輔仁管理評論

中華民國 93 年 9 月，第十一卷第二期，183-206

應用 XML/EDI 整合技術建立供應鏈廠商間訊息交換與資訊共享機制之研究

邱瑞科．郁筱平*

(收稿日期：90 年 11 月 6 日；第一次修正：92 年 7 月 21 日；
接受刊登日期：92 年 10 月 23 日)

摘要

隨著全球貿易自由化的腳步，在我國加入 WTO (Organization of World Trade) 世界貿易組織之後，企業間的競爭必然越加劇烈。因此如何有效利用供應鏈電子化訊息交換策略將有助於強化企業間資料的傳遞並進而提昇企業的競爭優勢。

與傳統 EDI (Electronic Data Interchange) 的比較下，透過網際網路的傳遞路徑，將可有效的降低企業資料傳遞成本，而常見的傳遞方案則是 HTTP (Hypertext Transport Protovol) 以及 MIME (Multipurpose Internet Mail Extension) 方式，配合上安全機制的資料保密方案，便可達成於網際網路的安全傳遞資訊的低成本方案。

由於 XML (eXtensible Markup Language) 資料格式具有較大的彈性，且能有效整合近代資料傳遞安全的機制，因此被許多研究者認為它將替代傳統 EDI 格式作為資料傳遞與交換之最可行的解決方案。本文中提出以 Rosettanet 所制定之 PIP (Partner Interface Process) 規格整合傳統 EDI 技術，利用 XML 資料格式，並加入 S/MIME (MIME-base Secure EDI) 之安全機制來代替傳統 EDI 格式來進行企業間安全資料交換及傳遞的系統建立，並結合企業內部 MIS 系統，可以提供企業界在網際網路上一個低成本、高效能且具高安全性的最佳的資料傳輸解決方案。

本文中提出一個符合 S/MIME v3 之 XML 安全資料交換系統架構用於供應鏈管理所建立之進銷存雛型系統，其主要的技術元件包括進銷存系統、XML 資料格式轉換以及安全性元件的使用。本文的研究成果及系統發展之經驗必可供讀者、後續研究者及企業進行類似研究及系統建置之參考。

關鍵詞彙：電子資料交換，S/MIME，XML/EDI，電子化企業，供應鏈系統

壹．前言

網際網路的發展，再加上其網際網路所具有的迅速傳遞資訊與不受時間與空間限制的特性，使得各式各樣的資訊皆可以容易的由網際網路上迅速取得。傳統的 EDI 有成本高、開放性低及安全性不足的缺失，EOI (EDI over Internet) 或是其他資料格式傳遞於網際網路上的方案自然也為訊息交換提供了一個新的途徑，目前正有許多研究人員進行有關 XML/EDI 之研究，相關的資料可自 XML/EDI Group 的網站中取得，目前世界上已有超過 800 家的企業

* 作者簡介：邱瑞科，輔仁大學資訊管理系副教授；郁筱平，中華民國財政部台北關稅局資深軟件工程師專員。

加入此一組織，並企圖將過去各種的 EDI 格式轉換成 XML 格式，以利於網際網路上傳遞[29]。但是在網際網路上傳遞的訊息仍然是非常容易遭到有心人士的截取，因此為保證資料只能被傳送者所指定的接收者讀取，必須有效的建立安全傳遞機制，PGP/MIME (Pretty Good Privacy/Multipurpose Internet Mail Extension)、PEM/MIME (Privacy Enhanced Mail/Multipurpose Internet Mail Extension) 及 S/MIME (MIME-base Secure EDI) 等方式便是利用 MIME 方式進行安全傳遞的方案，而使用 HTTP 協定時，則常用 SSL (Secure Sockets Layer) 方式進行安全性的防護。

隨著技術的演進，在 XML 資料格式逐漸形成 EOI 的方案時，利用 XML 資料格式作為傳遞的資料格式，已被許多研究者進行其可行性研究。在本研究中，乃遵循 XML 之資料格式，提出一套得以藉由 HTTP 以及 S/MIME 機制下的傳遞雛形系統，並將發展的經驗討論於本論文中，以做為企業在建置安全資料傳遞雛形上之參考。

貳．文獻探討及相關學術研究

一、電子資料交換

在過去，供應鏈廠商之間的訊息傳遞皆透過電子資料交換 (EDI) 方式進行。所謂電子資料交換，簡而言之就是一套自動的訊息溝通工具，藉由電腦的資料處理與通訊功能，將交易雙方彼此往來的商業文件，像是詢價單或訂貨單等文件，利用標準格式的電子資料透過通訊網路，將交易訊息傳送給交易對象。EDI 最大的特色，是利用電腦與通訊網路來完成標準格式的資料流通，無須人為的資料重複鍵入，而且因其訊息建構法則與訊息含義具有共通的標準，雙方所往來的資料便能被雙方的電腦系統所辨識與處理，因此也就使得資料的傳輸與交易的效率可以大幅提升。

目前國際常用的 EDI 標準有北美地區的 X.12 和國際標準的 EDIFACT (EDI For Administration, Commerce and Transportation) 等兩種[1][2]。

由於傳統 EDI 於傳遞時必須藉由公正的第三人做為認證基礎，因此傳輸時期之成本必須包含其認費用，以目前關貿網路公司之收費方式而言，其收費方式如下[14]：

1.郵箱租用費，分成撥接與專線二種類別，撥接為每月每一郵箱 650 元；專線為每月每一郵箱 5000 元，第二郵箱起為每月每一郵箱 2500 元；若

採用定時主動傳送者，其郵箱租用費按每一郵箱每月 5000 元收費，第二郵箱起為每月每一郵箱 2500 元。

2.訊息傳遞與接收費用，分成離峰與尖峰二種費用，離峰時段每千字元組收費 4.65 元，尖峰時段每千字元組收費 7.5 元；若採用定時主動傳送者，其每千字元組收費 2.5 元。

上述費用計算並不含網路連線費用。但若使用網際網路做為傳輸方式者，其負擔之費用除了同樣需要網路連線費用外，其信箱費用與訊息傳遞與接收費用皆可省略，但需負擔網路憑證費用，以國內 HiTrust 公司而言[13]，其一年之憑證費僅需 299 元，遠低於採用傳統 EDI 方式之信箱租用費 7800 元/年。

由於網際網路的迅速發展，再加上其網際網路所具有的迅速傳遞資訊與不受時間與空間限制的特性，使得各式各樣的資訊皆可以較低成本的代價，經由網際網路上迅速取得，而 EDI over Internet (EOI) 的做法自然也為訊息交換提供了一個新的途徑。過去 EOI 的做法乃是將 EDI 訊息利用網際網路傳遞，如此將可以降低傳遞成本，但是隨著 XML 技術的提出，將資料轉換成 XML 格式傳遞，已是目前許多研究人員所贊同的做法，如 EDI Group[29]、Rosettanet [25]等，且據 Rosettanet 表示其成員在全球已經有超過 400 家以上的企業加入該組織，並投入 XML 資料交換格式的研究。但在網際網路上進行資料傳遞與交換所遭遇的問題，除了文件格式、傳輸技術、網路效能之外，安全問題亦是大家所關心的議題。

二、EDI Over Internet的資料交換方式

常見的 EOI 做法，分別是全球資訊網 (WWW, World Wide Web)、電子郵件 (E-mail) 以及檔案傳遞協定 (FTP, File Transfer Protocol) 方式[3][5][11]。全球資訊網係利用瀏覽器方式，登入至伺服器主機上進行資料的瀏覽與擷取，電子郵件運用在資料交換上，則是將欲傳遞之資料以郵件方式包於 MIME 機制的軟體內進行傳遞，而檔案傳遞協定的方式，則是透過檔案傳輸軟體自動登入或是手動登入伺服器方式，在進入伺服器後選擇所需的檔案，而上述三種方案皆有其優缺點，例如 WWW 方案中需要人員的介入行為而中斷了自動化的機會，E-mail 方案則有批次執行時間的時間差問題，而 FTP 方案則有登入帳號的問題，因此必須要視實際上的需求選擇適當的方案，而其中全球資訊網與電子郵件傳遞方式則是較常見的運用方案。

雖然 EOI 的做法提供了一個便宜的傳遞途徑，卻也增加了訊息傳遞的危險性，其由於網際網路係為開放環境，傳遞的訊息是非常容易遭到有心人士的截取，諸如 Sniffer、SessionWare 等軟體，甚至於微軟公司之 Windows2000 作業系統所免費提供之 Network Monitor 服務程式，皆可輕易的於網路上攔截訊息封包並解讀內容。故透過網際網路傳遞訊息時，安全性的考量便非常重要。

儘管最早將 EDI 應用結合網際網路傳輸媒介的相關標準是 RFC1767[19]，且在這份文件提出了一個可在網際網路傳送 EDI 訊息的簡單方法，並做為相關標準的基礎；但是其內容卻未提及處理安全相關問題的做法，亦未說明建置的方針。因此，實際上並沒有依據這份文件建置而成的軟體出現，且也未達到實用的地步。有鑑於此，便有許多研究者基於 RFC1767 之基礎上，結合 PGP/MIME[21]或是 PEM/MIME[15][18][22][30]等安全機制進行 EDI 資料的傳遞，而使得 EDI Over Internet 變成可行[3][6][7][9][11]。

三、XML與RTF資料格式

談到 XML 時，必須先了解 RTF (Rich Text Format) 格式。RTF 格式是標籤語言的一種重要格式，標籤語言中的標籤常用來改變文字的外觀，如斜體、粗體、字型大小、文字縮排等，且於必要時標籤會啟動上述屬性，而於不需要時關閉上述屬性。由於標籤內沒有任何訊息告知有關整份文件的標籤規則，因此文件的作者能在文件中放置任何文字與樣式，並可以隨意編排順序。當然這種自由的格式，有其方便性，也有其缺點，問題之一是，當解讀某一部份的標籤時，可能無法得知標籤與其他部分是否有相關，以及為何被放置。這種鬆散的架構，除了作者之外，其他人似乎不可能產生相同的文件。問題之二是，特定的文件不能移植到其他的平台或裝置上，因為那些平台或裝置上並不存在文件的架構或規則，如此對其他人來說要開發一個能精準解譯文件的處理器是相當困難的。

解決上述問題之一的方法是採用 XML 資料格式，XML 文件必需遵循一組規則，這組規則正確的規範了文件應如何整合，同時也告知處理器在標籤語言中可讀取哪些元素，並判定哪些元素可以包含哪些元素，以及識別何種類型的外部檔案可以置放於文件中。而這些規則都包含在文件型別定義中，此文件型別定義稱為 DTD (Document Type Definition)，在 XML 文件中 DTD 的宣告，可以讓處理器知道該用哪一個 DTD。

DTD 有效的指出 XML 文件中的結構規則，使得 XML 解析器可以正確的驗證 XML 文件，並使得該 XML 文件內容得以被分享。事實上 DTD 文件可能

存在與 XML 文件同一部電腦內，或是同一企業內，或是網際網路上另一個企業內，因此對於進行資訊交換的雙方必須取得有效且相同的 DTD，以確認所交換的 XML 文件具有相同的驗證格式[28]。

XML 在與 HTML 以及 SGML (Standard Generalized Markup Language) 比較上，XML 格式充分的表現出更適合作為資料傳遞格式的特性，因為 XML 有能力整合並處理資料的顯示及表現方式，所以對於在 Web 上傳遞資料，XML 更是具備了一些超越 SGML 與 HTML 的優點：

1.XML 的設計者嘗試在 SGML 中去除一些在 Web 傳遞資料上所不需要的東西。如基本的 SGML 規格書有 155 頁之多，而 XML 的規格書則僅有 35 頁。

2.XML 不僅支援在 HTML 中的基本超連結，並且應用了延伸鏈結，這種鏈結規格被描述成一種獨立的語言，稱為可延伸的鏈結語言 (XLL, Extensible Linking Language)。

3.XML 包含了樣式語言的規格，此種樣式語言稱之為可延伸的樣式語言 (XSL, Extensible Stylesheet Language)。XSL 提供對樣式表格結構的支援，並提供某些在 SGML 中找不到的支援，樣式表格允許作者為相同文件開發不同樣式的樣版，甚至結合多重樣式並應用他們於文件中的元素。

這 XML 許多的特徵，意味著 XML 不但具有語言特性，更可以定義標準的文件，而這個標準文件的特性，便可被利用來製作出不同企業間的標準文件，並藉以達成應用 XML 整合供應鏈廠商間訊息交換及資訊共享的參考方案。

四、安全性的探討

由於在網路上，訊息封包將經由一連串的網路節點傳遞給接收方，因此有心人士企圖攔截其傳遞於網路上封包，是相當容易的事，也因此使得在網際網路上進行訊息傳遞將面臨到資料被竊取的危機。為避免資料被竊取，使用在網路上的解決方案可以是，接收端與傳送端直接建立獨立的專線，但是此法的成本非常的高，並非企業所樂見的方案。較常用的解決方案則是使用較低成本的傳輸管道並經由加密方式，即使資料被竊取，其竊取者亦無法解讀其內容，如此便可保證資料的安全性。

密碼學發展至今，已有三大類的密碼系統，第一類是對稱金鑰 (Symmetric Key) 密碼系統，第二類是非對稱金鑰 (Asymmetric Key) 密碼系統或簡稱公

開金鑰 (PKI, Public Key Infrastructure) 密碼系統，第三類是信託金鑰密碼 (Key Escrow) 系統或稱金鑰回復式 (Key Recovery) 密碼系統[8, 12]。在實際的運用時，則通常混合了上述之二種或二種以上的金鑰安全機制，以達到更高的安全性。

在 HTTP 的資料傳輸機制下，常使用 Secure Socket Layer (SSL) 機制作為安全性之防護。SSL 是由 Netscape 所制定的加密協定，其目的是為了網路傳輸中的不特定資料進行加密動作，只用來確保資料傳輸的安全性，而非設計於特定的用途之上。SSL 經過多次改進，目前最新的版本為 SSL 3.0 協定。SSL 3.0 的做法是在雙方進行通訊之前，以非對稱式金鑰演算法之公開金鑰進行身分認證，而雙方同時協調出一個通訊用的會期金匙，之後的所有訊息則均以此會期金匙做加密傳送。由於對加密演算法及金鑰長度均無限制，因此可用標準的加密演算法，也可利用自行開發的演算法進行加密。一般而言，SSL 使用 MD5 的訊息摘要，與 RC4 的個人密碼。目前因為美國外銷法令 (Export Law) 規定，故 RC4 在可採用 128 位元的安全認證方式，因此 SSL 可以使用 128 位元之加密鍵值。依據微軟公司指出，其公司在內建置 SSL 安全機制於其每一種作業系統與 Internet Explorer 中時，均會將 RSA (Rivest-Shamir-Adleman) [23] 加密演算法整合內建於其中。

在 MIME 的機制下，較具代表性有 PEM/MIME、PGP/MIME、S/MIME 等三種機制。三者具有不同程度的安全建置的方式，以下分別說明它們之間的主要建置特性。

(一)PGP/MIME

PGP/MIME 是 1991 年由 Phil Zimmermann[21]所提出。它強調以 Freeware 方式在 Internet 上散佈給任何人使用，而目前則有許多的版本存在於市面上。PGP 使用之 RSA 演算法[12]所使用的金鑰長度是可選擇的，某些版本提供有 384 bits、512 bits、1024 bits 供選擇，某些版本則提供 512 bits、768 bits、1024 bits、或允許使用者自訂金鑰長度。其做法上是利用以 MD5 (Message Digest 5) 對訊息本體產生長度為 128bit 之訊息摘要 (Hash Code)，再以 RSA 演算法用發信者的私密鍵對訊息摘要做簽章後，將簽章資訊加至訊息本體尾端作為身分認證之用，但是此數位簽章部份是選擇性的項目。對資料而言，則是以亂數隨機產生一個 128 bits 之會期金鑰 (Session Key)。利用 IDEA (International Data Encryption Algorithm) 演算法，並以此用會期金鑰對訊息本體加密，再以 RSA 演算法用收件者的公開鍵 (Public Key) 對會期金鑰做加密，最後則是將加密

後的訊息本體及加密後的會期金鑰結合成最後的文件。一項特色是，在數位簽章步驟完成後，可以對資料進行壓縮或不壓縮。其在認證基礎上，則是採用小團體彼此認證方式，因此在資料傳遞上或許已經安全，但對通訊雙方的身份確認上，卻具有不確定性的隱憂。

(二)PEM/MIME

PEM/MIME[15, 18, 22, 30]是在網際網路上以安全電子郵件傳送企業資料文件的另一個標準，它提供安全相關的服務給發展電子郵件的使用者。PEM/MIME 的規格包括了 RFC1421、RFC1422、RFC1423、RFC1424 四個 Request For Comment (RFC)，其 RFC1421 定義了訊息加密與來源鑑別之程序，RFC1422 定義了系統所需之基礎建設[30]，RFC1423 定義了加密演算法規範[18]，RFC1424 則定義了金鑰之註冊、註銷及取用資訊[15]，因此 PEM/MIME 一樣具有身分驗證、資料加密、密碼認證等功能。

訊息摘要可由 MD2 或 MD5 產生，其產生之訊息摘要，再以 RSA 對訊息摘要做加密，就形成了數位簽章。但其訊息摘要，以 DES (Data Encryption Standard) 或 triple DES 對訊息摘要做加密，則稱為電子密碼簿 (Electronic Codebook)。其會期金鑰亦是隨機產生一個 128 bits 之亂數金鑰。訊息本體加密則是以 DES 演算法用會期金鑰對訊息本體加密後，再使用 RSA 演算法用收件者的公開鍵 (Public Key) 對 Session Key 做加密。而會期金鑰則可使用 DES 或 triple DES 演算法對會期金鑰做加密，並將加密後的訊息本體及加密後的會期金鑰組成傳遞的密文，PEM/MIME 並未定義資料壓縮的功能。其在認證基礎上，係採用 X.509 的階層式認證 (Certification Authorities, CA) 來做為使用者的證明文件。

(三)S/MIME

S/MIME[17]是 MIME 與 PKCS#1、PKCS#7、PKCS#10 的結合，目前最新的版本為第三版，其相關的 Request For Comment 為 RFC2630、RFC2631、RFC2632、RFC2633、RFC2634。

訊息摘要可由 MD5 或 SHA1 產生，其產生之訊息摘要，再以 RSA 對訊息摘要做加密而形成具有身分證明的數位簽章。其訊息本體加密則是可採用 RC2 (40 bits) 演算法或是 triple DES 演算法對訊息本體加密，其在認證基礎上，同樣係採用 X.509 的階層式認證來做為使用者的證明文件。S/MIME v3 版為增加 S/MIME 的安全性而利用 RFC2634 以增強其安全性，這是 S/MIME

v2 版中所沒有的，但在 S/MIME v3 版的文件內容中，強調必須與 S/MIME v2 版相容，因此在許多地方 S/MIME v3 版則是使用比 S/MIME v2 版較長位元的加解密演算法，或是建議改用較佳的演算法。其相關的 RFC 內容大致如表一。而 S/MIME V3 版主要演算法相關規定如表二。

表一　S/MIMEv3 版相關 RFC 內容簡述

RFC2630[26]	描述有關加解密的語法，包括數位簽章、簽章時間、簽章演算法、密鑰管理演算法、金鑰協議演算法、金鑰運輸演算法等規範。
RFC2631[20]	描述 Diffie-Hellman 演算法，如何用發信者的私密鍵對訊息摘要做簽章加密。
RFC2632[16]	描述 S/MIME 憑證管理 (Certificate Handling) 的規範，其中明確指出 S/MIME 之憑證管理係遵循 X.509 的規範。
RFC2633[17]	描述 S/MIME 訊息規格說明，包括傳送與接收代理程式的規範，訊息摘要與簽章的確認等。
RFC2634[24]	增強 S/MIME 的安全性，其中此部份是無法與 S/MIME v2 版相容的，但是這部分是可選擇性加入的。主要說明四項服務：簽章收據 (signed receipts)、安全性標籤 (security labels)、安全的郵寄表 (secure mailing lists)、簽章證明書 (signing certificates)。

表二　S/MIMEv3 版演算法規定

訊息驗證	可選擇使用 MD5 或 SHA-1 產生訊息摘要 (Hash Code)，再以 Diffie-Hellman 演算法用發信者的私密鍵對訊息摘要做簽章加密。
資料加密	加密方式可依不同安全需求等級對訊息本體提供二種對稱式加密方法：RC2 (40 bits) 演算法以及 triple DES 演算法。
認證基礎	依據 RFC2632，使用 X.509 方式，即透過 CA (Certification Authority) 來做證書的核發、確認及作廢等動作。

而其相關之加密與認證之資訊均係儲存於稱為簽章資料 (SignedData) 的欄位之中，簽章資料欄位主要分為三個部份，分別是簽章標頭 (Header)、認證欄位 (Cerificate) 以及簽章資訊 (SignedInfo)。在簽章標頭中載明有關於 S/MIME 版本及使用之訊息摘要演算法，在認證欄位中儲存了身份驗證資料，而簽章資訊欄位則保存了其他驗證所需的資訊。

其中對於 Diffie-Hellman 演算法之金鑰對的產生 (Key Pair Generation) 部分，由於由於受限於美國外銷法令之 128bits 長度限制，故 RFC2633 中針對此一限制建議，可採行多重加密方法增強安全性，本研究實做 中採用此多重加密之方法，作為加強安全性策略。然而在 RFC2633 中指出 512 bits 是危險的，故至少應為 768 bits，但 1024 bits 是較可行的安全長度。

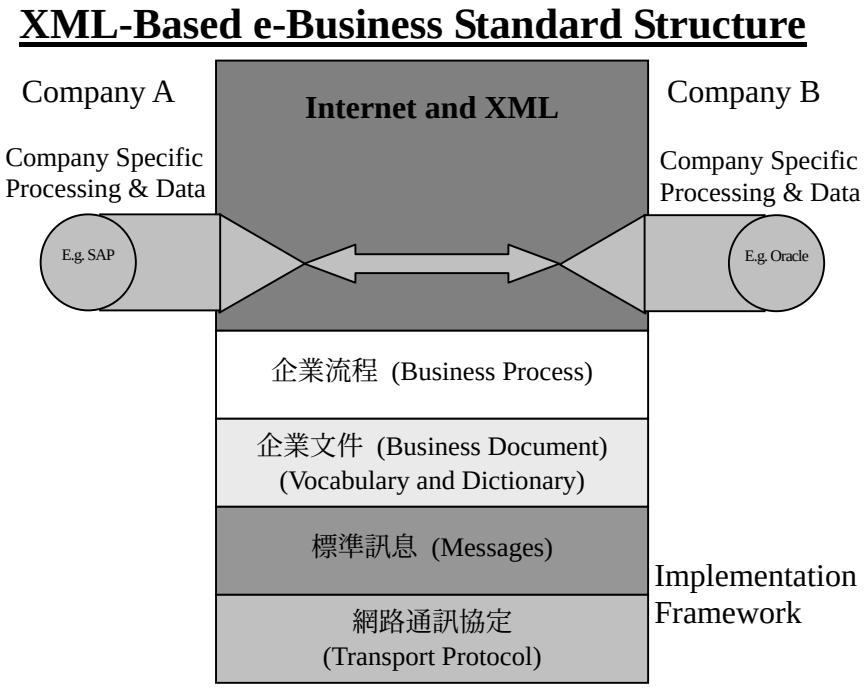
五、供應鏈管理系統

由於企業間的競爭是相當激烈，提昇競爭優勢則一直都是企業所關心的焦點之一，而供應鏈系統則被認為企業提升競爭力的方案之一，如能有效的利用供應鏈策略將有助於強化企業的競爭優勢。依據美國供應鏈協會 (Supply Chain council，SCC) 對供應鏈所下的定義是，供應鏈是由供應商的供應商、供應商、製造商、客戶、客戶的客戶之間，所有的相關活動，包括了原物料供需管理、產品製造、倉儲管理、總量稽核、運送交貨等活動。同時美國供應鏈協會也提出了一套供應鏈的參考模式 SCOR (Supply Chain Operation Reference-model) [27]。模式中包括四個基本的功能，計劃 (Plan)、資源 (Source)、製造 (Mark)、配送 (Deliver)，這些功能分別定義了供給與需求管理、物料資源的採購、產品的製造以及運送的程序。

在過去，市場供給的決定來自於製造商自己訂出的生產排程，因此製造商成為決定市場銷售量與價格控制者。但是現在卻改變了，使用者希望得到自己想要的，因而製造商開始為客戶量身訂做產品，而客戶成為決定市場的主要力量，而這種現象使得製造商必須快速且敏感的察覺使用者的需求，故供應鏈管理變得更加重要了。當製造商有效的透過供應鏈功能，則可將產品迅速且有效率的送達客戶手中，當然也提前反應了客戶產品需求的變動性，便使得供應鏈流程中的企業與客戶均蒙受其優勢。

六、Rosettanet的標準商業流程

Rosettanet 的標準商業流程是由 Rosettanet 組織[25]所制定的供應鏈交易夥伴間標準商業交易流程。它將 XML 標準格式格式溶入傳統 EDI 格式的交易訊息之中，並清楚的定義商業交易流程與架構如圖一所示。



資料來源：http://www.rosettanet.org/

圖一　電子商務標準架構

而 RosettaNet 目標在於推動企業間的合作協力發展且快速應用以網際網路為基礎的商務標準, 並發展出共通的語言和開放式的電子商務程序以提供可見的利益，並進一步提昇全球高科技交易網路的進化[25]。

Rosettanet 架構指出，所謂的 Rosettanet 標準規範三個功能層，包括 RNIF (RosettaNet Implementation Framework) 及標準訊息兩個層次的規範、Dictionaries 及 PIPs (Partner Interface Process) 三者。RNIF 又包含網路通訊協定及標準訊息兩個次功能層用來規範 RosettaNet 訊息物件並具體說明貿易夥伴間如何的傳輸, 它提供共通的通訊協定藉以提供商業的服務, 為了交換訊息而採取 XML 標準文件格式。而 RosettaNet 的字典能降低因不同公司間使用不同的字彙而在採購流程中產生的誤解, 其商務字典則明確定義出買賣雙方的性質, 而 RosettaNet 技術辭典則將產品及服務作出清楚的解釋。RosettaNet 的 PIP 夥伴介面程序是一種於系統間以 XML 語言為基礎, 針對交易夥伴間的商業流程而訂的程序。每一套中介程序皆包括了附有字彙的商業文件及包含訊息的商業流程。PIP 可應用在各種的交易流程中，例如行政、會員、產品和服務的評估、產品介紹、訂單管理、庫存管理、行銷資訊管理、服務和支援、製造等等。

其所建議的 PIP 中，描述了流程的三要素，分別為商業操作規範 (Business Operational View, BOV)、功能服務規範 (Functional Service View, FSV) 及實作架構規範 (Implementation Framework View, IFV)。

(一)商業操作規範

商業操作規範是企業操作流程的說明，其單一文件中均針對單一流程做流程的說明，包括目的與步驟。例如 RosettaNet 之 PIP 3A1 文件為需求報價流程文件，其文件中指出需求報價是買方向賣方要求產品報價，而賣方也許回覆報價資訊或是傳回另一賣方的資訊，買方則再向新賣方要求報價。其作業流程包括四個步驟，分別為買方產生要求報價之需求、買方發出報價要求、賣方接收報價要求、賣方回覆報價要求。

又如 RosettaNet 之 PIP 2A2 文件為產品資訊查詢流程文件，其文件中指出使用者是買方向賣方要求產品資訊，而賣方將回覆產品相關訊息或是傳回另一賣方之產品相關資訊。其作業流程包括二個步驟，分別為使用者產生要求資訊之要求、買方則回覆使用者查詢產品之相關資訊。

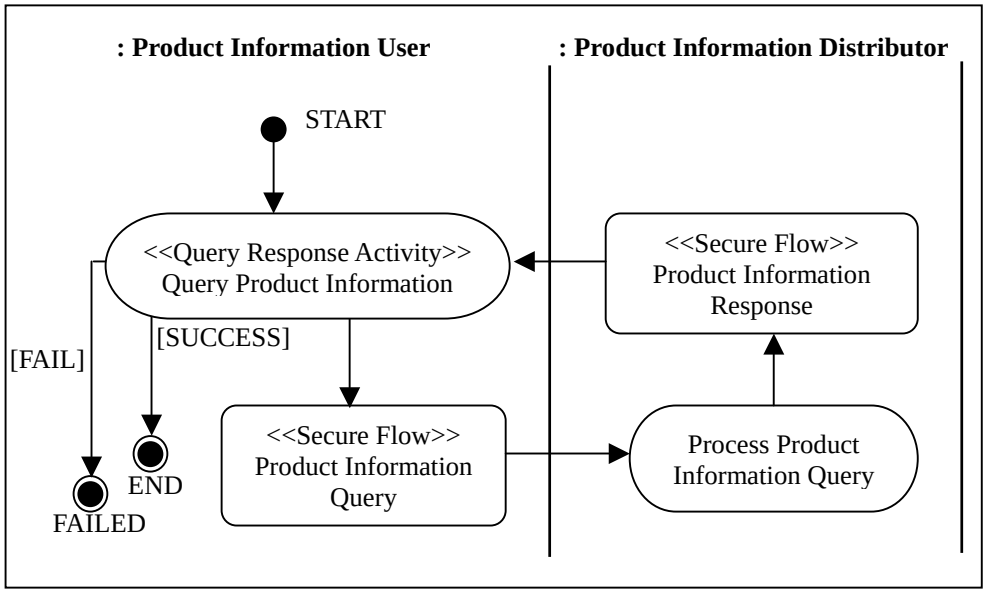
(二)功能服務規範

功能服務規範是介紹此流程所需的相關元件。在文件中說明此流程需要網路代理者 (Network Agent) 及企業服務者 (Business Service) 二元件。其元件之相互作用與延伸後，將使得原件之間的關係變成複雜。同樣以 3A1 需求報價為例，元件的關係變成了三種情況，分別是：

1. **Service-Agent-Service interaction configuration**：Services 交互作用於一個或多個 agents 之二端。典型的狀態是 services 並不知道其他的資訊或是當員工必須加入私人的資訊在活動中傳遞給其他的 service。
2. **Service-Service-Agent interaction configuration**：第二個 service 如同 agent 的 mailbox，記錄暫存的資訊。
3. **Agent-Service-Service interaction configuration**：service-to-service 交易處理是 agent-service 交易處理的子交易行為。

(三)實作架構規範

實作架構規範則是定義流程所需的架構，包括說明此流程是否需要認證與 SSL 之安全機制。如圖二即為 Rosettanet 之 PIP 2A2 所規範之查詢產品資訊文件之流程圖。



資料來源：http://www.rosettanet.org/

圖二　Rosettanet 之 PIP 2A2 Query Product Information 文件流程圖

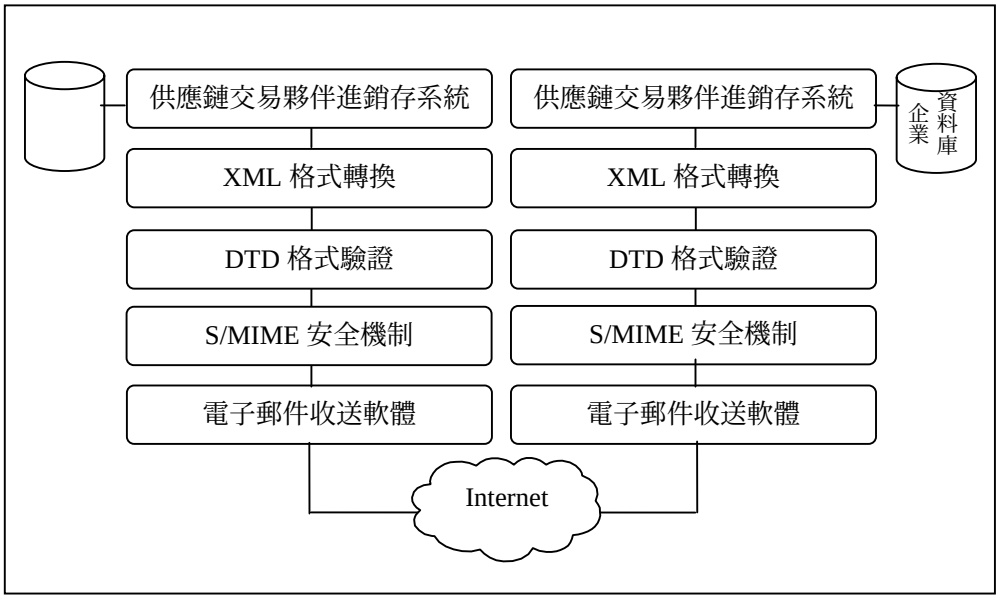
圖二中說明了產品使用者向產品供應商要求產品資訊之流程。在 Rosettanet 所建議之規範中，尚指明訊息交易的雙方對於另一方所發之訊息皆須以予回應，以供對方確認訊息已正確傳達對方，其回應時間亦被規範於其中。本系統中有關於流程部分，將會遵循 Rosettanet 所建議之商業流程進行，其流程中相關之有效回應時間、文件有效期限以及文件資料格式，亦將遵循 Rosettanet 所建議之相關規範進行。

參・實驗設計—供應鏈系統間之安全電子資料交換架構

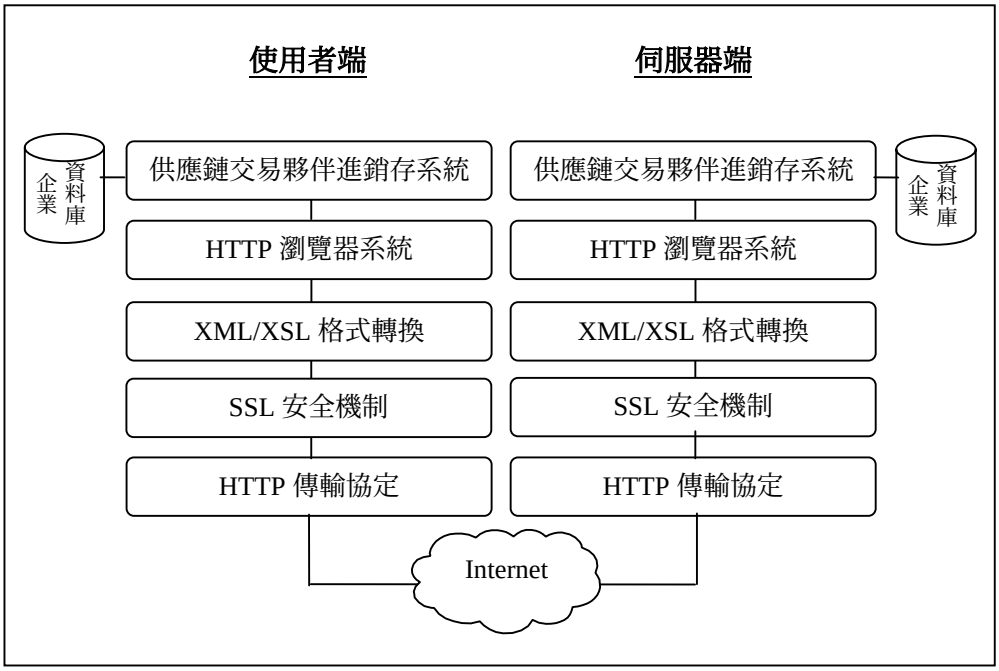
本研究的架構係針對 XML 與 S/MIME 之結合以及 XML 與 Secure HTTP 之結合的二種方案，並將 EDI 傳遞資料轉成 Rosettanet 標準 XML/EDI 資料格式，依 Rosettanet 所規範的交易流程建立層次性架構實作模式，同時也依此架構模式實際的建置了一套雛型交換系統。當然讀者亦可參考本研究之模型而使

用 PGP/MIME 或是 PEM/MIME 來取代 S/MIME 或 Secure HTTP 之安全電子郵件資料傳輸機制。

因此，在本研究中也實際建置了一套簡單的進銷存 MIS 系統，以完成整個供應鏈的運作。本研究之雛形系統架構描繪如圖三及圖四。



圖三　S/MIME 雛形系統架構圖



圖四　Secure HTTP 雛形系統架構

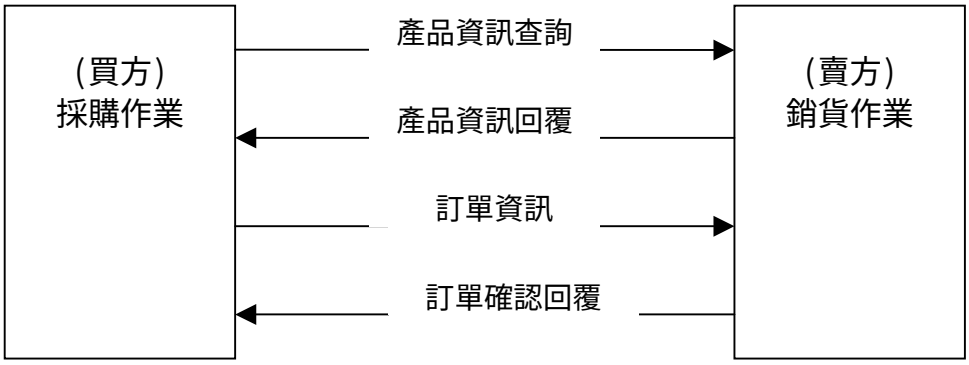
在雛形系統實作中，其系統實作部份係使用微軟公司之 Windows 2000 server 平台，並使用 IIS 5.0 以及該公司的 Visual Basic 6.0 程式語言開發系統，其資料庫部分則是以 Microsoft SQL 2000 作為資料庫，並且利用微軟公司所提供之 ADVAPI32.DLL 加解密元件及 XMLDOM 元件處理有關加解密與 XML 轉換的作業。而在硬體方面，則是使用了 Pentium IV 10GHz 以上 CPU 之個人電腦，作為硬體平台。不同運作系統架構則分別於下兩節中加以說明。

一、S/MIME雛形系統架構運作

(一)安全訊息傳遞

進銷存 MIS 系統針對 S/MIME 技術為基礎的安全傳輸為重點設計，其整體上的功能包括企業內部之資訊應用與安全機制的設計。本研究中以實驗方式建置了一套進銷存系統，模擬零售業/製造業供應鏈夥伴間的電子資料交換模式，其主要功能包括了如採購單之開立、訂單之確認、進貨單之建立等，其 XML 訊息傳遞部分則是直接利用 XML 所具有之自訂標籤特性自行訂立。雖然此系統只是一個實驗性的雛型系統，而且針對進銷存的系統為資訊系統研究標的，但系統應用的觀點完全可以移轉。因此，讀者可以依據自身需求開發出類似的系統，輕易的取代本研究之進銷存系統。

在本研究的實作的商業流程中主要包括產品資訊查詢、產品資訊回覆、訂單資訊、訂單確認回覆等四項，其流程如圖五。



圖五　訂貨作業商業流程

查詢作業流程指買方使用者依據特定條件發出產品查詢資訊，而賣方供應商則依據使用者要求之條件，回應其相關產品資訊。而當買方進行查詢作業時，首先進銷存系統將使用者條件轉換成符合 Rosettanet 標準之 XML 格式訊息，並經 DTD 驗證資訊後，再經由加密機制轉成密文後，利用 S/MIME v3 安全機制建立安全格式傳送給賣方。當賣方收到後，除了需將密文解密外，尚需利用 DTD 驗證 XML 文件，並需回覆相關產品資訊予買方。接下來的定單資訊及訂單確認回覆也是一相同的資料轉換及加解密方式進行。

(二)S/MIME加解密處理

本研究中，對於 S/MIME 加解密上乃遵循 S/MIME v3 版中之相關規範，並利用 Microsoft 公司之 advapi32.dll 函式庫所提供之加解密函數完成。

在訊息本體加密上，利用隨機產生之二個 Session Keys 做為 Triple DES 的加解密鍵，完成訊息本體加解密;而在訊息驗證上，則是利用 SHA-1 的演算法，將產生簽章資訊做驗證，其簽章資訊以及訊息本體使用之演算法等資訊，則利用 Diffie-Hellman 演算法，先用發信者之私密鍵加密後，再用收信者之公開鍵予以加密，以完成最後安全性的加密處理，再將訊息本體及以上經過加密的資訊形成一個安全可靠的郵包傳送至收信方。再依據 SMTP (Simple Mail Transport Protocol) 通訊協定為送信部份，並以 POP3 (Post Office Protocol 3) 通訊協定為收信部份。由於電子郵件技術已相當成熟，且市面上有著相當多的產品及函數庫支援，因此讀者可自行設計出符合本身需求之電子收送軟體或是引用現有的電子郵件軟體於系統中來提供電子郵遞的功能。

因受到美國密碼出口法令 128 bits 之限制，故亦僅能產生最長 128 bits 之鍵值，其安全性並不高。其解決方式是採用 RFC2633 中之建議，利用多組不同鍵值予以多重加密，以產生較高之安全性，因此本雛型中所產生的憑證，乃係隨機產生 8 組 128 bits 鍵值之憑證予使用者，而此處選擇 8 組之目的，在於遵循 RFC2633 之建議而採用 1024 bits 之長度。當使用者運用在加解密時，則必須連續完成 8 次加密或 8 次解密動作，雖較為耗時，但已可符合 RFC2633 之安全性要求。

二、Secure HTTP雛形系統架構運作架構

如圖四所示，本研究並依據 Secure HTTP 系統架構提供買方藉由 HTTP 傳輸協定至賣方網站進行網頁產品查詢的安全性資料傳送。Secure HTTP 主要是藉由 SSL 安全機制來進行資料傳送之加解密處理。

(一)SSL加解密處理

本雛型系統系以 SSL 3.0 為安全電子交換機制建立網頁資訊查詢的實作，並要求使用者端亦需具備有使用者端憑證。在本雛形實驗中，無論是伺服器端或是使用者端之憑證皆係以申請 HiTrust 公司[13]之測試用憑證作為實驗。SSL v3.0 被普遍應用在 Netscape 公司的 Navigator 瀏覽器，但 Microsoft 公司的 Explorer 瀏覽器亦完全可以支援。目前負責擔任簽發 SSL 協定所使用公鑰憑證的 CA，主要以美國 VeriSign 公司為主，任何人希望使用 SSL 來從事安全通訊者通常須向 VeriSign 公司註冊，取得公鑰憑證。

SSL 機制的金鑰憑證分為兩個等級，一個是僅有美國公民可申請，申請時必須提出身分證明且以離線方式處理；另一個資格較鬆，只要線上向其註冊，並回覆 VeriSign 所發出的確認 E-mail，即可獲得其金鑰憑證。

其在實際運作過程中，則是配合 IIS 5.0 所提供之 Request.ServerVariables 指令，以擷取使用者端之憑證資訊，並據以判定使用者的身分，同時該憑證也完成傳遞過程的加解密工作。

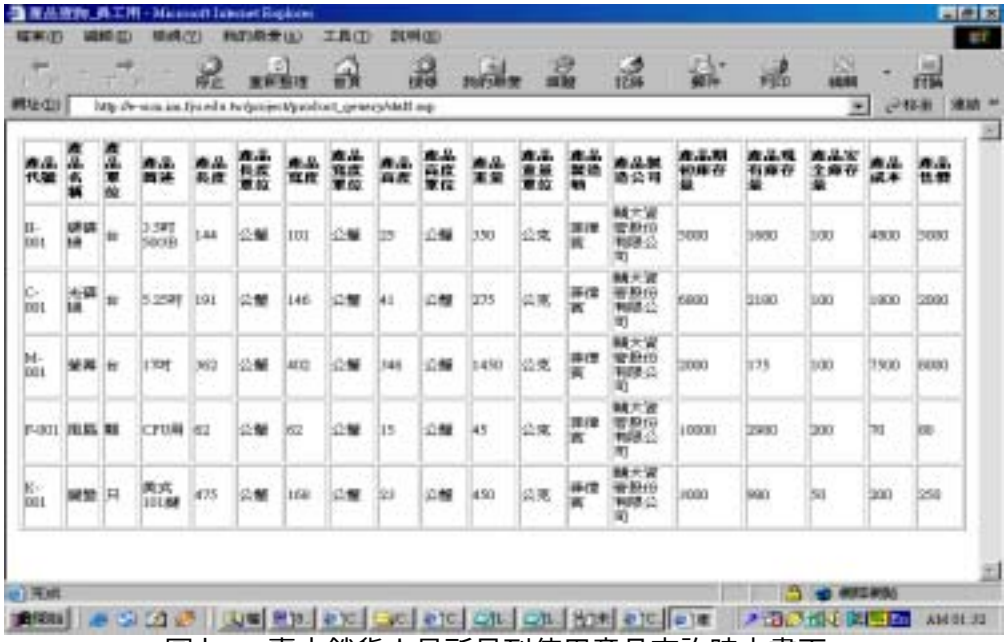
(二)XML/EDI訊息格式

由於本雛形系統實作中，係使用微軟公司之 IIS 5.0 作為伺服器平台，而使用端並無限制，唯必須是可以解析 XML 格式之瀏覽器。而由於使用之資料庫係為關聯式資料庫，因此需要進行 XML 資料格式轉換的作業。

在 XML 資料格式轉換上，SQL 2000 提供了透過 URL 指令，直接將 XML 自資料庫中轉出的功能，例如指令： HTTP://163.29.25.1/project?sql=select+*+from+product+for+xml+root=root，則可將 product 表格中的產品資料，全部擷取出來，並自動轉換成 XML 格式，呈現在瀏覽器上。

此外，利用 XMLDOM 物件配合 VB Script 指令，亦可得到類似的效果，再加上 XSL 樣板的套用，便可依據不同使用者給予不同資訊的作業模式，如圖六與圖七部分別是本雛形系統在不同人員對同一交易產品查詢時的所提供的不同查詢畫面，其畫面是依據相同條件查詢之產品資訊、並以不同樣本檔所得到之不同呈現結果，圖六顯示買方採購人員所看到產品查詢的畫面，而圖七顯示賣方銷貨人員所見到之產品查詢畫面。

圖六　買方採購人員使用產品查詢時所看到之畫面



圖七　賣方銷貨人員所見到使用產品查詢時之畫面

由於登入時之權限不同，因此在產品查詢時，將會使用不同的 ASP 查詢程式，並且套用不同的樣式檔，以呈現不同畫面或是遮閉部分資訊的效果。如圖七係為提供予賣方銷貨人員查詢畫面，因此畫面上可以看見全部資訊，包括

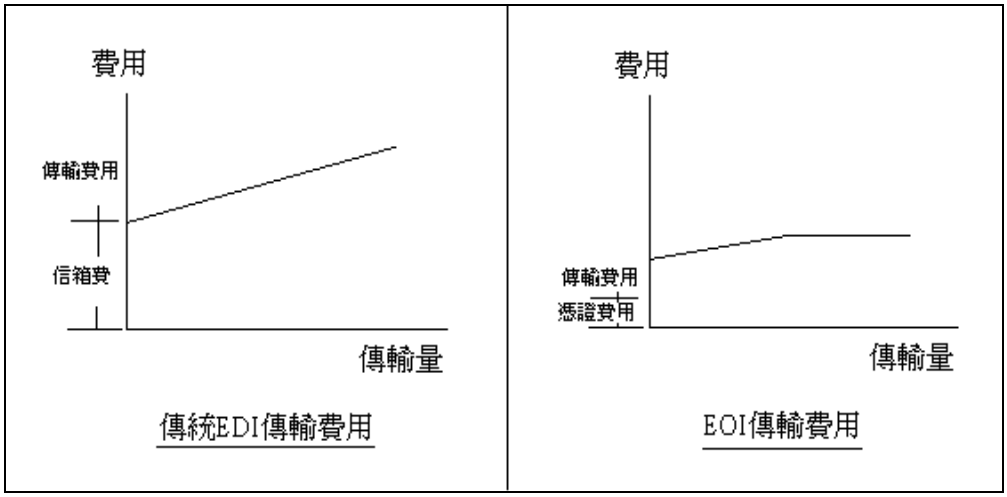
產品的期初庫存、現有庫存以及產品成本等資訊，而這些資訊在買方採購人員則是看不見的。

肆．實驗結果分析

一、雛形系統實驗結果

依據本雛型系統實驗結果，本雛型系統將傳遞的資料輕易轉換成符合 Rosettanet 之 PIP2A2 之 Product Information Query Message 標準格式之文件。此文件資料將再經過 S/MIME 的加密處理後，即可於網際網路上安全的傳遞。經過 S/MIME 的加密處理之文件傳至供應商端經過供應商解讀之訊息後，並依據要求將回應之訊息，其訊息格式為符合 Rosettanet 之 PIP2A2 之 Product Information Response Message 標準格式之文件，故實驗結果一可證明資料確實可經由 XML 格式傳送並被接收端正確的解讀。

就通信費用而言，本研究實驗之網路環境之二端分別為 T1 專線與 512K/64K 之 ADSL 專線，其傳遞品質則均可符合需求，故在線路使用上，本實驗證明確實可採用 ADSL 專線方式並透過網際網路進行。再依據現行中華電信之不優惠之收費標準為線路費 595 元以及網際網路使用費 499 元，合計每月 1094 元。EDI 信箱費用之基本費用每月則需 650 至 5000 元之間，故可得證將資料傳遞於網際網路上之傳遞成本遠低於傳統 EDI 方式。兩者之傳輸量與所需費用趨勢如圖八所示。



圖八　傳統 EDI 與 EOI 之傳輸費用比較圖

圖八中比較傳統 EDI 與 EOI 之傳輸之費用，其傳統 EDI 之信箱租用費已然明顯高於憑證費用與 EOI 之傳輸費用；此外對於 EOI 方案上，其傳輸費用將依據 ADSL 費用而有上限值，但傳統 EDI 費用則會與使用量呈正比而持續上升。

就建置費用而言，本研究雛型系統之實際系統發展建置階段，共約花費 2 人月時間，以一般公司程式設計人員按每月 5 萬元薪資計算，則本實驗之開發成本以人力成本計算則儘需 10 萬元。

二、雛形系統效益評估

本研究中，其主要目的在於透過 S/MIME v3 機制以及 Secure HTTP 機制，以整合企業內部之進銷存 MIS 系統，將 XML/EDI 訊息安全的傳遞於網際網路上。在結合企業內部系統上，本雛型系統有關於進銷存系統以及 EOI 系統部分，係分為二獨立模組來完成。模組之一先對企業進銷系統所產生 plain 文件資料存入一中間共通資料庫，模組之二之安全傳遞模組再由此中間資料庫提取文件資料進行後續的安全建置及傳送的工作。此二模組間利用共通資料庫作為資料整合介面。因此現行企業若已有此類進銷存系統，則僅需引用本雛型之 EOI 傳遞模組部分，並將傳遞資料遞送或擷取此共通資料庫，便可達成與企業現有系統整合之要求。且 EOI 傳遞模組部分又可分為 S/MIME 機制與 Secure HTTP 機制二部分，因此企業亦可依其實際需求，進行實際之企業流程運作，此為本研究中對於整合現行企業 MIS 系統之貢獻。而在不同企業間建立訊息交換機制，明顯的可以幫助企業群體達成加速資訊流的目的，進而增加企業群體的商機。此外，訊息交換機制亦為供應鏈系統之基礎，因此建立訊息交換機制，亦將對企業有正面且長遠的效益。

在開發成本上，本研究雛型系統採用元件化開發方式，並以模組方式針對單一訊息逐步加入系統中，因此其架構呈現可大可小的特性，對於台灣擁有之 85%之中小型企業而言，其低開發成本與高便利性，絕對有正面的效益。

在傳遞方案上，研究中實作了 Secure HTTP 與 Secure/MIME 二種傳遞方式，透過任一傳遞方式皆可將訊息送達。雖藉由 MIME 方案傳遞資訊的方案雖並不創新，但卻尚鮮有 XML 資料格式利用 MIME 機制上傳遞之研究報告的產生，而本研究則是證實 S/MIME 進行傳遞是可行的方案，至於運用 PGP/MIME 或是 PEM/MIME 之傳遞方案上，則可提供其他研究者進行後續類似的研究。

在傳遞資料格式上，本研究中乃採取了 XML/EDI 作為傳遞訊息格式，並與過去傳統 EDI 格式的一對一轉換。XML 技術發展至目前為止，仍然在快速的演進與進步之中，許多新的技術正被提出與被認同之中，例如 XML Schema、Xlink 等。而本研究中僅僅使用 XML 轉換技術與 DTD 驗證，後續的實務建置者及研究者對於未來 XML 被提出的相關新技術可再進行類似的實作及研究。

在安全性方面，我們於訊息傳遞過程中，加入 S/MIME 與 SSL 安全機制，此機制以現階段而言，仍屬於安全機制。而此可信賴的安全機制，同樣達成了身分確認、私密性、正確性與不可否認性四項安全原則。

因此本研究提出之架構，不僅明顯降低加入供應鏈之建置時間與適應時間，同時又具有延展資訊系統的長度的效益，且可作為供應鏈系統的基石，歸納本架構提供了下列的具體效益：

1. **低傳輸時期成本：**經實驗證明本研究之傳輸時期成本與 EOI 成本相同，同時透過網際網路傳遞，不再需要透過傳統 EDI VAN Center 的轉送，因此如圖七中，明顯低於傳統 EDI 之傳輸時期之成本。
2. **可靠的安全性：**本架構同時使用了 Secure HTTP 及 S/MIME 安全機制，避免了網際網路的安全顧慮，使得傳遞訊息的安全性變成可信賴的。
3. **高彈性的 XML/EDI 格式：**利用 XML/EDI 格式特性，可將相關產品資料透過網際網路傳遞給其他可以接受 XML/EDI 標準的企業，進而提供較有彈性之資料傳遞方案，同時也有助於其他 XML/EDI 解析搜尋引擎的搜尋，而增加一個附加價值。
4. **標準的規範：**藉由 RosettaNet 之 XML/EDI 文件規範與 DTD 規範，將可依產業配合語意的方式，使得傳遞之資料更具公開性及可讀性。
5. **加入供應鏈之機會：**經實驗結果三證明，本雛型之開發成本亦相當低廉，因此在低傳輸成本與低開發成本之下，將可增加小型企業加入供應鏈的機會。

三、問題與解決方案

本研究在實作雛型系統的過程中，曾經遭遇到一些問題，而這些問題可提供讀者做為參考。

(一)安全性之假設

由於本架構之安全性基礎建立在 S/MIE 以及 Secure HTTP 基礎上，倘若此安全性有疑慮，則安全問題便有問題。其次，本論文所建之雛型系統內所使用之安全方面元件，係採用微軟公司以及他人於網路上散發之公開元件，其安全元件內是否含有安全性漏洞或是木馬程式，亦同樣將引發擔憂。而此部分之顧慮，提供給讀者在採用之安全元件上之參考。此外，本雛型系統使用之加密元件受限於美國密碼出口法令限制，迫使本研究的雛型系統必須使用多組鍵值加密方式，以加強安全性問題，加解密過程較為繁複，且是否可以達到所預期之高度安全性，亦必須經過更嚴密的驗証。

(二)RosettaNet格式問題

由於 RosettaNet 組織目前仍不斷對其各個 PIP 流程與 XML 文件格式規範提出新版本修正，因此讀者將造成 XML 文件，在各個版本之間有所差異。建議讀者依據本架構設計系統時，必須加入新版本資訊，以克服 XML 文件版本問題。

此外，在 RosettaNet 制定之 XML 文件中，經常引用國別貨幣代碼欄位(GlobalCurrencyCode)，其欄位亦指明係依據 ISO 4217 於 1995 年訂定規範，但其中國別 3 碼並不足以表示所有國家，導致 XML 文件實際傳遞後，將遭遇到可能無法確實指出國家別問題，引發可能無法確認售價國家貨幣別、稅費國家貨幣別等問題。而此問題，在實作之雛型系統中並未特別加以檢驗，未來應進一步加入驗證的功能。

(三)資料庫格式設計問題

對整體的架構而言，資料庫存取層扮演了重要的角色，所有元件間的聯繫皆以資料庫為主，使得聯繫性資料庫之設計良窳，影響了系統的運作品質。在實作過程中，發現盡可能依據 RosettaNet 所訂定之 XML 文件格式設計之資料庫格式在應用時，可降低修改資料庫的機率。

伍．結論與建議

以目前而言，許多企業或是研究單位正利用 XML 為基礎進行建構資訊系統，而本雛型系統建置完成時，將可提供讀者以及企業作為建構類似訊息傳遞系統之參考。此外，就資料格式轉換而言，XML 資料格式確實可以取代傳統

的 EDI 格式，本研究中採取 RosettaNet 之 XML 格式規範，便可輕易完成資訊交換的目的。

本研究架構所建立訊息交換機制，應可迅速完成在不同企業建立資訊傳遞之連結機制。在安全傳遞機制方面，目前視為安全的方案，對未來而言，並不一定是安全的，目前常用的演算法，如 Diffie- Hellman 、RSA、triple DES 等演算法技術，只要鍵值長度足夠，對目前而言，安全上便無太大的顧慮，但就未來仍需不斷考慮是否有更適當的安全機制可供做為改善之參考。至於目前針對 XML 文件所發展的安全協定，如 XKMS 協定、S2ML 標準等是否更適合做為企業傳遞資訊的安全基礎，亦可成為未來後續研究方向的參考。

而就目前 RosettaNet 之 XML 文件規範而言，主要針對電子相關產業制定所需之規範，對於其他產業而言，是否有適當的 XML 文件標準提出可為參考或使用同一文件標準，則可留待讀者研究，再者目前 RosettaNet 之 XML 文件規範中係以 DTD 做為驗證基礎，未來是否改為以 XML Schema 為驗證基礎，則有待觀察。但單從資料格式轉換的技術而言，XML 整合 EDI 資料格式，即 XML/EDI，確實可以取代傳統的 EDI 格式，本研究中也確實採取了 XML/EDI 與過去傳統 EDI 格式的一對一轉換。以純粹 XML 技術而言，仍然在快速的演進與進步之中，目前仍有許多新的技術正被提出與並待被認同，例如 ebXML、SVG (Scalable Vector Graphics)、Xlink (XML Linking Language)、XR2 (XML Registry and Repository)、XQL (XML Query Language)、XSLT (Extensible Stylesheet Language Transformations)、XMTP (eXtensible Mail Transport Protocol)、SMIL (Synchronized Multimedia Integration Language) 等，而本研究中僅僅使用 XML 轉換技術與 DTD 驗證，便可輕易完成資訊交換的目的，但卻未驗證使用 XML 外之其他技術時，是否可更輕易完成資訊交換，而此部分將隨著 XML 技術的進展繼續研究，相信讀者亦可進行類似的研究。

參考文獻

中華民國商品條碼策進會，「商業加值網路應用專輯－技術應用篇」，經濟部商業司，1998 年。

中華民國電子資料交換標準委員會，「我國電子資料交換標準應用現況」，1999 年 5 月。

吳泰宏，「網際網路電子資料交換之研究與設計」，國立交通大學資訊管理研究所碩士論文，1999 年。

吳泰宏，蔡銘箴，「支援網際行銷的互動式網際網路電子資料交換技術之研究」，商業自動化研討會，1999 年，頁 277-299。

邱瑞科，「EDI 在流通業的應用與實務研討」，國際資訊管理學術研討會，1998 年。

邱瑞科，郁筱平，「建立安全電子資料交換機制的實務應用與研究」，2001 年科技與管理學術研討會，台北：國立台北科技大學管理學院工業工程系主辦，2001 年 10 月 15 日，頁 10。

許昌平，「在網際網路上應用 MINE 整合 EDI 與電子郵件機制之可行性分析與系統實作」，國立交通大學資訊管理研究所碩士論文，1999 年。

張真誠，賴溪松，韓亮，「近代密碼學及其應用」，第二版，松崗電腦圖書資料 (股)，1999 年 11 月。

陳昱仁，羅濟群，林川景，張文鐘，「開放式網路下之電子資訊交換安全架構」，*資訊管理學報*，第六卷第一期，1997 年 12 月，頁 85-107。

陳建豪，「網際網路安全電子郵件的設計與實作」，國立成功大學資訊工程研究所碩士論文，1997 年。

蔡銘箴，吳泰宏，「MIME 電子郵件系統的網際網路電子資料交換技術」，商業自動化研討會，1999 年，頁 129-136。

樊國楨，「電子商務高階安全防護」，資訊與電腦出版社，1997 年 10 月。

網際威信公司，「VERISIGN 數位憑證服務」，http://www.hitrust.com.tw/hitrustexe/frontend/default.asp

關貿易網路公司，「關貿網路電子資料交換服務費率」，http://www.tradevan.com.tw。

B.Kaliski, "Privacy Enhancement for Internet Electronic Mail:Part IV: Key Certification and Related Services", RFC1424, 1993.2.

B.Ramsdell, "S/MIME Version 3 Certificate Handling", RFC2632, 1999.6.

B.Ramsdell, "S/MIME Version 3 Message Specification", RFC2633, 1999.6.

D.Balenson, "Privacy Enhancement for Internet Electronic Mail:Part III: Algorithms, Modes, and Identifiers", RFC1423, 1993.2.

D.Crocker, "MIME Encapsulation of EDI Objects", RFC1767, 1995.3.

E.Rescorla, "Diffie-Hellman Key Agreement Method", RFC2631, 1999.6.

P.Zimmermann, "PGP User's Guide", Massachusetts Institute of Technology, 1994.5.

J. Linn, "Privacy Enhancement for Internet Electronic Mail:Part I: Message Encryption and Authentication Procedures", RFC1421, 1993.2.

Microsoft, "IIS Server - 產品資訊 - 資料機密性", http://www.microsoft.com/Taiwan/products/servers/iis/products-5.htm.

P.Hoffman, "Enhanced Security Services for S/MIME", RFC2634, 1999.6.

Rosettanet, "RosettaNet Overview", http://www.rosettanet.org.

R.Housley, "PKCS#7: Cryptographic Message Syntax",RFC2630, 1999.6.

Supply-Chain Council, "SCOR Overview", http://supply-chain.nidhog.com/default.htm

W3C, "Guide to the W3C XML Specification ("XMLspec") DTD, Version 2.1", http://www.w3.org/XML/1998/06/xmlspec-report.htm.

XML/EDI Group, "XML/EDI Group", http://www.xmledi-group.org/xmledigroup/xmledigroup.htm

S. Kent, "Privacy Enhancement for Internet Electronic Mail:Part II: Certificate-Based Key Management", RFC1422, 1993.2.

The Study of Applying XML/EDI Integrated Technologies to Build the Mechanism of Message Exchange and Information Sharing between Supply Chain Firms

RUEY-KEI CHIU, SHIA-PING YU*

ABSTRACT

As the approaching of global free trade, entering the Organization of World Trade (WTO) is one of the important policies of our government. It is highly possible that the competition among enterprises will become more challengeable after entering WTO in the near future. Therefore, the strategy of effectively making use of supply chain management and enhancing the exchange of electronic message will strengthen the competition advantages of an enterprise.

Owing to the more flexibility of XML data format with the capability of integrating modern secure data transferring technologies, the data transferring and exchange by using XML technology with secure data mechanism to implement the SCM system is recognized by a lot of researchers as the most feasible solution to achieve this goal. In this paper, we propose an effective solution to integrate the technologies of XML and traditional EDI with S/MIME secure mechanism to implement a secure data transmission prototyping system. With this approach, we can achieve the goal to transmit the data on the Internet under lower cost with high security.

A prototype of secure XML/EDI system which complies with S/MIEM version 3 for the supply chain management is implemented and presented. Thus, a new alternative of data transmission can be chosen for enterprises with their trading partners. The components of know-how used for implementation including buying, selling, and inventory system, XML/EDI data format conversion, and the use of secure system components will be discussed in this paper as well. The results and findings of this research incurred by the design of prototype is also discussed for the future reference to readers, later research, and enterprises to conduct similar research and implementation.

Keywords: electronic data exchange, S/MIME, XML/EDI, electronic business, supply chain system.

* Ruey-Kei CHIU, Associate Professor, Department of Information Management, Fu Jen Catholic University. Shia-Ping YU, Senior Software Engineer, Taipei Customs Office, Ministry of Finance, ROC.