行政院國家科學委員會專題研究計畫成果報告

在網際網路上應用 MIME 整合 EDI 與電子郵件安全機制之可行性分析與系統實做 — 以金融 EDI 為例

Using MIME to Integrate EDI and Security Mechanisms of the Internet Electronic Mail – Feasibility Study and System Implementation with Case of Finanical EDI

計畫編號：88-2416-H-009-019-
執行期間：87 年 8 月 1 日至 88 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 架構在一個開放式的網路上，如 Internet，可以使得資料交換更為快速便捷，從而提昇產業整體的效能。但是架構在一個開放式網路上之 EDI 會面臨四面八方的威脅，譬如資料的竊取、竄改等。如何在 Internet 上確保 EDI 資訊的安全，是一個很重要的研究課題。本研究探討在網際網路上以電子郵件來傳遞 EDI 資料的方式，應用多用途網際網路信件延伸（Multipurpose Internet Mail Extensions, MIME）整合 EDI 與電子郵件安全機制，使 EDI 資料能在網際網路上安全的被傳遞。

關鍵詞：電子資料交換、電子郵件安全機制、多用途網際網路信件延伸

Abstract

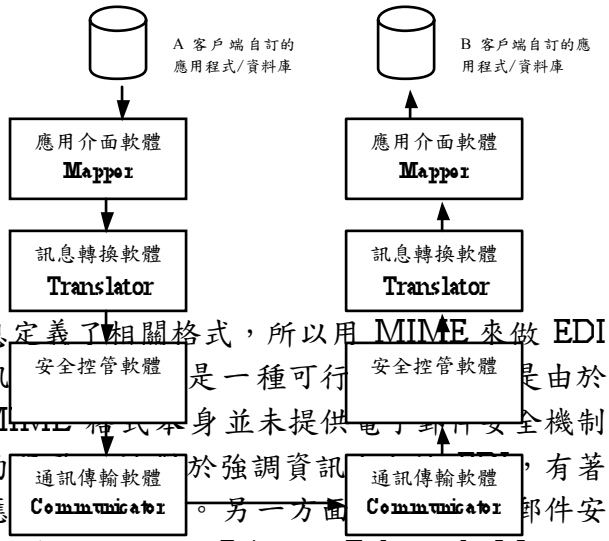
As communication networks been highly developed, the Electronic Data Exchange(EDI) has become essential to the success of the operation of governments and enterprises. When an EDI document is transferred on an open network, such as the Internet, it can be exchanged more rapidly and conveniently; thus, the performance of the enterprise is improved. However, an EDI document inevitably faces various threats; e.g., data stealing or manipulation, when electronic information is transmitted via open networks. Consequently, the security of EDI should be seriously concerned. This study will focus on applying Multipurpose Internet Mail Extensions (MIME) to integrate the EDI and the Internet e-mail security mechanisms.

Keyword: Electronic Data Interchange, Internet Electronic Mail Security Mechanisms, Multipurpose Internet Mail Extensions.

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。當 EDI 架構在一個開放式的網路上，如 Internet，可以使得資料交換更為快速便捷，從而提昇產業整體的效能。但是架構在一個開放式網路上之 EDI 會面臨四面八方的威脅，譬如資料的竊取、竄改等。如何在 Internet 上確保 EDI 資訊的安全，是一個很重要的研究課題。

RFC 1341 定義了多用途網際網路信件延伸（Multipurpose Internet Mail Extensions, MIME）。MIME 擴充了原始網際網路電子郵件的功能，允許使用者製作和讀取非文字格式的 mail 資訊，定義自己的訊息段落格式。RFC 1767 針對利用 MIME 傳送 EDI 訊



息定義了相關格式，所以用 MIME 來做 EDI 訊 是一種可行 由於 MIME 格式本身並未提供電子郵件安全機制 的 於強調資訊 有著 應 。另一方面 郵件安全機制，如 Privacy Enhenced Message（PEM）、Pretty Good Privacy（PGP）等，乃是為一般電子郵件的規格（RFC 822）所設計，並不能直接使用於 MIME 格式的電子郵件上。雖然近來有提出以 MIME multipart/signed、multipart/encrypted（RFC 1847）與 MIME Object Security Service（MOSS）（RFC 1848）為基礎的整合方案如 S/MIME 與 PGP/MIME，但仍屬發展初期，有待進一步的研究與改進。

本研究目的是，應用 MIME 整合 EDI 與網際網路電子郵件安全機制。我們會先做可行性分析：綜覽 MIME 的格式，分析現有電子郵件安全機制，討論這些協定在安全性及實際建構上的優缺點，探討 MOSS、S/MIME 與 PGP/MIME 格式，研究如何將其與 EDI 做完美的整合。在可行性分析後，會以一金融 EDI 訂單子系統為例，建立一個以 PGP/MIME 為基礎的雛形系統，並以此雛形系統實際評估 EDI 與電子郵件安全機制的整合效果。

三、結果與討論

（一）以 MIME 結合 EDI 與網際網路電子郵件安全機制的架構

針對現有的 EDI 傳輸方式及種種的網際網路電子郵件安全機制，我們提出一個整合的架構如圖 1：

圖 1 安全的 Internet EDI 傳輸架構

基本的 EDI 傳輸包括了應用介面軟體、訊息轉換軟體及通訊傳輸軟體，而我們在傳輸之前再加上一安全控管軟體以確保訊息的正確性及傳輸過程的安全性。

1. 應用介面軟體 Mapper

應用介面軟體是介於客戶端的應用程式、資料庫系統與轉換軟體間的物件，功能是在傳送 EDI 訊息出去時將客戶端自訂格式的檔案資料轉換成訊息轉換軟體可處理的 EDI 訊息平面資料檔(Flat file)，及當收到 EDI 訊息時將訊息轉換軟體轉換後的 EDI 訊息平面資料檔再轉換成系統可讀取的檔案資料。

2. 訊息轉換軟體 Translator

訊息轉換軟體提供 EDI 訊息的轉換，可將應用介面軟體產生的 EDI 訊息平面資料檔轉換成標準的 EDI 格式檔案；反之可將收到的 EDI 格式檔案轉換成 EDI 訊息平面資料檔(Flat file)。對於轉換軟體的選擇性，亦即其所提供的 EDI 訊息轉換標準，目前較常使用的為之前介紹的 UN/EDIFACT 及 ANSI X.12。

3. 安全控管軟體

提供訊息資料安全控管功能，以加密、數位簽章等方式對傳送的 EDI 訊息提供了訊息完整性、不可否認性、訊息隱密性等等。

4. 通訊傳輸軟體

即負責 EDI 資料的傳輸。在本研究中，我們使用 MIME 格式以 SMTP 的方式來傳輸。

（二）以 PGP/MIME 為基礎的系統實作探討

1. 系統實作環境

實作及測試環境所需的硬體設備主要包括了：

- Sun Ultra 10 Workstation 一台
- 插有 RJ-45 網路卡之 Pentium PC 兩台

實作所用到的相關軟體程式及作業平台：

- 提供 E-mail 服務的 Sun Ultra 10 Workstation 以 SunOS 5.7 為執行平台
- Client 端以 Win95 OSR2/Win98 為程式發展執行平台
- sendmail.8.8.8
- RSAEURO 1.06 cryptography library
- Borland C++ Builder 4.0 為程式開發及編譯環境

2. 實作系統規格選擇

根據實作的可行性考量及規格和參考資料的取得，實作系統採用了以下的規格：

- EDI：UN/EDIFACT
- MIME 安全機制：PGP/MIME

ANSI X.12 為美國所訂定的 EDI 標準，目前採用此一標準的區域為北美；UN/EDIFACT 為聯合國所訂定，目前已獲國際性的承認及採用。所以，我們決定採用接受度高、使用範圍廣的 UN/EDIFACT 為實作的 EDI 標準。

在 MIME 安全機制中，我們研究了 MOSS、S/MIME 及 PGP/MIME。MOSS 為一較早期的 MIME 安全機制，主要功用可說是為 MIME 安全機制提供了一個雛形及範例，S/MIME 及 PGP/MIME 均參考 MOSS 而改進。而 S/MIME 需要一個完整的 CA 架構來做認證的核發、管理與作廢，而在台灣目前的環境中並無功能完整的 CA，如以 S/MIME 來實作可能在 CA 部分會有實作的困難，所以我們採用不需要 CA 的 PGP/MIME 為實作的 MIME 安全機制。

（三）系統模組及功能說明

實作系統的流程，如圖 2，可大分為 EDI 資料發送端跟 EDI 資料接收端兩方面，透過 EDI Center 提供的 E-Mail Server 來溝通。

1. RSA 金匙對產生程式

主要功能為產生發送端及接收端加解密所需的公開金匙及私密金匙。程式每次執行時透過不同的亂數作為起始值，讓不同使用者得到相異的 RSA 金匙對。

2. EDI 發送端系統程式

EDI 發送端系統的工作在於從模擬訂單的使用者介面輸入，將 EDI 資料轉換成 EDIFACT 標準格式並做 MIME 封裝，再經符合 PGP/MIME 規格的簽章及加密，經由 SMTP 將 EDI 資料寄送出去。整個 EDI 發送端系統可分為下列六個模組：

(1) 使用者介面

模擬一公司系統中的傳送訂單子系統，在選單中提供了 Security 選單讓使用者選擇是否簽章及是否加密的選項，並要求使用者指定發送端的私密金匙檔案及接收端的公開金匙；Mail Setting 選單則提供使用者輸入寄送電子郵件所必需的資訊。

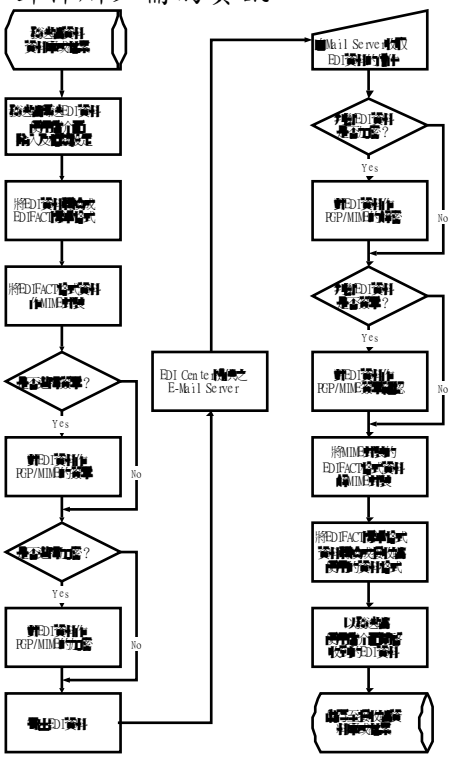


圖 2 EDI 資料發送及接收端系統流程

(2) EDIFACT 轉換模組

主要的工作是將使用者介面輸出的 EDI 資料轉換成符合 EDIFACT 標準格式的檔案。

(3) EDIFACT 的 MIME 封裝模組

主要的工作是將 EDIFACT 轉換模組所輸出的 EDIFACT 格式檔案加上 MIME 封裝。

(4) PGP/MIME 簽章模組

當在使用者介面中選擇要簽章時會執行此模組。此模組的主要工作為：對 EDIFACT 資料做 MD5 的訊息摘要後，再以發送端的私密金匙對訊息摘要作加密，完成 PGP/MIME 的簽章後再以適當的 MIME Header 封裝。

(5) PGP/MIME 加密模組

當在使用者介面中選擇要加密時會執行此模組。此模組的主要工作為：隨機產生一 IDEA 交談金匙對 EDI 資料加密，再以接收方的 RSA 公開金匙加密交談金匙。加密後本文外再加上適當的 MIME Header 封裝。

(6) 電子郵件傳輸模組

此模組的主要工作是把處理完畢的 EDI 資料，經過傳輸編碼後寄送到指定的 EDI 資料接收端的電子郵件信箱。

3. EDI 接收端系統程式

EDI 接收端系統的工作由電子郵件接收程式開始，從接收端 EDI 專用的電子郵件信箱中收取 EDI 資料郵件，將收到的經加密及簽章的 EDI 資料做解密及簽章確認後，再從 EDIFACT 標準格式轉換成接收端所使用的資料格式，最後以模擬接收端的訂單系統的使用者介面來呈現收到的訂單。整個 EDI 接收端系統可分為下列五個模組：

(1) 電子郵件接收模組

此模組的主要工作是連接 POP3 Server，接收電子郵件信箱中的 EDI 資料並解傳輸編碼，接收後解讀 MIME Header 判斷資料是否加密、或僅有簽章、或是明文傳送。模組包含了 POP3 相關設定的選單。

(2) PGP/MIME 解密模組

主要工作判斷資料經過加密時，先利用接收端的私密金匙解出交談金匙，再對內文做解密。

(3) PGP/MIME 簽章驗證模組

主要工作是當判斷資料經過簽章時，先利用發送端的公開金匙解出 MD5 訊息摘要，再對簽章所封裝的內文做 MD5 訊息摘要比對訊息摘要是否相符。

(4) EDIFACT 格式轉換模組

此模組的主要工作是將以 EDIFACT 標準格式呈現的 EDI 資料，轉換成接收端自訂的檔案格式或資料庫格式。

(5) 接收端訂單介面

此訂單介面為模擬接收端公司之接收訂單子系統的接收情形。主要工作是將已轉成接收端自訂格式的訂單內容以模擬的介面呈現。

四、成果自評

將 EDI 架構在 Internet 上使 EDI 的應用範圍得以擴大，但 EDI 資料的安全問題也更形重要。UN/EDIFACT、ANSI X.12 等 EDI 標準的使用使 EDI 系統開發更加方便及標準化；而 MOSS、S/MIME 及 PGP/MIME 等 MIME 安全機制可針對各種產業 EDI 所需不同程度的安全需求提供適合的服務，在轉換成 EDI 標準格式的 EDI 資料外加上 MIME 安全機制使得 EDI 資料能在 Internet 上以電子郵件的方式安全的傳遞。我們利用 UN/EDIFACT 及 PGP/MIME 模擬了兩機構間的金融 EDI 訂單傳輸子系統，從而確認在網際網路上應用 MIME 整合 EDI 與電子郵件安全機制是可行的。

未來有下面幾個方向可以去繼續研究和探討：結合真正的 CA 以擴大應用範圍和實用性、系統可與智慧卡(Smart Card)結合，將雙方的私密金匙及憑證存放於智慧卡上，當要存取智慧卡上的資料時必須先輸入一個個人識別碼可提供多一層的保護，比將私密金匙存放於沒有保障的硬碟機中要來得安全。

五、參考文獻

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

[2] R. Power. R., "UN/EDIFACT Syntax Implementation Guideline", UNECE

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

[4] N. Borenstein, N. Freed., "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing

the Format of Internet Message Bodies, RFC 1341", June 1992

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

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

[7] D. Atkins, W. Stallings, P. Zimmermann, "PGP Message Exchange Formats, RFC 1991", August 1996

[8] J. Linn, "Privacy Enhancement for Internet Electronic Mail, Part I-IV, RFC 1421-1424", IAB 1993

[9] S. Crocker, "MIME Object Security Services, RFC 1848", October 1995

[10] J. Galvin , "Security Multiparts for MIME, RFC 1847", October 1995

[11] S. Dusse, "S/MIME Version 2 Message Specification, RFC 2311", March 1998

[12] B. Kaliski. "PKCS #1: RSA Encryption Version 1.5, RFC 2313", March 1998

[13] B. Kaliski, "PKCS #7: Cryptographic Message Syntax Version 1.5, RFC 2315", March 1998

[14] B. Kaliski. "PKCS 10: Certification Request Syntax Version 1.5, RFC 2314", March 1998

[15] M. Elkins, "MIME Security with Pretty Good Privacy, RFC 2015", October 1996

[16] Chuck Shih, "MIME-based Secure EDI, draft-ietf-ediint-as1-08", May 1998