control for the management of EDI documents. The method is based on the version three of the X.509 public-key certificate defined by ITU-T. In addition to the information about a user and his public-key, we add into the certificate information about the role which this user plays in the organization, and we also add information about the documents which the role is authorized to process. As a result, the public-key certificate is used for both purposes of user authentication and authorization control.

Keywords: EDI, X.509 public-key certificate, Verification of Authorization-at-Source (VAS)

二、緣由與目的

本研究「Internet/Intranet 電子文件的來源識別：ITU-T Rec.X.509 公開金鑰電子証書的延伸與應用」是整合型計畫「網際網路電子資訊交換：產業標準之競爭、整合與應用」之子計畫。

傳統以紙張文件來交換訊息的方式，發文方可以在文件上簽章，以聲明該文件的來源，並作為憑證表示對內容的負責。而收文方也可以檢驗紙張文件的簽章，以確認文件來源的真實性，避免發生假冒他人身份的欺騙行為。

以電子資料的方式來交換文件，也應該要提供類似紙張環境的來源識別檢查(Origin Authentication Check)的機制，使得收文方可以確認電子文件的來源。

雖然數位簽章方法可以讓電子文件的收文方確認文件的來源，以及內容的完整性，但卻無法保障文件是經過發文方組織的合法授權人員核決其內容。

所以，如何在網際網路電子文件交換的環境中，設計一個文件內容授權的驗證機制，使得發文方及收文方都能確定電子文件在離開發文方時是經過合法的核決程序，這是一個重要的研究議題。如果能將電子文件的來源識別與內容核決程序的檢驗機制加以整合，就能達到更高的安全性，這也是本研究的目的。

三、本研究提出的方法

本文所提出的方法，是延伸 ITU-T Rec. X.509 標準，在公開金鑰證書的擴充欄位中加入了組織員工的職務資訊，使原本只具有來源識別功能的公開金鑰證書具有員工電子職務證(digital credential)的功能，也就是說，我們是利用公開金鑰證書來承載員工的職務指派授權資訊。

首先，組織的設計、管理者可以為每一種組織職務選定一個唯一的識別碼。然後在組織成員公開金鑰證書的 Directory Subject Attributes 擴充欄位中記錄該組織成員被指派的所有職務的識別碼。依照 X.509 標準的規範，Directory Subject Attributes 欄位的目的主要是用來記載擁有公開金鑰擁有者(subject)之屬性資訊，例如所隸屬的群體，或是存取控制的機密等級分類等。

接著，組織可以訂定一個公開金鑰證書核發政策，稱為 EDI 授權政策(EDI-authorization policy)，記錄於公開金鑰證書的證書核發政策(certificate policy)擴充欄位，藉以宣示該公開金鑰的用途是作為員工在核決與 EDI 文件所代表的交易時，簽章與加解密用。此外，關於這個 EDI 授權政策，我們還可以在此政策的 policy qualifier 附屬欄位中，記錄此公開金鑰適用的 EDI 表單種類，如下所示。

Policy Identifier	EDI_Authorization_Policy	
	Policy Qualifier	Purchase order

有了上述的設計，要達到 EDI 文件的寄方來源授權確認，我們的建議是由寄方企業的稽核人員(或是稽核程式)來擔任 EDI 文件交易內容核決程序的查驗工作。也就是說應該由寄方企業來完成 EDI 成件的寄方授權確認(Verification of Authorization at Source, VAS)的工作

寄方的稽核不僅可以知道 EDI 文件上數位簽章之金鑰的擁有者和他的公開金鑰的對應關係，還可以知道簽署者在組織中有資格扮演的職務之資訊。進一步從公開金鑰證書核發政策欄位中，還可以得知金鑰的所有者能簽署的 EDI 文件種類。若確定整個核決程序無誤，則稽核可以用公司的私密金鑰來簽署這一份 EDI 文件，表示這一份 EDI 文件所代表的交易已滿足生效的條件。其程序如圖一所示。

上述的設計延伸了 X.509 來源識別的功能說使得 EDI 成件之收方企業可以藉由檢驗 EDI 成件所附加寄方企業稽核的數位簽章說來確定該成件所代表的交易是否滿足生效所須的條件作

四、計畫成果自評

要使得企業內部利用網內網路和企業間使用網際網路來進行電子資料交換說換須解決安全上的顧慮說其中寄方企業授權確認是 EDI 安全需求中重要但卻較少被研究的主題作本研究所提出的方法可以提供電子資料交換的寄方組織確認寄出的文件都是經過合法授權的。我們的研究與原計畫申請書的提案內容相符，研究的成果也於「1998 網際網路應用論壇—產業標準之競爭、整合與應用」研討會中發表[11]，可作為學界討論相關議題時的參考，以及業界在構建其公開金鑰基礎設施時的參考。另有一篇英文著作[12]將在 ICS'98 發表，我們也準備了另一篇論文[13]，將投稿於國際期刊。

本研究的主要貢獻是延伸 ITU-T Rec. X.509 標準，在公開金鑰證書的擴充欄位中加入了組織員工的職務資訊，使原本只具有來源識別功能的公開金鑰證書具有類似員工電子職務證的功能。此外，在公開金鑰證書的核發政策欄位中加入適當的資訊，可以聲明此證書的用途可作為驗證 EDI 文件在寄方是由具適當職務資格的人員完成。

上述的研究成果適用於政府組織或事業單位對個人所發單據的授權驗證，也可以應用在企業間的 EDI，使寄方企業確認寄出的 EDI 文件，其所代表的交易已經過合法的內部授權程序，即該交易已滿足生效所須達成的條件。

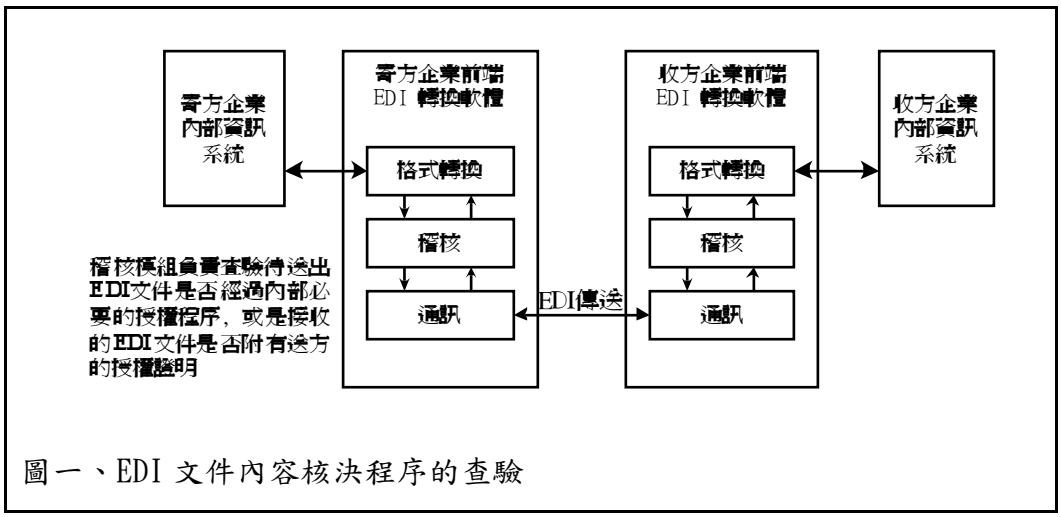
本研究的成果可以作為其他相關研究的基礎。例如，為達到 EDI 文件交換的安全要求而設計的控制機制，應該和企業內部資訊系統的安全控制做適當的整合。我們可以將本研究提出含職務資訊的公開金鑰證書之核發和企業內部授權管理相結合，並擴展此證書的使用至資訊資源的存取控制。我們也可以討論一個自動化工作流程業務處理的環境中，如何確保一筆 EDI 文件所代表的交易是經過合法的授權程序。這些都是和本研究相關且值得去研究的題目。

五、參考文獻

[1] Pauline Ratnasingham, Paul Swatman, "EDI security: a model of EDI risks and associated controls," *Information Management & Computer Security*, Vol.5, Iss.2, 1997, pp.63-71.

[2] Snehamay Banerjee, Damodar Y. Golhar, "Security issues in the EDI environment," *Information Management & Computer Security*, Vol.3 No.2, 1995, pp.27-33.

[3] Role-Based Access Control (RBAC): Features and Motivations, National Institute of Standards and Technology. Dec 1996. (http://walts.ncsl.nist.gov/rbac/newpaper/rbac.html)



圖一、EDI 文件內容核決程序的查驗

[4] Ravi S. Sandhu, Edward J. Coyne, Hal L.Feinstein Charles E. Youman, "Role-Based Access Control Models," *IEEE Computer*, Feb 1996, pp.38-47.

[5] *ITU-T Recommendation X.509|ISO/IEC 9594-8, Information Technology-Open Systems Interconnection-The Directory: Authentication Framework*, ITU-T SG/7|ISO/IEC JTC1/SC21/WG4.

[6] Selwyn Russell, "Paradigms For Verification of Authorization at Source of Electronic Documents In an Integrated Environment," *Proceedings of the 8th Annual Computer Security Applications Conference*, San Antonio, Texas, December 1992.

[7] Selwyn Russell, "Audit-by-receiver paradigms for verification of authorization at source of electronic documents," *Computers & Security*, 13, 1994, pp.59-67.

[8] Carol E. Brown, *Internal Control Concepts*, Jan 1995. (http://www.bus.orst.edu/faculty/brownc/lectures/controls/control1.htm)

[9] Christopher King, "Building a Corporate Public Key Infrastructure," *Computer Security Journal*, Vol. XIII, Number 2, 1997.

[10] Hitesh Tewari, Maurice McCourt, Donal O'Mahony, "Advanced Electronic Commerce Security in a Workflow Environment," Electronic Commerce Current Research Issues and Applications, Chapter 6, Springer, 1996.

[11] 黃景彰，吳國禎，1998，"Internet/Intranet 文件交換的來源識別：ITU-T Rec. X.509 的延伸與應用，" 網際網路應用論壇—產業標準之競爭、整合與應用，pp.44-52。

[12] Kou-Chen Wu, Jing-Jang Hwang, Duen-Ren Liu, "Extension of the X.509 Authentication Framework for the Access Authorization in Distributed Computing Environments," *Proceedings of the International Computer Symposium,* 1998. (to be published)

[13] Jing-Jang Hwang, Kou-Chen Wu, Duen-Ren Liu, "Access Control with Role Certificates: An Application of the ITU-T X.509 Standard," (working draft).