行政院國家科學委員會專題研究計畫成果報告

網際網路電子資料交換：傳輸與安全標準之整合與評估

EDI over Internet: Integration and Evaluation of Communications and Security Standards

計畫編號：NSC87-2416-H-009-016-N8
執行期間：86 年 8 月 1 日至 87 年 7 月 31 日
主持人：羅濟群 交通大學資訊管理研究所副教授

一、中文摘要

隨著電腦網路的高度發展，電子資料交換 (Electronic Data Interchange, EDI) 已成為企業及政府提高效率的新利器。當 EDI 架構在一個開放式網路上時，固然可以擴大資料交換的範圍，但同時也會面臨四面八方而來的威脅，確保 EDI 資訊在網路上的安全成為一個重要的研究課題。而本研究之目的在於探討 EDI 在網際網路上的安全架構。我們將探討目前 EDI 的發展以及目前網際網路傳輸的安全機制，加以比較與分析，評估其優缺點，從而提出一個適用於 EDI 的安全架構。

關鍵詞：電子資料交換、網際網路安全機制。

Abstract

As communications network been highly developed, the Electronic Data Exchange (EDI) has become essential to the success of the operation of governments and enterprises. When EDI transfers over an open network environment like Internet, it can make data exchange more repidly and conveniently, and improve the performance of the enterprise. However, the EDI system inevitably faces various threats such as data stealing or manipulation when the electronic information is transmitted via the open networks Consequently , the security of EDI should be seriously concerned.

This study will focus on applying EDI on internet and discussing its security mechanism . We will first introduce EDI standards and its security requirements , then discuss advantages and disadvantages of these protocols. After feasibility study, we will purpose suitable security mechanisms to meet different EDI system's requirements. Providing Internet Solution for EDI.

Keyword: Electronic Data Interchange, EDI, Internet Security Mechanism.

二、緣由與目的

隨著電腦網路的高度發展，電子資料交換 (Electronic Data Interchange, EDI) 已成為企業及政府提高效率的新利器。EDI 的定義為：貿易夥伴(Trading partner)利用電腦來傳送標準格式的業務資料。換句話說，EDI 提供了更快、更有效率的溝通管道，甚至成為一種新的企業經營方式。

電腦與電腦之間的資料可以直接透過雙方協議好的協定來傳送，也可以透過第三者來提供服務。而貿易夥伴則是指顧客、供應商或是其他業務上的相關組織，彼此之間需要透過文件與資訊的交換來進行工作。

使用者可以透過 EDI 系統和顧客、供應商溝通，傳送訂單、定價單、送貨通

知、或是付款資訊等等。此外，設計圖、電子資金轉帳、資料庫交易動作都可以利用 EDI 來達成。

由於 EDI 需要透給固定的格式標準來傳送資料，因此貿易夥伴都必須協調共同的 EDI 格式標準。隨著標準範圍大小的不同，EDI 可以是應用於組織之內，亦可以應用於組織與組織之間。當 EDI 的範圍越來越廣，參與的組織越來越多，一個通用的標準則必須提出，例如聯合國在 ECE/WP.4 下的 UN/EDIFACT 和北美的 ANSI X.12。

當貿易夥伴(Trading Partner)利用 EDI 良好整合之後，EDI 文件也可以直接由接收方的應用程式來確認與處理，因此 EDI 也可以是應用程式與應用程式之間的資料傳送，而不侷限於電腦與電腦之間的資料傳送。不限制格式的傳真文件與視訊資料，由於並不使用特定的格式，因此並不屬於 EDI 的範圍。

當 EDI 架構在一個開放式網路上時，固然可以擴大資料交換的範圍，提高產業整體的效能，但和其原來透過私有的 Value-Added Network 來傳送相較，四面八方而來的安全問題成為更大的隱憂。如何確保 EDI 資訊在網路上的安全，便成為一個重要的研究課題。

而本研究之目的在於探討 EDI 在網際網路上的安全架構。我們將探討目前 EDI 的格式標準、EDI 目前在產業界的應用、EDI 的分類、EDI 的安全層級、目前網際網路傳輸的安全機制，依據不同的應用，加以比較與分析，提出一個分類法，讓讀者可以根據此分類法，找出自己組織使用 EDI 的定位與安全需求，利用 Internet 現有提供的安全機制，達成各項安全需求。

三、結果與討論

（一）EDI 與網際網路安全機制之整合

我們將應用在不同產業方面的各種 EDI，針對他們的不同安全與效率等需求，將其分成三個等級的安全層級，根據安全需求由高至低分別為 EDI 安全層級最高的第一級、安全層級次高的第二級及安全層級最低的第三級。接下來我們將針對網際網路安全機制，為三個安全層級的 EDI，推薦不同的安全機制組合。

1. EDI 安全層級第一級之建議安全機制

在需要 CA 的情況下，我們建議採用 PEM 的 Encrypted mode，因為此模式提供對每個訊息使用不同的 DES 秘密金匙來對原來的訊息明文和 MIC 作加密，再將加密後的訊息、加密後的 MIC 和秘密金匙分別作傳輸編碼，然後經由郵件閘道器傳送。可達到訊息完整性、隱密性、訊息來源驗證、與不可否認性。PEM 的機制選擇如下：

Message Processing: MIC-ONLY
Digest Protection: DES-ECB mode
Key Management: DES-ECB mode
Message Encryption : none

在沒有 CA 的情況下，我們可以建議使用 PGP，並使用簽章和加密等步驟，PGP 的加密與簽章可以讓使用者加以選擇，使用簽章及加密後，可達到訊息完整性、隱密性、訊息來源驗證、與不可否認性。

2. EDI 安全層級第二級之建議安全機制

在需要 CA 的情況下，建議使用 PEM 的 MIC-ONLY Mode：先對訊息作傳輸編碼，再加上完整性檢查 (Integrity check)，產生 Message Integrity Code (MIC)，不作訊息加密。MIC 能確保訊息傳送過程中不會被郵件閘道器 (Mail gateway) 修改訊息內容。可達到訊息完整性、訊息來源驗證、與不可否認性。PEM 的機制選擇如下：

Message Processing: MIC-ENCRYPTED
Digest Protection: DES-ECB mode
Key Management: DES-ECB mode

Message Encryption: DES-CBC mode

在沒有 CA 的情況下，建議使用 PGP，使用簽章步驟，而不採用加密的步驟。

3. EDI 安全層級第三級之建議安全機制

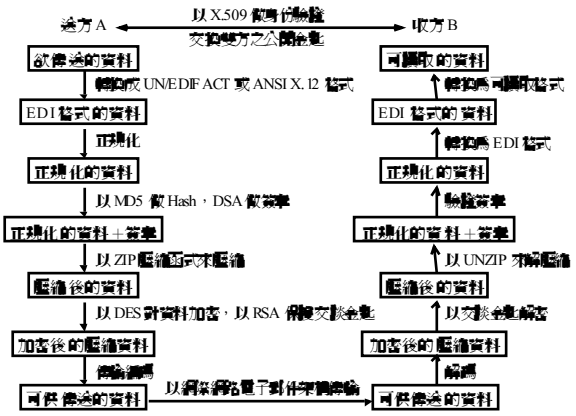
在需要 CA 的情況下，建議使用 PEM 的 MIC-CLEAR Mode ：只提供訊息完整性和訊息來源驗證，不提供訊息加密，訊息傳送時亦不作傳輸編碼 (Transmission encoding)，可達到訊息完整性。PEM 的機制選擇如下：

Message processing: MIC-ENCRYPTED
Digest Protection: DES-ECB mode, RSA
Key Management: DES-EDE mode, RSA
Message Encryption : DES-CBC mode

在沒有 CA 的情況下，建議使用 PGP，但不採加密與簽章步驟。

（二）網際網路電子資料交換之安全架構

綜合之前所分析的結果，我們可以提出一個兼具安全性與效率性的一般性 EDI 安全架構如圖一。相信此架構可以適用於國內的大部分 EDI 應用之需求。下面我們將詳細敘述在此架構下與 EDI 相關之問題。



圖一、EDI 安全架構圖

1. EDI 的傳輸架構

當 EDI 的參與者眾多，而遍及全球時，此時就需要一個有效的系統來組織及管理各個主體。電子郵件架構不只可用來連接各個 E-Mail 系統，達到 store-and-forward 訊息傳送之需求，同時其架構可用於 EDI 的傳輸環境中，因此 ISO/OSI 的 MHS 和目前 Internet 上廣泛使用的 PEM、PGP 或 MIME/MOSS 皆可用來傳輸 EDI 的訊息。

整個傳輸的架構如下：

正規化 → 簽章 → 壓縮 → 加密 → 傳輸編碼

2. EDI 的訊息格式

不論是用 MHS、E-Mail 或 FTP 及 WWW 來傳送 EDI 訊息，以及採用哪種加密方法如：PEM、PGP 或 MIME/MOSS 來加密 EDI 訊息，包含在訊息主體部分中的 EDI Interchange 可以是 UN/EDIFACT、ANSI X.12 或 UNTDI 等標準格式。這些格式均可支援各種加密、訊息驗證碼或數位簽章等安全機制。

3. EDI 的驗證

身份驗證採用以公開金匙為基礎的身份驗證協定，例如 X.509：每一位系統參與者皆需指定至少一個 CA 替他的金鑰做保證簽名，以產生其公鑰簽證 (Certificate)，而所指定的 CA 或多個 CA 應為該參與者所信任。

訊息來源驗證採用數位簽章做訊息來源驗證。

4. EDI 的數位簽章

在 EDI 的應用環境裡，我們考慮了數位簽章演算法的安全性、效率性與彈性，決定採用美國政府所定的數位簽章標準 DSA，作為訊息驗證時數位簽章的演算法。DSA 可以選擇不同的雜湊函數與不同的加密演算法，這裡我們建議 DSA 採用兼具安全性與效率性的 MD5 為其不可逆的雜湊函數。

4. EDI 的金匙管理

a. 秘密金匙：可透過金匙中心，以「階層式秘密金匙傳送法」來散佈金匙。
b. 公開金匙：則採納 ITU-T X.509 或 PEM 的樹狀階層來管理各參與主體。

c. 公開金匙的註冊、散佈及註銷：結合目錄服務來管理。此外，UN/EDIFACT 所制定的 AUKACK、CIPHER 及 KEYMAN 等訊息格式可用來支援金匙的散佈或交換。

四、成果自評

在本研究中我們首先介紹了 EDI 的規約標準、產業應用分類及其安全需求、探討在網際網路上 EDI 的傳輸方式：以電子郵件來傳輸及以檔案傳輸規約來傳輸、以及傳輸所需的相關安全機制如：PGP、PEM、MOSS、S/MIME 等等，並按照不同 EDI 安全層級的不同需求分析並建議了 EDI 安全架構所需的各項功能及實際使用的安全機制，包括資料格式、傳輸環境、驗證機制、數位簽章機制與金匙管理等，評估每一個項目的優缺點，並考慮其安全性、效率性、彈性、可行性，以及在 EDI 應用上的適用性。

針對各個功能，我們嘗試去找出最佳的解決方案，再由這些解決方案建構出一個理想的 EDI 安全架構，此架構不僅確保 EDI 之安全性，同時提升其效率。

一個良好的 EDI 安全架構提供了一個完整的環境來做電子資料交換，而這個環境中的每個組成部分都會影響到 EDI 的安全性和效率性，因此如何改進這些組成部分，諸如驗證機制、數位簽章機制、雜湊函數和金匙管理等機制，在理論上加強它們的安全性和效率性，並從而提升整個 EDI 的安全與效率，將是下一步必須要做的事情。

五、參考文獻

[1] Kaufman, Perlman, and Speciner, "Network Security: Private Communication in a Public World", Prentice Hall, 1995

[2] Andrew Fletcher, "EDI-Electronic Commerce, EDI and the Internet", Reed Business Information, England 1997

[3] Zimmermann, p., "PGP User's Guide, Vol.I Essential topics", 1994

[4] Zimmermann, p., "PGP User's Guide, Vol.II Special topics", 1994

[5] White, G.B. et al., "Computer Systems and Network Security" CRC Press, 1996

[6] Salomaa, A. "Public-key Cryptography, 2nd ed.", Springer-Verlag, 1996

[7] Pfleeger, C. P., "Security in Computing, Second Edition", Prentice-Hall, 1997

[8] Phyllis K. Sokol, "From EDI to Electronic Commerce", McGraw-Hill, 1995

[9] Hagan K.C. Pfeiffer, "The Diffusion of Electronic Data interchange", Springer-Verlag, 1992

[10] Nabil R. Adam, Yelena tesha, "Electronic Commerce" Springer, 1995

[11] Martin parfett, "What is EDI?", NCC Blackwell, 1992

[12] Paul Kimberley, "Electronic Data interchange", McGRAW-HILL, 1991

[13] Valerie Leyland, "Electronic Data Interchange", Prentice-Hall, 1993

[14] Richard H. Baker, "EDI: What Managers Need to Know about the Revolution in business Communications", TAB BOOKS, 1991

[15] J. Linn, "Privacy Enhancement for Internet Electronic Mail, Part I: Message Encryption and Authentication Procedures, RFC 1421", IAB 1993

[16] [26] S. Kent, "Privacy Enhancement for Internet Electronic Mail, Part II: Certificate -Based Key Management, RFC 1422", IAB 1993

[17] D. Balenson, "Privacy Enhancement for Internet Electronic Mail, Part III: Algorithms, Modes, and Identifiers, RFC 1423", IAB 1993

[18] B. Kaliski, "Privacy Enhancement for Internet Electronic Mail, Part IV: Key Certification and Related Services, RFC 1424", IAB 1993

[19] D. Atkins, W. Stallings, P. Zimmermann, "PGP Message Exchange Formats", RFC 1996, 08/16/1996.

[20] "The Secure HyperText Transfer Protocol", 03/25/1997,<draft-ietf-wts-shttp-04.txt>

[21] Jing-Sha He ,"Security in Gobal Internet Roaming", Information Security Conference, 1997

[22] 樊國楨, "電子商務高階安全防護：公開金鑰密碼資訊系統安全原理" 資訊與電腦, 1997

[23] 樊國楨, "公開金鑰基磐與電子公文交換作業安全簡析", 資訊視訊技術與應用研討暨展示會, 1997

[24] 樊國楨等, "電子商務安全簡介",電腦與通訊 55,民 85,12

[25] 李昌雄, "商業自動化與電子商務導論", 松崗, 民 86