南　華　大　學

資訊管理學系碩士論文

企業間電子商務認證交換平台發展程序

A Development Procedure of Commerce Identity

Exchange Platform for e-Business Electronic Commerce

研 究 生：林胤良

指導教授：吳光閔　博士

中　華　民　國　九　十　二　年　六　月

南　華　大　學

碩 士 學 位 論 文

資訊管理學系

企業間電子商務認證交換平台發展程序

A Development Procedure of Commerce Identity Exchange Platform for e-Business Electronic Commerce

研 究 生：林胤良

經考試合格特此證明

口試委員：阮金聲

李易訓

吳光閔

指導教授：吳光閔

所　　長：資訊管理學系主任 吳光閔

口試日期：中華民國 九十二　年　六　月 廿六 日

誌　　謝

兩年的碩士生涯，由生澀轉至成熟，然孤獨一路走來，秉著堅定的毅力，朝向目標前進終達成功。在此之際，回首過往，歷歷在目，心靈感觸自是筆墨難以形容，卻也有如獲獎般的喜悅與肯定！

這本論文的順利完成，首先要感謝的是指導教授吳光閔教授。從論文方向的選定、資料的收集、研究方法及架構的建立，這一路走來，吳光閔教授對學生論文寫作過程中的指導及要求，讓我逐漸培養出清晰的邏輯思考及敏銳的觀察；論文口試期間王昌斌教授、阮金聲教授不吝撥冗給予寶貴的意見，讓我的論文研究能更加周嚴與完整，在此致上學生由衷的感謝。

其次要感謝在南華的這兩年求學期間，同學全福、佳昌、玉玲、信旭及桐旗的幫忙與協助，在此特致最高謝忱！

最後要感謝我的家人，感謝父親的教誨及母親的悉心照料，你們的細心呵護，成就了現在的我。同時感謝妻子瑩瑩的無形關懷與翔云寶寶安靜的支持，凡此願與他們分享！

碩士研究生林胤良

叩謝

謹識於嘉義南華

企業間電子商務認證交換平台發展程序

學生：林 胤 良　　指導教授：吳 光 閔

南 華 大 學 資 訊 管 理 學 系 碩 士 班

摘　　要

台灣的經濟競爭力長久以來是建立在一個"快"的基礎上。然而，隨著市場環境的變遷，以及企業規模、型態的轉變，這樣的優勢早已受到質疑，而 Web Services 則帶來另一種全新的市場優勢。利用 Web Services 所建立的單一簽入與單一整合操作介面，運應於企業內或企業間，可以更輕鬆地利用電腦資訊做溝通整合。本研究即從電子商務資訊流互通問題切入，探討 Web Services 與 ebXML 兩大議題的處理，再結合 UML 的技術在商業流程上做應用驗證。未來企業間電子商務或是電子化服務〔E-Service〕若朝著標準與整合的趨勢發展，將可預期效率會更加提昇及更加強企業於網路的應用發展。

關鍵詞: 電子商務〔EC〕、網路服務〔Web Services〕

A Development Procedure of Commerce Identity Exchange Platform for e-Business Electronic Commerce

Student：Yin-Liang Lin　　Advisors：Dr. Guang-Ming Wu

Department of Information Management
The M.B.A. Program
Nan-Hua University

ABSTRACT

The competitiveness of Taiwan economy is based on the foundation with "quick-response" feature. However, complying with transition of the market nowadays and the transformation of enterprise scale and business model, this advantageous feature is calling in question. On the other hand, Web Services brings into a brave new advantage of market position. By using Web Services, building up the one-time login and unifying the user interface, it is easy to communicate and integrate the computer information within enterprise or inter-enterprise. This research is investigated into the problem of e-business data stream convergence, discussion the two big topics of Web Services and ebXML, and applied verification of UML technology in business procedures. In the future, if the e-business or e-service between the enterprises is developing in the trend of standardization and integration, we can expect the efficiency and highly development of the enterprise in the network effect.

Keywords: E-Commerce, Web Services, ebXML, SAML

目　錄

表　目　錄

圖　目　錄

第一章　緒論

第一節　研究背景與動機

現代企業電腦普及網路及軟體科技正以數十倍速的速度發展，給企業建置電子商務系統的願景，創造一個最佳的執行環境。正因為現在電腦使用環境及網際網路發展日趨成熟，以最新的軟體技術所建立的網路新通路，對傳統 Business 而言，是一個危機，亦是一個新商機，更是不得不積極因應的新 e-Business 戰場。網站經營的勝負，除內容的優寡外，新軟體科技的特徵、新的資訊技術標準、網路各社群間互動的深度及整個 e-Service 的效率更是網路競爭的決戰因素。

隨著資訊科技日新月異的發展與全球性的競爭愈演愈烈，傳統企業進入到電子商務已是迫在眉睫，而這一波的資訊電子革命正在改造全球企業與社會，面對快速變遷的經濟環境，昔日企業賴以發展的競爭優勢也隨著消失，故為了維持其競爭優勢，企業應盡速發展成為商務型的網站服務架構模式，本研究著重於企業電子商務發展及未來整合趨勢之研究, 使得企業能藉由 web-services 資訊發展技術, 架構一對企業間 ebXML〔Electronic Business using eXtensible Markup Language〕安全性整合的電子商務認證模式，進而應用資訊技術服務客戶與合作夥伴分享資訊與交易，實踐企業整合願景。

目前就資訊廠商的網站技術或架構發展多以ebXML 為基礎的網站服務 Web-Service 導向。本研究在此整合W3C 組織公佈的相關ebXML 安全規範標準，應用相關ebXML 安全技術作為網站認證服務環境之安全保護，並以UML 建立一個ebXML 為基礎跨企業的安全通訊架構，並依據相關XML 安全的標準規範，制訂商務流程的安全交易授權書，使用者只要向網站服務安全提供者取得安全授權書，就可以通透相關授權的合作認證進行網站商務交易，並可以延伸與其他網站提供者轉換安全授權書，連結到另一個網路聯盟進行交易。

自兩岸積極通商交流後，使得原本台灣的企業商務由 OEM、ODM 的 SCM 模式延伸到兩岸三地商務模式。目前兩岸三地的台、中資企業正積極的進行企業間商務整合，相對地在台灣經濟不景氣的情況下，許多產業深受影響而飽受衝擊，而未能商務化的企業更是受影響。故本研究主要目的為結合資訊技術與電子商務發展，研究提出一新的企業採詢的電子商務認證商務模式架構，其結果亦可供企業未來導入電子商務的參考。

第二節　研究目的

本研究在電子商務聯網趨勢發展前景看好的動機下，針對企業間電子商務認證架構進一步探討。在企業間電子商務活動中，企業多傾向借助資訊公司所提供之暨有套裝軟體— 稱之電子商務平台，進行資訊及交

換行為之處理。而針對商務型的網站認證部分卻未能有較進一步的討論，因此一套好的電子商務認證平台架構應能提供企業間資訊交流之認證交換機制。

在金流、物流及資訊流中，資訊流可視為電子商務活動中之基礎，也是最重要的一環，唯有企業間之資訊共享及傳遞行為順暢無阻，方可進一步進行正確商流層面的探討與企業間電子商務行為管理模式。因此，針對企業間或體系間的商務交易模式，安全與認證是最重要與最新的討論議題，一套好的電子商務認證平台需要提供的資訊安全有四個要項：

一、身分識別〔 Authentication 〕：檢驗並確定通訊的雙方之真正身份，以確認買賣雙方企業的身分正確性。

二、資料機密〔 Confidentiality 〕：確認資料傳輸的私密性，確保在通訊的過程之中，別人無法偷窺到資料的內容。

三、資料真確〔 Integrity 〕：確保在通訊的過程中，資料沒有被人動過手腳而產生破損的狀況。確認訂單付款資料在傳輸的傳程中不至於被修改。

四、不可否認〔 Non-Repudiation 〕：確認買賣雙方企業交易之正確及完整性，賣方確實收到從買方來的訂單，並且如期交貨，買方也收點貨品，依約付款。

針對專用於處理企業間認證之資訊課題工具，在本研究中將以“資

訊認證交換平台”稱之。目前市面上企業間認證交換平台多僅著眼於企業間之資訊格式交換或通訊協定，而未提供從流程的角度審視企業間的商務行為。因此，本研究之主要目的是基於相關的 ebXML 安全標準，以 UML 建立流程式的認證模式平台，提供一資訊認證交換之發展程序，供開發人員可依據不同之供應鏈體系特性〔集中式或聯邦式〕的架構，從流程塑模開發端，透過一連串分析、設計、執行、測試步驟，開發資訊交換認證平台之元件庫，以完成一適用於不同供應鏈體系之資訊認證交換平台。

第三節　研究範圍與限制

網際網路提供了企業新的型態與典範，在企業間頻繁的交易過程中 e-services 的成型與架設已是無庸置疑的需求，本研究僅針對企業 Web 的網路交易模式，探討如何相互認證達成 Single-Sign-On 網網相連，但就實體物流〔Physical Logistics〕及電子交易〔Payment Authority〕已有相關的資訊系統提供整合到企業的商務平台；如前一節所述，本研究目的在於針對企業間電子商務之認證流程進行探討，提出一適用於不同供應鏈體系之資訊認證交換平台發展程序，因此對於金流及物流的商業模式不予以討論。此外，對於電子商務環境中受矚目的電子商務安全課題，牽涉如加解密、數位簽章等課題，屬於另一門值得深入專門研究課題，亦不在本研究之範圍內；對於整個環境基礎工程的建置，包括法定規章、

行為規範、網路頻寬及其他系統公司的解決方案等電子商務相關課題，本研究也不加以探討。

第四節　研究架構

本研究依現行之 XML Web Services 資訊整合架構與趨勢，探討相關 ebXML 的資訊安全標準及 Web Services 的技術，再依微軟公司〔Microsoft〕及昇陽電腦公司〔Sun Microsystems〕所開發的電子商務認證平台資訊架構模型，配合電子商務的階段演進進程，進行 IT 資訊技術及相關技術發展整合探討，期望能協助企業有方向的導入電子商務認證技術，運用相關的企業及工業的 XML 標準，進而建置出符合企業需求的電子商務的認證服務入口網站，以達到企業間網站與網站的聯結單一登入作業。本研究之企業間電子商務交換認證平台研究架構整理如如圖 1 所示。

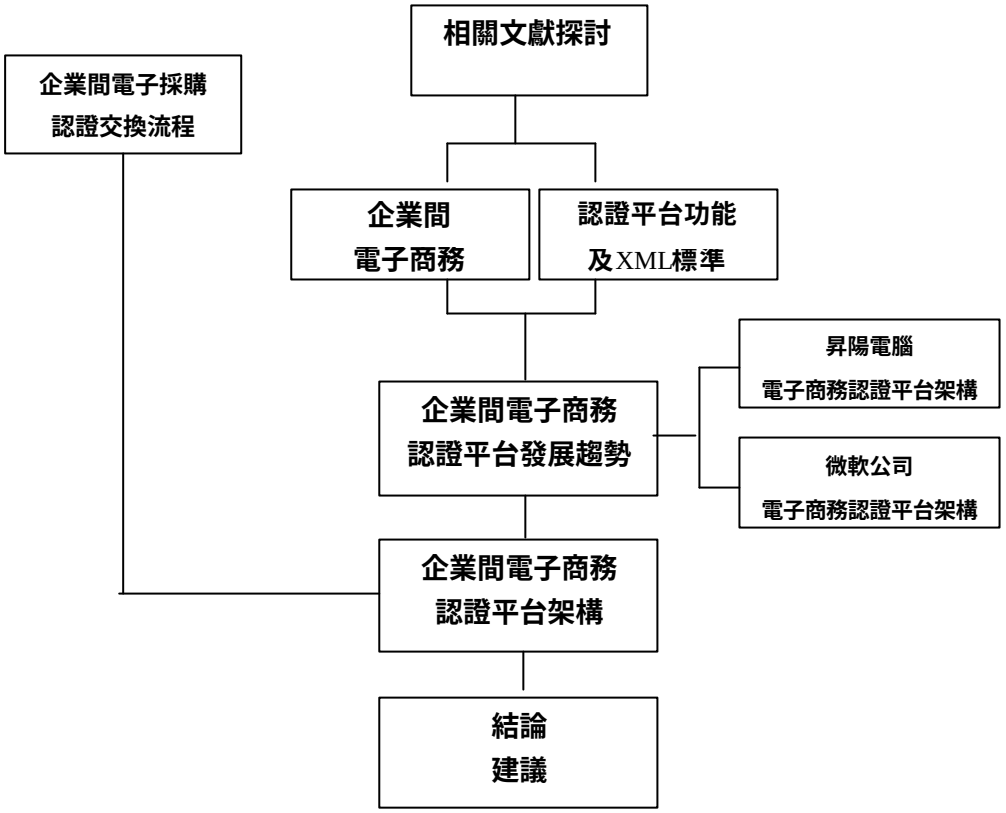


圖 1: **研究架構，﹝資料來源，本研究整理﹞**

本研究探討企業如何有系統地建置其企業的商務網站，在實際推行上，是需要哪些功能? **各個功能內所要做的步驟及屬性又是哪些**? **是否具有達到系統目的與效果的功用**? **並經由** UML **的塑模方式提供企業一個建置電子商務認證平台的架構基礎，並根據微軟公司﹝**Microsoft**﹞及昇陽電腦公司﹝**Sun Microsystems**﹞所開發的電子商務實踐模型，建構整合運用在個案企業中，其目的是藉由架構的探討，不斷地擴充與提升企業的商務網站的質與量，將它加以組織與整合，使電子商務網站成為企業中未來重要發展。企業間電子商務認證平台的功能是將企業相關的傳**

統架構與商業流程，經由與 IT 資訊技術整合後，透通企業間的商業交易，並產生新的附加價值，以提升整體企業間與體系間的服務與競爭力。

第二章　文獻回顧

第一節　電子商務與電子化企業

壹、電子商務定義與類型

電子商務狹義的定義為透過網際網路中的電腦網路來進行產品、服務、與資訊的交換以及購買、銷售過程的重要概念（Turban et al., 2000），其廣義的定義指企業運用資訊科技與網路連結溝通之功能，使企業的資源有更佳的利用、與顧客的互動更獲改善、使營運的流程更為順暢 以及使企業內與企業間的資訊交換更有效率（Kalakota & Whinston, 1997）。

根據美國政府資訊通訊基礎與應用任務小組（1994）所發表的電子商務與國家資訊架構（Electronic Commerce and NII）技術白皮書定義，電子商務係建立在電子資料交換應用所實施的線上資料與商務交易資料，內容包含有快速回應系統（quick response, QR）、效率顧客回應系統（efficient consumer response, ECR），為電子資料交換（electronic data interchange, EDI）及加值網路（value added network, VAN）的延伸。

企業往來的對象包括上游的供應商與下游的顧客，因此電子商務基本上可分為企業對企業與企業對顧客兩種類型（Cliton & Gore, 1997），但若以交易型態來分的話, 可分為下列四種類型(Turban et al., 2000) [14]：

一、企業對企業（business to business, B2B**）：企業直接在網路上與另一個企業進行交易活動，使整個「供應鏈」與「配銷鏈」自動化，包括組織間系統（**interorganizational systems, IOS**）交易作業以及組織間的電子市場交易作業。**

二、企業對顧客（business to customer, B2C**）：企業透過網站與顧客進行交易活動，如**Amazon.com**、** Dell.com**。**

三、顧客對顧客（customer to customer, C2C**）：顧客利用網路公司所提供的網站直接銷售產品給顧客，網站經營者僅提供系統機制，扮演「市場促進者」的角色，如**eBay**公司。**

四、顧客對企業（customer to business, C2B**）：顧客透過聚集社群，利用網站傳輸與生產供應或代理廠商溝通，提出產品議價或進行服務支援活動。**

五、非營利電子商務：如學校機構、非獲利組織、宗教性組織、學會組織以及政府代理機構等非營利機構以透過網路來降低其成本，包括改善採購或是改善作業與客戶的服務。

六、內部經營（組織）電子商務：在此類別中包括所有組織內部的活動，通常是在企業內網路進行。此種電子商務牽涉到產品、服務或資訊的交換，從銷售產品給員工到線上訓練與成本降低活動等。

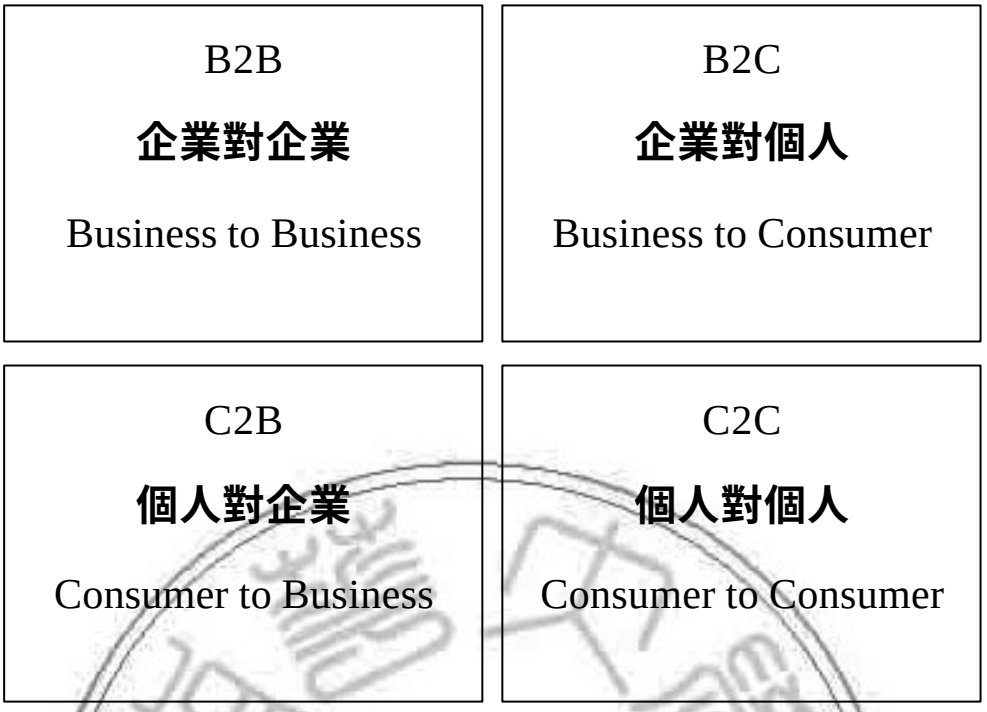


圖 2.交易型態的電子商務經營架構圖，（資料來源，本研究整理）

貳、聯結的電子商務的模式--*eB3c*

未來企業與企業間的商務需求與交易行為日趨複雜，不只是上節描述的二維度電子商務模式，進一步因為商業型態與交易模式複雜化，因此 BroadVision **公司提出** ebpc（employee、business、partner、consumer）**電子商務架構**[21]**，以下針對該模式調整為整合式的電子商務經營架構圖*eB3c*，以下就各個部份進一步說明分析。**

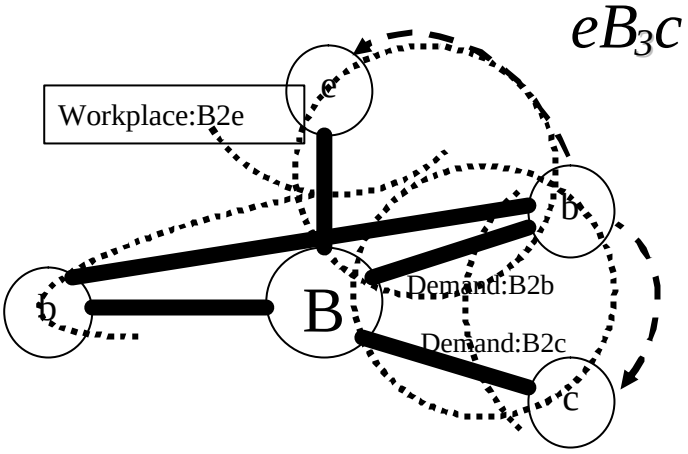


圖 3：聯結的電子商務經營架構圖，（資料來源，本研究整理）

一、B2b2c**：以企業** B **中心廠為核心，向外分為** B2b **及** B2c **的需求鏈（**Demand Chain **）的商務服務交易模式，進而發展成為** B2b2c **的整合交叉的商務服務模式。**

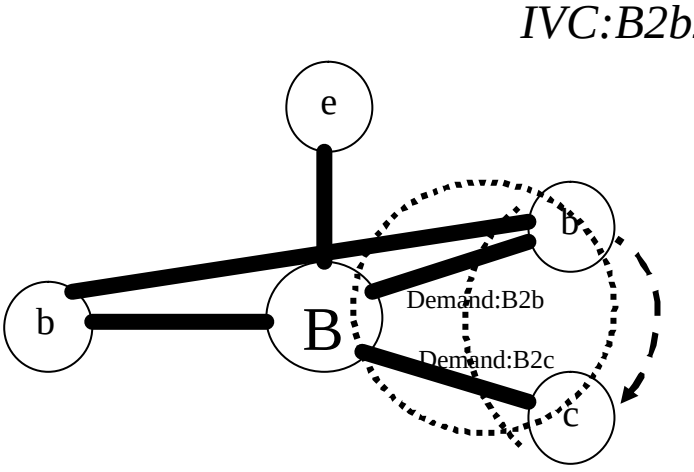
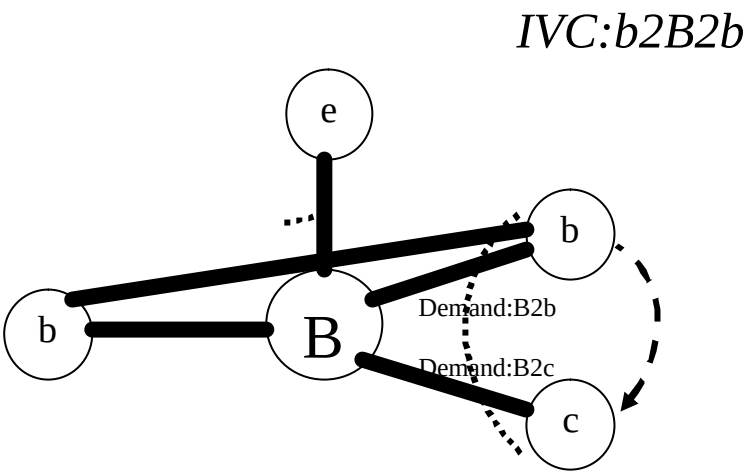


圖 4：聯結的 B2b2c **電子商務經營架構圖，（資料來源，本研究整理）**

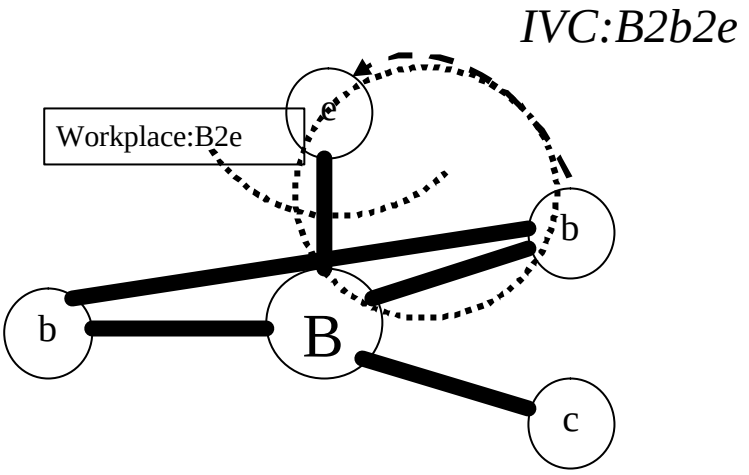
二、b2B2b**：以企業** B **中心廠為核心，往前為** B2b **的需求商務服務交易模式；往後則為** b2B **的供應商務服務交易模式，進而發展整合成為供應鍊** SCM **的** b2B2b **的商務服務交易模式。**



IVC—Integrated Value Chain

圖 5**：聯結的** b2B2b **電子商務經營架構圖，﹝資料來源，本研究整理﴾**

三、 B2b2e**：以企業** B **中心廠為核心，往前為** B2b **的需求商務服務交易模式，往上則為企業為員工﹝**Employee**ﴞ** KM **服務模式，進而發展成為企業與企業間並整合企業內部員工的資源模式。**



IVC—Integrated Value Chain

圖 6：聯結的 B2b2e **電子商務經營架構圖，（資料來源，本研究整理）**

因為企業與企業間的商業交易行為日趨複雜，而對客戶服務的優劣，決定了企業生存或淘汰的關鍵，故電子商務 e-business **的連結並整合為未來的趨勢走向。若再整合到政府機構，則商業的連結模式更為複雜，如** B2b2G2b …**等模式，若要解決彼此雙方的整合機制，則需要更進一步的信任及認證法則，國外目前就企業間電子商務的網站整合信任機制，已經有相關組織與認證交換標準提供給企業建置電子商務的依詢。**

第二節　我國政府產業的電子商務與認證機構

壹、政府推動產業電子化

政府有鑑於台灣資訊電子產業所憑藉著低成本、高品質的經營優勢，在開發中國家如中國大陸的急起直追情況下，我國資訊業的競爭優勢有被拉近的趨勢。近年來全球化之發展快速，產業國際分工成為一股銳不可擋的趨勢，而電子簽章技術、網路科技的日新月異，更形成了今日的產業全球運籌模式。我國的經濟部工業局，基於輔導國內電子產業，創造更強的國際競爭力，並參考美國電子流通業之樣式〔Business Model〕及探討國際供應鏈〔Global SCM〕整合架構，提出 A、B、C、D 與 E 計畫。

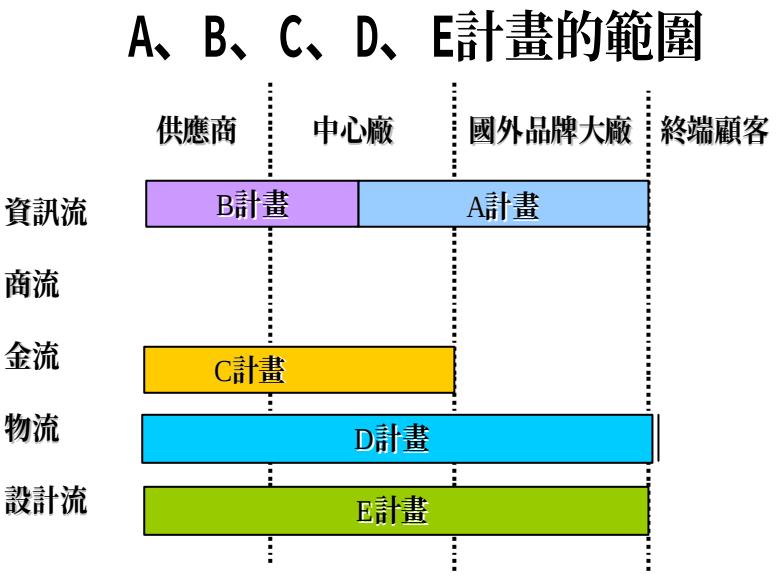


圖 7：A、B、C、D、E 計劃的範圍，〔資料來源，經濟部〕

其中 A 計劃是建立國外大廠與國內中心廠之間的資訊流之基礎建設，A 計劃是由 IBM、Compaq、HP 三家國際採購大廠與國內中心廠商四十二家建立含設計到採購階段之電子化供應鏈。這三個國際性電子化供應鏈體，使我國資訊大廠成為全球資訊電子產業供應鏈中重要的一環，並自純代工角色轉型為策略合作夥伴。B 計劃是建立國內中心廠與國內供應商之間資訊流的基礎建設。而 B 計劃主要是以國內電子產業十五個重要系統組裝大廠，與其下游如計將近 4000 家國內零組件供應商，建立含採購到製造電子化的供應鏈，並推動相關軟體系統廠商及資訊整合廠商業者共同投入。藉由運用網際網路與資訊技術，順利地讓資訊產業在 B2B 運作方案落實，並協助資訊相關產業建立創新經營模式的成功案例或典範，有效地提高企業營運效益及產業整體合作競爭優勢。也讓我國的資訊產業的系統業者成為國際供應鏈市場中，不可或缺的成員。

經濟部工業局為了延伸產業電子化之 A、B 計劃的執行成效，使台灣成為高附加價值運籌營運中心的角色，經濟部技術處又推動金流、物流及研發設計，協同作業電子化 C、D、E 計劃，使得三計劃在既有的電子供應鏈體系架構基礎上，可以進一步整合物流和金流，協助相關資訊電子產業優先解決與國際性的金流、物流及協同設計之需求，使得供應鏈體系的整體運作連貫一氣，實現「台灣接單、全球生產」的願景。

貳、我國PKI 環境架構分析

為加強產業電子化，提供企業間的電子化資訊交換與資金交易，建立國家一個安全及可信賴的認證機制及環境及提昇國家競爭力，政府主導規劃CA（Certificate Authority）認證機制[16]，用以建立我國完整之認證組織體系。其應用了金鑰基礎建設使重要交易資料加密，確保資料完整及正確性，且能鑑別交易雙方之身分，並防止事後否認已完成交易之事實，杜絕冒認及在發生爭端時提供相關佐證資料，以確保資訊在網路傳輸過程中不易遭到偽造、竄改或竊取，此乃電子化政府及電子商務能否全面普及之關鍵所在。

就公開金鑰基礎建設 PKI（Public Key Infrastructure）架構之運作方式，係先由使用者向 RA（Registration Authority，主要功能為確認使用者身份）申請公鑰及私鑰數位憑證，待認證機制 CA（主要功能為頒發數位憑證、列管憑證有效期限、將廢止憑證置入清冊）產生數位憑證，透過 RA 將數位憑證送達使用者，並將公鑰相關資料存於 CR（Certificate Repository，主要功能為儲存數位憑證及憑證清冊）供使用者查詢。

而我國公開金鑰基礎環境架構，在國家行政機構設置「PKI 推動小組」作為我國推動 PKI 政策指導單位，主要任務為研訂國家 PKI 政策、健全法制環境、推動研發 PKI 相關技術、引進與推動 PKI 標準、研究規劃 PKI-Based 經營模式、人才培訓與推廣應用等基礎建設工作。並且成

立政策審定單位 PAA〔 Policy Approval Authority 〕**，負責審核所有欲建立憑證機構之團體或組織所提報之憑證政策** CP〔 Certificate Policy 〕**及憑證實作準則** CPS〔 CP Standard 〕**，並定期的稽查已核准營運憑證機構是否確實執行所提報之憑證政策及憑證實作準則。就跨國內企業間或國際的認證機制，設置了橋接式憑證管理機構** BCA〔 Bridge CA 〕**，提供國內外憑證機構交互認證服務，用以解決不同體系間憑證機構之間憑證政策與技術互通的問題。在政府領域設置政府憑證總管理中心** GRCA〔 Government Root CA 〕**，提供簽發下層政府憑證管理中心憑證服務，建立相關安全機制及運作模式。**

第三節、認證機構趨勢之淺析

隨著網際網路普及與盛行，全球企業皆積極進行電子商務架設，努力將網路運用在企業營運中，以提昇效率、降低成本並拓展新商機。網際網路跨國界及無疆界的特性，亦讓素未謀面的人及公司只要連接到其企業電腦至網路系統上，隨即有交易的機會與管道，地理或區域因素不再成為國際貿易之主要限制。而就相關的認證趨勢上，認證機構的管理制度與認證機構管理是目前國內外積極在佈建與立法探討的。

壹、認證機構管理制度

在大多數承認公開金鑰基礎建設的國家立法例子中，認證機構採用證照管理制或自願認可制兩種方式。在歐洲國家立法例方面，義大利對於認證機構係採強制登記制。認證機構必須向義大利的資訊科技公共管理部門登記，並符合特定之技術標準；德國立法方面，在形式上法律雖然承認無證照的認證機構所發出的數位簽章法律效力，但實質上該法卻希望所有認證機構還是要經國家總認證機構（National Root CA）登記；反觀歐盟指令，則禁止強制登記制，並希望各會員國能在「客觀、透明、合理及不歧視」的前提上接受自願證照制。

在亞洲各國立法例方面，馬來西亞數位簽章法案，則以刑罰要求認證機構必須向認證機構的監督單位登記申請。新加坡的電子交易法中，雖對認證機構的管理未採強制證照之規定，但對認證機構卻多有規範；日本於其電子簽章與認證則採用自願認可制。

貳、認證機構管理之解決

對於認證機構的規範管理，就目前實際交易的運作與實施上，絕對有其利多於弊的充分性，但理論上並無列入電子簽章法的必要性。認證機構的規範應該與其他權益例如：針對消費者權益的保障併入討論中，而利用「空白立法」或「授權立法」等立法技術，將其納入電子簽章法的相關配套法令中。

電子商務及其相關法律之推動，宜強調應用的實際性及普遍性，並充分提供市場誘因以鼓勵科技技術發展。為了追求市場商務交易自由度，就相關的資訊技術與法律行政策略探討下，本研究認為：第一、不宜在電子簽章法中太過闡釋數位簽章及認證機構，以維持技術中立並有利於企業自由選擇不同的安全機制；第二、電子簽章法及其相關配套法令若要對於認證機構有所規範，建議採用自願許可制並納入國際間相互承認的趨勢；第三、就目前認證機構與交易企業間之責任歸屬，應該回歸該國現行法律規範。

第四節認證機構交互認證淺析

鑑於資訊系統安全的重要性，歐、美、日等先進國家已積極投入在商務安全技術上的研究，並廣泛地在推廣及使用中。PKI（公開金鑰基礎建設）是建構安全及互信交易關係的基礎架構，而建立一套整合性的 PKI 架構則是為解決不同系統間互通性問題；也是本研究的重點。

IDC 2000 年 12 月的一項研究分析顯示，全球 PKI 相關產品和數位認證服務的市場規模，將從 1999 年的 2.81 億美元，快速成長至 2004 年的 30 億美元。因此提供相關的安全線上交易環境，實為發展電子商務最迫切的資訊基礎。就電子商務安全多方運用來說，針對下列相關的安全議題提出討論議題如下：

壹、憑證機構間達互通性的考量

在評量達成跨領域互通性（Inter-Domain Interoperability）方法優劣時，依相關文獻探討[19]，本研究整理出三項考慮重點：

一、技術考量：實質上來說，技術考量包含從事互通所需的傳輸協定、資料結構和其他如執照核發及廢止相關資訊分享等範疇；技術也可說是三個考慮重點中最容易瞭解之處。

二、政策或商業應用關係：此部份是為了達成兩個 PKI 領域間互通認證的非技術性細節，建立企業與企業之間互通性關係的基本在於電子化資訊交換的需求與應用，而這些應用資源也就是用來處理不同領域間互通性，例如將國外發放的憑證套用在本土領域中。

三、法令考量：法律方面的考量恐怕為三要點中最難理解之處，而列於最重要互通性議題之一的，便是各國不同法令環境對數位簽章的接受度。

貳、憑證機構達互通性之方法

達到憑證機構間的互通性，特別是不同領域之互通性，有數個選擇性的方法，針對相關文獻的收集資料，本研究以下針對下列各個方法分別做簡單說明。

一、交互認證（Cross Certification）：交互認證為由一個憑證機構核發認證給另一個憑證機構之過程，並確保建立兩認證機構間信賴關係。相互的交互認證建立在兩個憑證機構間的互惠前提原則下，由雙方依照 X.509 標準互相發給一「交互憑證」並將此交互憑證儲存於管理名錄中。換句話說，這樣的過程是兩個不同 PKI 領域或同一 PKI 領域內的兩個憑證機構間單一或多重應用互通軌道的建立。前者為跨領域間的交互認證 ，而後者為領域內部交互認證 。

二、Bridge CA：Bridge CA 存在於一種特定信賴模式，也可以說是集中再分散模式。Bridge CA 扮演著憑證機構間傳遞者角色，免除憑證機構必須與每一個有往來的其他憑證機構建立雙方交互認證所進行的手續。從企業經營角度來看，Bridge CA 可減少企業間在建立這些認證信賴關係上所必須的開支。

三、憑證信賴清冊（Certificate Trust Lists）：其為一份簽署後包含「信任憑證機構」名單的資料結構；並藉由一大串憑證機構的隸屬公開金鑰憑證鑑定出合格信任憑證機構，同時也包括鑑定出信任憑證機構的政策依據。

四、鑑定憑證（Accreditation Certificate**）：該方法首度於去年** 2000 **年** 3 **月，澳洲政府主導之**“Gatekeeper”**專案所出版之論文中被提出；其基本原理是憑證機構由澳洲政府來鑑定 。**

Accreditation Certificate **方法與相互承認（**Cross -Recognition**）方法相同處為，兩方法皆不需要交互認證的保證（**the assurance of cross-certificates**）。由於鑑定評量標準由澳洲政府所訂定，未來亦非常有可能發生其他國家政府採用相類似方式的情況出現。**

五、絕對階層式（Strict Hierarchy**）：嚴謹層級制概念以由一共同** Root CA **授權發出所有**“**信任**”**為根基。在此一制度下，即使下層憑證機構存在，其所發出的憑證卻不受使用者所採用，除非該下層憑證機構的有效憑證之路徑可追溯至該** Root CA **中。**

六、委託路徑查詢與確認（Delegated Path Discovery and Validation**）：該方法目前正由美國** IETF **組織積極進行研發中，該方法可完全或部分擺脫憑證使用者在決定使用哪一家憑證機構是否可信賴的困擾。**

第三章　電子商務架構標準與功能

第一節、web-Services 與 ebXML 標準

根據全球電子商務專家預測，新一代的「可延伸性標示語言 XML」〔Extensible Markup Language，簡稱 XML〕，利用其所具有的可延伸性以及自我描述〔self-descriptive〕特性，從電子文件內容之收集、資料的處理解析、儲存、自動傳輸，乃至後端的資料搜尋比較、運算、再處理和呈現，幾乎完全可以由電腦代勞。相關 ebXML 已獲 IBM、Microsoft、Oracle、Sun Microsystems、Novell、Netscape、HP、SAP、Software AG 等國際知名資訊業者的支持。目前國際上業已有為數眾多的組織，積極建立和推動 XML-based 相關垂直產業和跨產業資訊流標準。ebXML 相關應用已成為全球資訊科學最重要的發展項目之一。

壹、Web-Services 技術與ebXML 標準

Web 服務這種新型的分散式物件運算方法，提供了很多技術上的優勢以及實用上的價值，讓企業級的應用程式在Internet 上發揮無所不在、無遠弗屆的特質。然而，要使得Web 服務能成為跨企業間電子商務應用的架構，最大的挑戰在於網路的安全問題。以目前在

Web服務上面大家所同意的標準，諸如XML、SOAP、UDDI和WSDL等等，對於在網際網路上的Web 服務並沒有嚴謹的安全考量，因此將這種分散式物件方法使用在防火牆之內的企業內部網路（Intranet）不會產生安全的問題；但是若要將Web 服務全面推廣到企業間的電子商務，使用在跨越防火牆的企業外部網路（Extranet），則在勢必要有良好的網路安全問題解決方案。

因此，網路安全問題是影響Web 服務成敗的重要關鍵；而Web 服務的安全性也是影響電子商務成敗最重要的問題之一。目前電子商務產業已經發出了安全的警訊，Web 服務之安全問題絕對是未來企業間電子商務產業是否能繼續前行之最重要的議題。

一、Web-Services 技術

Web Services 是一個具有開放性、分散式的軟體元件，基礎建立在HTTP、XML、SOAP、WSDL 等標準的協定上，使用者可利用任何的程式語言開發工具和作業系統來描述與撰寫Web Services 。Web Services 提供一個標準的遠端物件呼叫介面和應用程式寫作規格，程式設計師可運用他所熟悉的程式語言與網路上的其它Web Services 元件進行存取與呼叫。無論是電子企業內各單位的資訊溝通，或是與外部合作夥伴之間的異質系統或資訊交換，網站服務架構皆可提供一致性的資訊傳

輸與整合服務，企業運用網站服務來整合他們的商業流程。

最基本的Web Services 平台是XML 加HTTP ，HTTP 是一個在網際網路上行之多年且廣泛使用的通訊協議，XML 則是一種標籤語言，我們可以用它來撰寫特定的語言，以描述用戶端與服務之間的互動關係，而在Web Services 後端，XML 格式的訊息會被轉換成對中間元件的呼叫，而傳回的結果也會被轉換成XML 格式。但若是要建構一個完整的Web Services 平台，就必需再加上SOAP、WSDL 與UDDI ，以擴充其功能，同時保持簡單性和普遍性，針對XML、SOAP、WSDL 與UDDI 技術架構說明如下[23]：

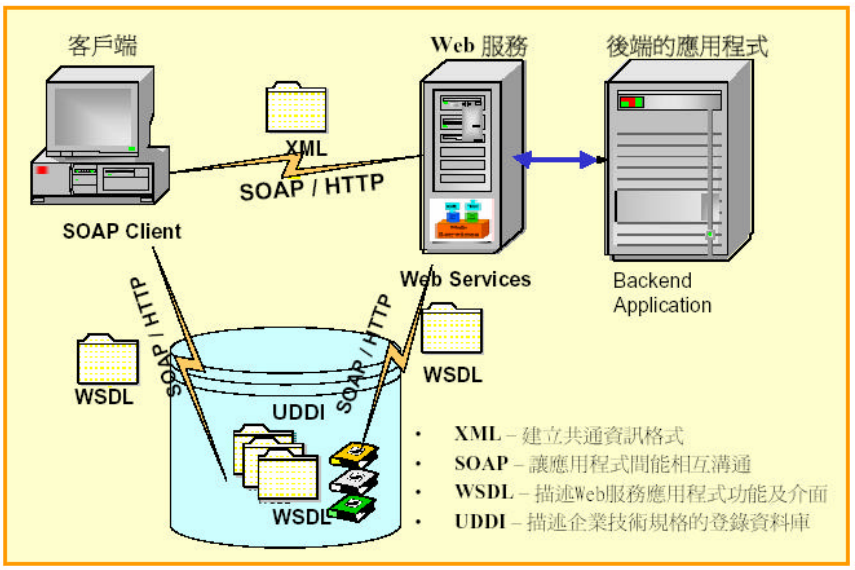


圖8：Web Services 技術架構，

〔資料來源，微軟電子商務研討會，2002〕

1. SOAP：SOAP 是一個協定規範，定義傳遞XML 資料的方法，也定義了使用HTTP 作為底層通訊協定時執行遠端呼叫（RPC）的方法。SOAP 是在2000年由IBM、Microsoft、 UserLand 和DevelopMentor 共同提交給W3C，SOAP 未來的發展規劃目前是由W3C 的XML 協議小組來負責制定，這也確定的SOAP 將會是一個業界通用的規範。SOAP 技術與任何程式設計模式無關，不論是使用微軟的COM/DCOM 物件或Java ，只要利用SOAP 技術，不同平台的程式設計模式都可以順利溝通。

2. UDDI (Universal Description, Discovery and Integration Service)：UDDI 是提供用戶端在網路上動態尋找其他Web Service 的機制，使用 UDDI 介面，商務處理可以動態的連接到外部合作者所提供的服務，其實我們也可以把它想像成商業應用程式上的 DNS 服務，而 UDDI 的註冊分為兩種：一種是要發佈服務的客戶，另一種則是想要取得特定服務的客戶。

3. WSDL：WSDL 是一種 Web 服務定義語言，WSDL 為服務提供者提供描述在不同協定或編碼方式上呼叫 Web Services 的方法，簡單的說，WSDL 就是用來描述一個 Web Services 能做什麼？位置在哪？如何呼叫？

貳、W3C 與OASIS 所制定的ebXML 相關安全標準

ebXML 是由聯合國貿易促進與電子商務中心(UN/CEFACT)與美國結構化資訊標準推動組織(OASIS)共同推動的一項電子商務架構標準。它提出一套完整的技術規範，訂定電子商務中各種功能標準，包括商業流程的建立、資訊的發掘、訊息的包裝與傳輸等，其目的是要使全球企業，無論其規模大小，都可以透過網際網路進行電子商務交易。

為了讓網路服務之間的互動與通訊可以做到認證性、資訊完整性、不可否認性與機密性，就需要有開放式的安全服務模式來支援，網站安全模式必須是獨立式的協定，如此網站服務才能夠將安全策略附加到網站服務定義上，讓客戶端可以安全地存取服務，網站服務安全所注重的是保護通訊安全與對互動雙方的身份驗證與授權。W3C[28] 組織與OASIS[25] 組織於近年來正陸續共同制定XML 安全相關的規範書與草案，一般總稱為「XML Security」，這個範疇包含了一般的資訊安全技術，如XMLEncryption[12]、XML Signature、XKMS 與SAML[26]，針對這些規範書說明如下：

一、XML Encryption（XML加密）：為了保留原本XML 結構化與彈性等特點，並做到XML 文件特定內容區塊的安全保護，

W3C 和Internet Engineering Task Force 〔 IETF 〕 還制定了一項標準來對一個XML 文檔中的資料和部分內容進行加密，這樣，如果一個文件檔只是某些敏感部分需要進行保護，你就可以他們單獨進行加密。對於同一個文件檔中的不同部分用不同的密鑰進行加密，你就可以把同一個XML 檔發給不同的接受者，而接受者只能看見和他相關的部分。

二、XML Signature〔 XML簽名 〕：也由W3C 組織及IETF 所制定，定義了將數位簽章的運算結果如何應用於XML 檔案上的標準， XML 簽名和XML 加密緊密相關。和安全認證簽名相似，XML 簽名也是用於確保XML 檔內容沒有被篡改的機會。為了適應各種檔系統和處理器在版式上的不同，XML 簽名採用了標準化 (canonicalization)。這就使得XML 簽名可以適應XML 檔可能遇到的各種環境；XML 簽名和XML 加密結合在一起，可以確保資料發送和接收的一致性。

三、XML Key Management Specification〔 XML加密管理規範 〕：

XKMS 密鑰管理規範書是由 VeriSign、 Microsoft、webMethods 合力制定送交給W3C 組織審核與公佈。它定

義了分發和註冊XML 簽名規範所使用的公共密鑰的方法。XKMS 包括了兩部分：XML 密鑰註冊服務規範（X-KRSS）和XML 密鑰資訊服務規範（X-KISS）。X-KRSS 是用於註冊公共密鑰的，而X-KISS 是用在XML 簽名提供的密鑰方面。

四、Security Assertion Markup Language〔安全聲明標記語言〕：SAML是OASIS 所發展來提供XML 架構下，提供商業交易的雙方透過Web services 交換經授權（authorization）及確認（authentication）的機制， SAML 採用了一項由OASIS 提出的"聲明計畫"。有三種聲明：認證，授權決定，和屬性。這三種聲明在一個應用中被用在不同的場合來決定誰是請求者，請求的內容，是否有權提出這項請求。SAML可以使得Web-based 的安全互通機制例如單一登入〔single sign on〕能跨站台供多個公司使用。SAML 運用了產業的標準協定及訊息架構，例如XML 簽章、XML 加密及SOAP 。SAML 可視為不同安全技術跨越Web services 的一項重要產業標準。SAML 允許各企業於線上交換認證和授權資料，公司之間就能進行不同的安全技術協同運作。SAML 允許用戶在不同的網站之間移動時攜帶授權和驗證證件。

這些標準和規範沒有一個已經被充分實現並廣泛採用了。W3C 和 OASIS 都在為XML 提供安全標準而努力工作著。隨著XML 的應用越來越廣泛，對於XML 安全性的需求也日益強烈。傳統的安全手段妨礙了 XML 的易用性，不過新的標準應該會很快出現並整合到相關的電子商務解決方案之中。

第二節、Microsoft 公司電子商務架構與認證

對於走進網路經濟世代的企業來說，如何善用新的網路服務來提昇企業競爭力，無疑的是未來企業生存爭戰中非常重要關鍵。而企業也都了解，要在網路經濟世代中占有領先地位，未來他們相對於資訊科技的仰賴就會更甚於過去。就電子商務的無論是針對資訊技術或者是資料交換格式上，遵循 XML 標準的 e-Service 架構已是企業所資訊應用的方向。在目前被視為是網路世代中最重要的二個競爭對手 Microsoft 與 Sun Microsystems ，他們各自為了因應網際網路應用及網路服務未來發展趨勢各推出的產品及技術 .NET 與 Java 。若是單單以 .NET 與 Java 來作比較是一較不理想的做法，因為它們並不是同等級的產品，在它們之下各自有不同的功能屬性。因此，我們將依據不同的功能屬性以相對應的產品來作分析，清楚地了解其各自的競爭態勢與優缺點。

壹、 Microsoft .NET 介紹

一、分散式運算

定義 .NET 的最佳途徑就是瞭解它的的功能。目前已有許多採分散式架構的應用程式，分散式應用程式的另一個例子就是立即訊息，您可以在網路上使用 Rich Client 與分散式朋友清單交談，並與其他 Rich Client （例如 Instant Messenger 及 Windows） 進行通訊。簡單地說， .NET 就是 Microsoft 為 XML Web 服務所提供的平台。XML Web 服務可讓多個應用程式透過 Internet 彼此通訊並共用資料，不論其使用的作業系統或程式語言為何。更明確地說，Microsoft 目前建構中的 .NET 平台分成五大範圍，包括：工具、伺服器、XML Web 服務、用戶端和 .NET 操作環境。

二、.NET 實現方法

Microsoft 認為，實現分散式計算最快的方法是藉由以下三大方法：

1. Web 服務：第一個方法是將 Web 服務普及化，包括軟體和網路上的相關資訊資源。

2. **歸納整合：第二個方法是準備好** Web **服務後，必須要能夠以非常簡易的方式將** Web **服務整合在一起。**

3. **簡單且吸引使用者的操作環境：推廣分散式運算的第三個方法，是您必須提供簡單且吸引消費者或一般使用者的操作環境。**

總而言之，以上這三個實踐方法是加速分散式運算發展的關鍵，Web **的服務普及化，能夠歸納整合** Web **服務及能提供簡單且吸引使用者的操作環境。**Microsoft .NET **的目的即是推動這三項方法，使分散式的** Web Services **計算更加應用普及。**

三、構成 .NET 的五大要項

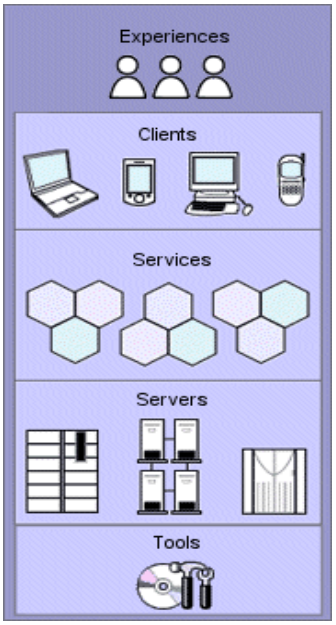


圖9：構成 .NET 的五大要項，〔資料來源，台灣微軟，2002〕

1. 開發人員工具：Microsoft 實踐的第一個要項是提供 .NET Framework 和 Visual Studio 工具組，將撰寫 Web 服務的工作儘量簡化，讓開發人員以最簡單的方式、最短的時間、最有效率的方式來撰寫最好的 Web 服務。

2. 伺服器：Microsoft 進行的第二要項訴求是歸納整合 Web 服務並推出 .NET 系列伺服器。這些伺服器分為兩種：第一種伺服器是眾所皆知，廣受歡

迎的 Windows Server、SQL Server、Exchange Server，這些伺服器都是以XML 為核心所建置而成。第二種是特殊的伺服器就是我們正在開發的伺服器，例如 BizTalk Server ，這類的伺服器可提供更高階、更具彈性的歸納整合能力。

3. 基礎服務：Microsoft 進行中的第三項要項訴求是簡單且吸引一般消費者的操作環境，我們以一組 .NET 建置區塊服務為實現方法。當我們上網時，經常需要登入多個網站和應用程式。為了因應這項需求，Microsoft 建置了一套能識別、告知並將儲存工作系統化的服務，讓消費者或使用者能輕鬆切換服務、應用程式，甚至切換環境都不成問題。.NET 建置組塊服務是構成 .NET 的第三要項。

4. 裝置：第四個要項訴求還是回到一般使用者操作環境。Microsoft 將重點放在透過我們正在建置的用戶端或裝置軟體，來開發極具吸引力的操作環境。全世界有許多系列裝置，如果能針對這些裝置提供更多的軟體，使用者就能享受功能更強的

系列裝置。例如用電話聯繫 PDA ，或連至平板電腦等其他裝置。

5. 使用者操作環境：最後一個要項就是提供引人入勝的使用者操作環境。Microsoft 設定具有特定訴求的使用者環境，整合了 Web 服務以及豐富功能，以提供特定訴求的操作環境。

以上前面四項歸納為所謂的 .NET 平台，而最後一項則是建置在平台上的應用程式。

貳、 Microsoft Passport 認證系統架構

微軟公司所提供的單一登錄機制，主要服務為「單一登入服務」允許用戶使用單一帳號和密碼登入Passport 的合作商務網站;其中並提供「電子錢包服務」讓用戶儲存信用卡及送貨地址以進行線上購物及付款的服務。所以使用Microsoft Passport 只需一組用戶帳號和密碼，登入任何Passport 合作商務網站之後，就可進行商務互通連結的服務。

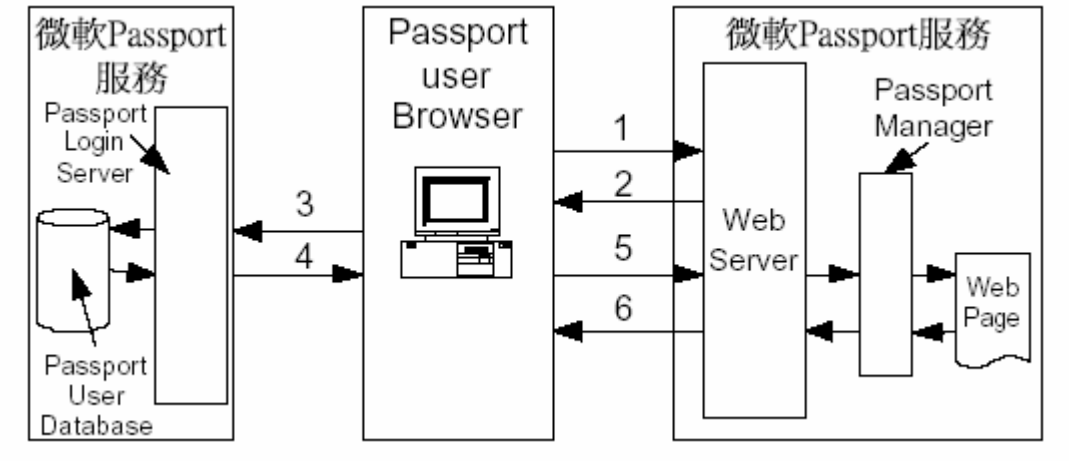


圖10：Microsoft Passport **的認證流程示意圖，**〔**資料來源，孫三才，**2001〕

Passport **的認證流程**[9]**如上圖：**

step 1. **消費者連結到相關的**Passport **合作商務網站要求服務。**

step 2. **合作商務網站導引連結使用者到微軟**Passport **網站進行登錄用戶資料。**

step 3. **消費者依據合作商務網站的指引到微軟**Passport **網站進行認證。**

step 4. **然後消費者取得微軟**Passport **網站的認證與授權。**

step 5. **消費者持有授權證明向合作網站提出或使用相關**Web **服務。**

step 6. **合作商務網站**Passport Manager **判讀授權內容後，檢驗通過就提供網站服務網頁給消費者進行服務與交易執行。**

第三節、Sun Microsystems 公司電子商務架構與認證

壹、Sun Microsystems 之 SUN ONE 介紹

為了滿足需要能隨時上線、且有要務在身的顧客需求，同時能提供超越簡易特定功能的隨選服務〔Services on Demand，SOD〕，新一代的網路服務必須發展更多可凌駕目前既有服務的新服務。SUN ONE 是一開放式的網路服務架構，同時也為將來可提供更多樣的隨選服務做準備。SUN ONE 讓企業現在就能夠建構、組合與部署隨選服務，同時可以因應未來的變化。

一、SUN ONE 架構的基本要素

Sun Microsystems 已制定一個開放式軟體架構，以支援可相互實行的隨選服務。SUN ONE〔Sun Microsystems OpenNet Environment〕架構則傳遞出一個重要的議題，如：隱私性、安全性、社群關係及主體性。同時，SUN ONE 也能支援可擴及多重網路的系統，包括傳統的網際網路、無線網路及家用網路。SUN ONE 架構的設計是用來確保所提供的隨選服務，不論是用任何工具開發或在任何平台上執行，同時能緊密的整合。SUN ONE 平台是經過特別設計，以支援現代企業的命脈 - 資訊，即所謂的 Data、Application、Reports、Transactions，〔DART〕。不論是用在電腦主機或是建置在網

際網路上， DART 包含的資訊來源，都可以滿足企業在 IT 方面的需求，就 DART 的說明如下[24]：

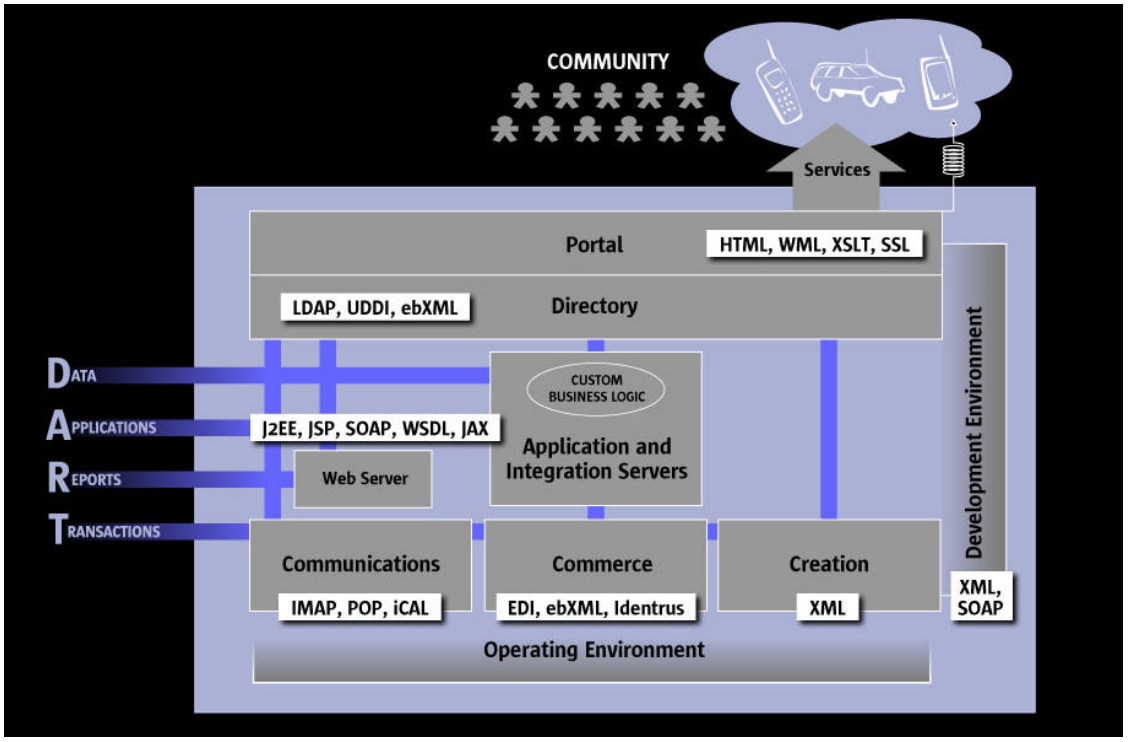


圖11：SUN的DART 架構，〔資料來源，Sun Microsystems，2002〕

1. Data〔數據資料〕：隨選服務架構必須能夠呈現並集合對企業往來社群〔括顧客、夥伴、供應商及員工等〕有意義的數據資料。這些個人化的內容是藉由入口網站傳遞。讓使用者可以獲取資訊的最主要關鍵機制是一個稱為「目錄」〔directory〕 的中控裝制。「目錄」儲存了所有使用者的資料，例如：他們的身份、他們擁有的權利為何，以及他們參與了企業的哪部份業務。

2. Application〔應用〕：在 DART 架構中，應用程式可以在 iPlanetTM Application Server 上執行。利用既有的資料庫及應用內容，使用者將可以透過 iPlanet Integration Server 取得在其過去使用環境中的資料並提供一個可延展的空間來執行以 Java 技術為基礎的任務。

3. Reports〔報表〕：對於企業而言，能追蹤使用者去向及評估本身提供的服務品質，是很重要的。SUN ONE 提供一個最快速的網路伺服器，供應企業有價值的報表，以因應不斷增加的網路需求。

4. Transactions〔業務往來〕：業務往來的範圍可確保企業社群能利用可獲取的資訊，進行有利的事情，例如：買賣、入帳、產品及服務的交易與屬於同一社群的人或其他外來的人進行溝通，或是可以更有效率地完成每天固定的工作內容。

SUN ONE 平台以能提供更具彈性、更符合成本效益的環境為目標，同時，DART 可在這個環境中發展、建置、彰顯及妥善運用。這個目標將可藉由使用開放標準、堅固的軟硬體元件而實現，也將創造大量整合性、可於企業中實行的，並可透過網路取得的服務。

貳、Sun Microsystem – 認證系統架構

Sun Microsystems 於2002 年公佈了網路認證解決方案（SUN ONE Platform for Network Identity），包含網路認證基礎的軟硬體與服務的規範標準。其主要目標有三個方面：

一、個人消費者和企業用戶能夠安全保管個人資訊，推展可相互運用並跨越多個網路的服務。

二、制訂實現單一登錄（Single Sign On）的開放標準。使用者在任何網站通過彼此認證後，不必接受其他網站認證就可以使用其Web 服務。

三、制訂所有接觸網際網路的設備都可以使用的網路認證開放標準。

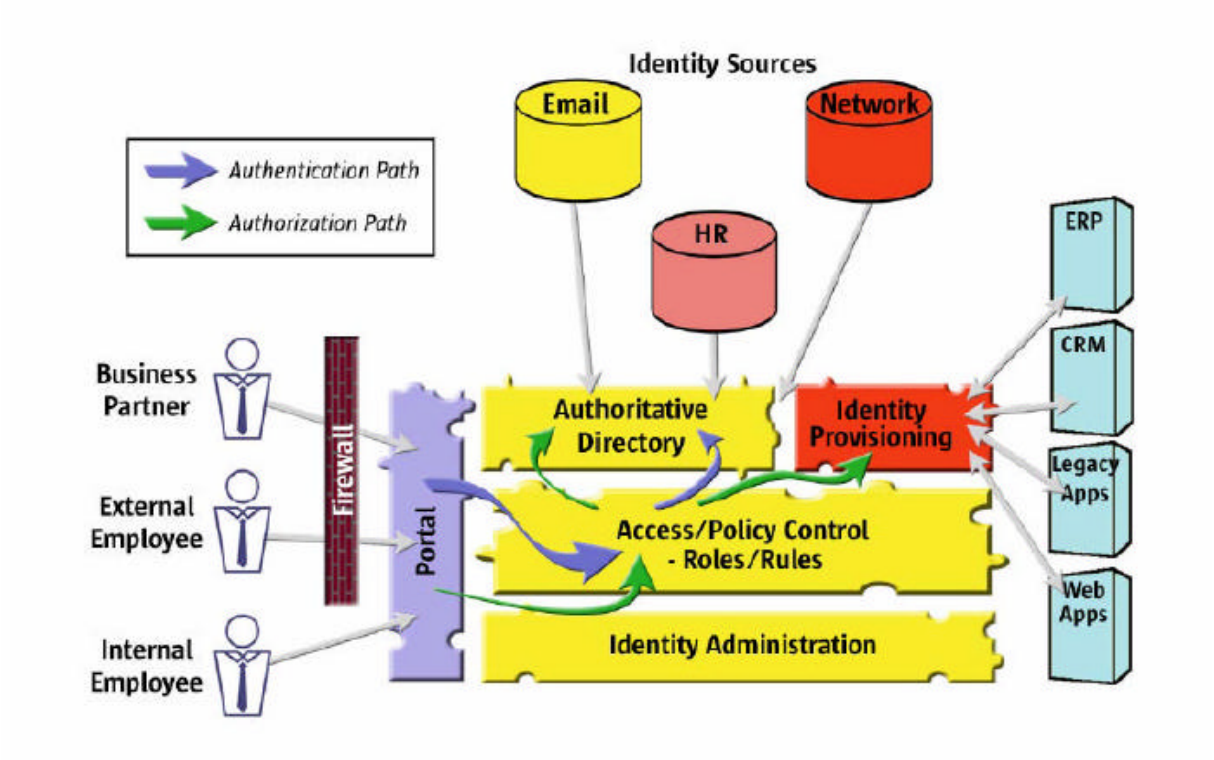


圖12：Network Identity**的作業流程示意圖，**

〔資料來源，Sun Microsystems，2002**〕**

網路識別〔Network Identity〕**的運作方式程序是, 當使用者要進行身份認證，應用程式或服務會依據相關規則或策略來審核使用者的識別帳號，給予適當的授權；授權處理**〔authorization process〕**依據識別編號**〔Identity Provisioning〕**給予使用者存取應用程式的權限，認證與授權兩個程序是**Network Identity **的核心部分，使用者界面是藉由請求應用程式**〔requested applications〕**或者入口服務**〔portal service〕**來處理，**Portal **架構提供兩個功能：**Portal **提供一致性的傳輸服務給企業使用，以及允許使用者依據企業間的信任關係與合作企業進行互動；與提供單一的帳**

號管理程序，另外，Portal 提供一般存取管道，如VPN 、安全與信任存取的網際網路環境。

第四節、建置XML 架構的Web Services 之比較

在本章節結束前，我們將深入的比較兩種可用來建置商業 XML Web Services 的平台，分別是 Sun Microsystems 所提供的 Java 2 Enterprise Edition（ J2EE ）以及 Microsoft 所提供的Microsoft .NET 平台。雖然J2EE 代表的是一個公開的標準，而 .NET 則是單 Microsoft 一家廠商的標準，反觀 Java 平台，確是所有除了 Microsoft 以外的各大廠商都遵循著 JCP 的標準制定所有規格。儘管在標準化上 Java 遙遙領先，但我們仍然將只針對伺服器端的 Web Services 架構做探討。

壹、工業標準與企業標準

透過 Web Services ，任何應用程式可以在網路上順利地整合在一起。 Web Services 的基本原理是利用標準的網路協定（例如：HTTP、SOAP ）來傳送 XML 訊息。這是一種非常輕便的溝通機制，因此可以讓任何程式語言、中間層元件或平台很輕易地整合進來。一般工業上或企業內部會接受成熟且廣為廠商採用的業界標準，有了 Web Services ，就可以快速且低成本的整合兩個企業、部門或甚至是兩個程式。要建置 Web Services 必須得採用業界通用的 Web Services 技術。而新一代的分散式服務，採用的是 XML 技術，但是目前最受歡迎的方式仍然是將 XML 植

於 HTTP 下較廣為接受，但是效能並非最佳的通訊協定上。面對這麼多的分散式技術，Microsoft 與 Sun Microsystems 產品對應與 J2EE 平台與 .NET 平台的支援程度如表 1、2 及 3。

表 1：Microsoft 與 SUN 的產品對應表

Microsoft	Sun Microsystems	描述
C#	Java	程式語言
CLI	Java bytecode	中介程式碼
CLR	Java runtime	語言平台及編譯
COM+	J2EE	企業及 Web 應用軟體平台
.NET	SUN ONE	Web 服務平台
Hailstrom	SUN ONE WebTop	終端使用者 Web 服務及入口網站

（資料來源，本研究整理）

表 2：Microsoft 與 SUN 就分散式技術的支援比較表

	J2EE	.NET
CORBA	支援	不支援
RMI/IIOP	支援	不支援
COM+	不支援	支援

（資料來源，本研究整理）

表 3：Microsoft 與 SUN 對新一代 Web Services 的支援比較表

	J2EE	.NET
XML-RPC	**支援**	**不支援**
SOAP	**支援**	**支援**

（資料來源，本研究整理）

從上述圖表之中我們可以得知，對於姿態保守的公司而言，J2EE 支援了較為廣泛應用於現有企業系統的分散式運算服務，而 .NET 平台仍然只支援延伸自 COM 與 DCOM 的 COM+ ，我們可以推斷 J2EE 提供的分散式服務比 .NET 的技術較為領先。此外，目前企業內部使用之大型主機所使用的皆為 CORBA 技術，J2EE 對舊有技術的支援當然是最佳的，因為 COM+ 只能在 Windows 平台上運行。

貳、使用 J2EE 以及 Microsoft .NET 來開發 Web Services

如果您想開發一個有用的網路服系統。所面臨的挑戰並非表面上所看如此簡單。您的 Web Services 必須可靠、普及、不容易出錯、有彈性而且必須讓大家願意接受。這些嚴格的要求並不亞於任何企業等級的商業應用程式。J2EE 以及 .NET 是現有用來開發伺服器端企業級應用程式的技術延伸。這些技術的早期版本並非專門用來開發 Web Services 用。如今 Web Services 已經成為趨勢。J2EE 以及 .NET 的共通願景就是希望能達成開發 Web Services 的基礎工程，例如：跨平台的 XML 溝通、負載平衡以及交易。

但是，當開發到一定規模的應用程式時，會產生一定的複雜度，這

個時候就必須有開發工具的輔助，如果您選用了這兩種其中一種平台，那麼您可以選用的工具如下表 4 所示:

表 4：開發新一代 Web Services 的開發工具表

平台	工具
J2EE	JBuilder (Borland) Forte for Java (Sun Microsystems) WebLogic Workshop (BEA) JDeveloper (Oracle) VisualAge for Java (IBM) Visual Café (WebGain)
.NET	只有 Visual Stdio.NET

（資料來源，本研究整理）

從上述整理的表教表中可以看出，就系統設計人員可以根據不同的需求來做最佳的選擇, 而不是只尋求單一廠商所提供的工具和解決方案。

參、J2EE 與 .NET 的比較

為了解這兩個平台所提供的架構模型，我們提供一個關於 J2EE 與 .NET 技術相同點的列表，參考如下表 5。

表 5：J2EE 及.NET 分析比較表

特徵	J2EE	.NET
技術型態	**標準**	**產品**
支持的廠商	**三十家以上**	**微軟一家**
翻譯程式	JRE	CLR
動態網頁	JSP	ASP.NET
中介物件	EJB	.NET Managed Components
資料存取	JDBC、SQL/J	ADO.NET
SOAP, UDDI ,WSDL	YES	YES
負載平衡	YES	YES

〔資料來源，本研究整理〕

Sun Microsystems J2EE **與** Microsoft .NET **兩者都提供一些執行機制，讓軟體開發人員可以避免觸碰到一些底層複雜的部分。除了在平台、程式語言以及企業架構上支援** XML Web Services **的中間層外，**Sun Microsystems J2EE **以及** .NET **還分別透過** Java Runtime Environment **〔**JRE**〕與** Common Language Runtime **〔**CLR**〕提供基礎層面的服務。**

最後，就本研究整理後 J2EE **與** .NET **所提供的這兩種程式的開發環境是完全不同的。**.NET **號稱有強大的程式開發工具** Visual Studio .NET **，**Java **也有各家廠商〔**Borland、Sun Microsystems、BEA、IBM **等〕的整合式開發工具可供選擇使用；在學習難度和系統設計及開發過程上面，** .NET **也是完全採用** Java **自始就採行的物件導向分析設計**

技術，而且到系統架構設計上，OOAD、UML、Design Patterns **等方法也是雙方都採行的標準步驟。**

第四章、B2B 認證平台發展程序

第一節、物件導向軟體發展程序

統一塑模語言（Unified Modeling Language, UML）是Rational 公司整合Grady Booch 的Booch 方法、James Rumbaugh 的物件塑模技術（Object Modeling Technique, OMT）、Ivar Jacobson 的物件導向軟體工程（Object-Oriented Software Engineering, OOSE）三種方法和其它的物件導向方法論，而提出物件導向系統的塑模語言。其實，只要仔細的環顧四週所用的開發工具，你會發現明顯的事實，原來我使用的開發工具都和物件技術多多少少有些關係。諸如VB、C++、Delphi、PowerBuilder，以及現今最熱門的電子商務開發語言Java ，都是物件導向語言。

壹、UML發展沿革概述

在1994 年之前，市面上存在著各種物件導向的分析設計方法，譬如在大型軟體專案受到青睞的Booch Method ，在企業資訊系統佔有相當比例的OMT ，以使用案例（use case）著名的OOSE 等，想要踏入物件工程的人往往必需在眾多的方法論中擇一而終。Rational Software 結合物件領域知名大師及其他資訊大廠的努力，終於讓UML 成為軟體界家喻戶曉

的物件技術。目前，最新的UML 為1.3 版，在2002 五月份剛剛推出，OMG預計在明年4 月推出較大幅度修正及納入其他新軟體科技（譬如XML 相容格式）的2.0 版。瞭解了UML 的沿革，我們回頭來看到底有那些UML 重要的本質與觀念，是在應用UML 前必需清楚的。

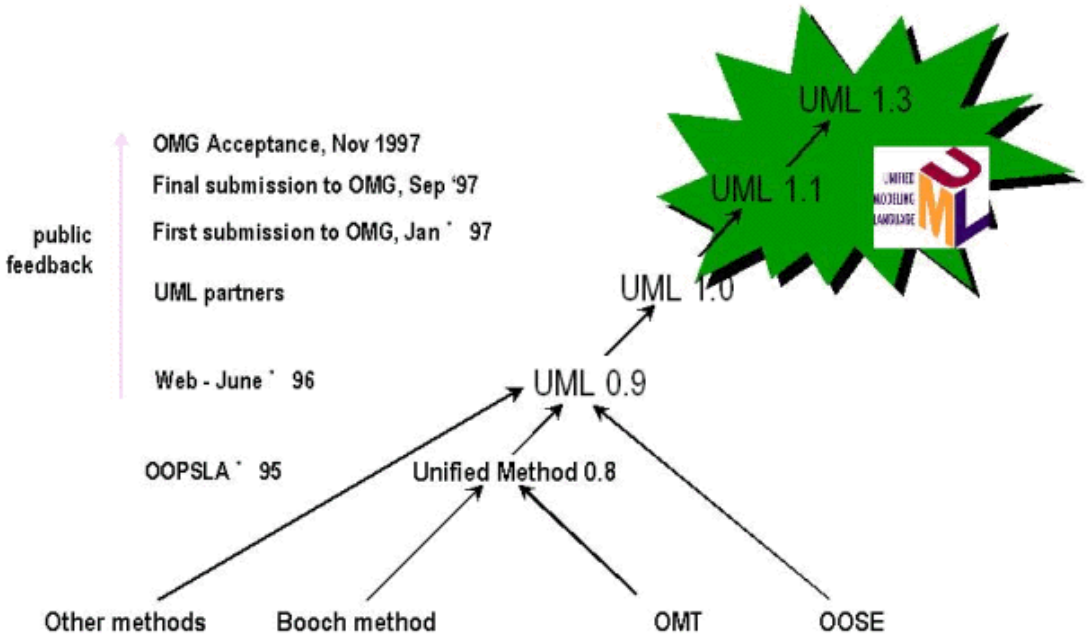


圖13：UML的發展沿革，〔資料來源，OMG，1999〕

貳、UML 是符號的標準，不是方法論的標準

前面談到物件導向軟體開發在早期有許多的方法論，但是UML 並不是物件技術的方法論。UML 是有定義了豐富的塑模（modeling）符號，讓你表達從業務流程分析、業務需求、物件塑模到物件設計的各種結果。 軟體的開發有著各式各樣可能的方法，每個人對自己專精的領域都有獨到的見解，物件導向的軟體開發也不例外。OMG 為了避免爭議，難

以達到共識，而能順利推行物件技術標準，UML 並不範規軟體專案應該怎麼使用UML 標準。然而Grady Booch 等三位專家，在累積多年的物件開發經驗後，其實對什麼是適當的物件導向開發流程，是有些特定的想法，這些想法也充分反應在UML 相關標準上。因此，接下來讓我們來看看什麼是UML 的塑模圖形與軟體架構觀點〔VIEW〕。

一、UML 的圖形

UML 定義了九種型態的圖形：使用個案圖（Use Case Diagram）、類別圖（Class Diagram）、物件圖（Object Diagram）、循序圖（Sequence Diagram）、合作圖（Collaboration Diagram）、活動圖（Activity Diagram）、狀態圖（Statechart Diagram）、元件圖（Component Diagram）和部署圖（Deployment Diagram）。所有圖形的基本原則，就是將概念描繪成符號，並將概念之間的相互關係描繪為連接符號的路徑，這兩種型態的元素都可以擁有自己的名稱。以下表6是UML 九種圖形的用途描述：

表6：UML的九種圖形說明

圖形名稱	圖形說明
使用個案圖	是引用Jacobson 的使用個案模式，從使用者之觀點描述系統的行為者與系統間之互動行為與關係。從外部觀點來看，使用個案可描述系統做什麼？從內部觀點來看，它可描述行為者與系統如何互動？

類別圖	是引用Booch 與Rumbaugh 方法論的類別圖，主要用以表示系統存在之物件型態（或稱類別）及各物件型態間的靜態資料結構與邏輯關係，也表達類別之屬性、操作與類別間連結之限制等。
物件圖	是用予描述一系統於某一時間點的靜態資料結構，該圖由一群相關之物件及其連結所組成，以表示系統在某一時間點之一個例子。
循序圖	是結合Booch 的互動圖與Rumbaugh 的訊息追蹤圖而成，主要用以描述系統運作時，物件間的互動行為且著重以時間之先後順序為主軸以表達物件間的訊息傳遞與處理程序。一個循序圖會有一個與之對應的合作圖，但表達的重點與方式不同。
合作圖	是從Booch 的物件互動圖與Rumbaugh 的物件導向資料流程圖改進而來，該圖主要表達相關物件間之連結結構，並能同時展現物件間的資料流程、控制流程與訊息傳遞的活動。因此，合作圖是一個巨觀的總流程，能同步表達資料的產生與資料轉變的過程，以改進傳統資料流程圖中只著重資料流的缺點。
狀態圖	是結合Booch 的狀態轉移圖與Rumbaugh 的動態模式而成，用以表達物件在其生命週期中的狀態變化。狀態圖是以微觀物件為主，細分物件所發生的各項事件，並表達物件生命週期之狀態轉變及活動結果。
活動圖	是狀態圖的一種變異，該圖表達涉及於執行某一作業行為中之活動。一個活動圖描述一群循序與同步的活動，一個活動狀態表示一個工作流程步驟或一個運算的執行活動。
元件圖	起源於Booch 的模組圖，用以說明系統設計過程各類別與物件的配置及敘述軟體元件間的組織架構和相依關係。元件是開發和執行過程之實際物件類別，將可拆散的實際基本單位模組化，這些基本單位包括模型元素並擁有特性和明確定義的介面。
部署圖	起源於Booch 的處理圖，它用來說明系統各處理器、處理元件的配置、關聯，以及同一處理器內執行處理的時程安排等。

〔資料來源，吳仁和，林信惠，2002〕

二、UML 塑模軟體系統的五個連鎖觀點

UML 發源地 Rational Software 所提倡的軟體架構：

“4+1”觀點（view）。而此架構被 Kruchten（1995）稱為 "4+1觀點"（4+1 View），就是要凸顯使用個案扮演的角色。一個

系統發展過程中的生命週期可透過這五個不同觀點之結合能有效溝通與整合不同角色人員對系統設計之看法而獲得一致的發展目標。另由 Booch 等人（1999）[10]對五個連鎖觀點描述中所使用到 UML 圖示與對象整理如下：

1. 使用個案觀點（Use Case View）：以使用案例模式充分表達軟體功能需求，並不實際描述軟體系統的組織。

2. 設計觀點（Design View）：由類別、介面與合作組成，這些是來自於描述問題及其解決方法中之辭彙描述。這個觀點主要支援系統的功能需求，表達系統應提供給使用者之服務。

3. 流程觀點（Process View）：一個典型的分散式系統，必然含有許多的工作元或執行緒（Thread）。你所設計的物件是存在那些工作元或執行緒？ 這些工作元或執行緒之間如何溝通？ 如何交換訊息？ 尤其是在網路世界裏的軟體，工作元觀點顯得特別重要。

4. 實施觀點（Implementation View）：以模組或元件的表示邏輯設計的物件是在那一個模組或元件中實作，並且以元件圖表示出它們之間的依存性。由可以不同方式組裝實際

可運作系統之獨立的元件與檔案所組成，這個觀點主要表達系統版本的結構配置管理。

5. 部署觀點（Deployment View）：在網路環境中，運用佈署圖充分表示工作元或執行緒對應到主機或裝置的實際狀況。由構成系統之硬體類型的節點（Nodes）所組成，這個觀點主要表達組成實際系統之零件的分配、傳遞訊息與安裝。

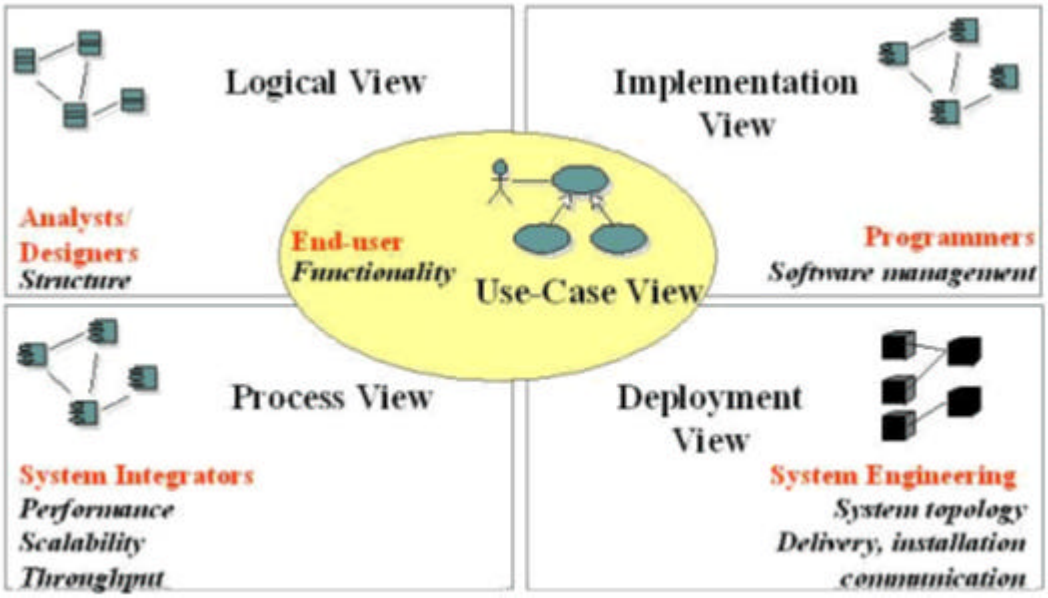


圖14：“4+1”觀點之軟體架構圖，〔資料來源，Booch等人，1999〕

嚴格地說，“4+1”觀點是間接促使UML 定義那麼多圖示的原因。健全的軟體架構在元件式開發及網際網路時代顯得特別的重要，在國外，軟體架構已成為軟體工程熱門的研究之一。就相關UML 技術，本研究提出一個企業間認證交換平台的雛型，提供企業於建置電子商務Web

Services 的網站時的認證依循，並依相關的XML 標準，建置一個符合企業間合作的認證交換平台，並於下一個章節中加以討論。

第二節、企業間認證平台發展程序

本研究在上一章中討論到Microsoft 及Sun Microsystems 應用ebXML 安全技術所設計出來的Web Services 的認證平台相關的資訊技術與架構。藉由相關的ebXML 標準及規格書及Web Services 的資訊技術，我們藉由UML 塑模方式，設計一個以ebXML 為標準的電子商務認證交易平台，我們稱此架構為XML Identity Exchange Framework〔XML IEF〕；這是一個以聯盟網站互通聯結環境為基礎的架構模型，進而達到單一登入〔Single Sign On〕的目的。主要的角色有使用者〔Users〕、網站服務認證提供者〔Web Service Identity Exchange Provider，WSIEP〕、商務網站服務提供者〔Web Service Provider，WSP〕。電子商務網站服務認證提供者〔WSIEP〕的程序是當使用者通過登錄使用者資料，取得帳號身份認證之後，給予他一份XML 格式的授權證明書，讓使用者持有證明書去與其他合作的商務網站進行服務交易；接下來網站服務提供者〔WSP〕會檢驗使用者持有的授權證明書，並提供其網站服務內容給該使用者，使用者〔Users〕就不需要於每個網站之間都要進行登錄認證，就可以使用互聯各家商務網站的

服務項目，使用者與該網站的交易內容就記載於使用者所帶來XML 格式安全授權書內的特定標籤位置中。

壹、使用案例

使用案例之目的在於幫助開發人員對系統做適當的切割，以達到建化系統設計之目的。使用案例之切割原則，在於找出相關之行為者及使用案例，使之成為一獨立之小系統，進行功能及規格之設計與實現。就企業間認證交換平台的使用案例圖如圖15所示：

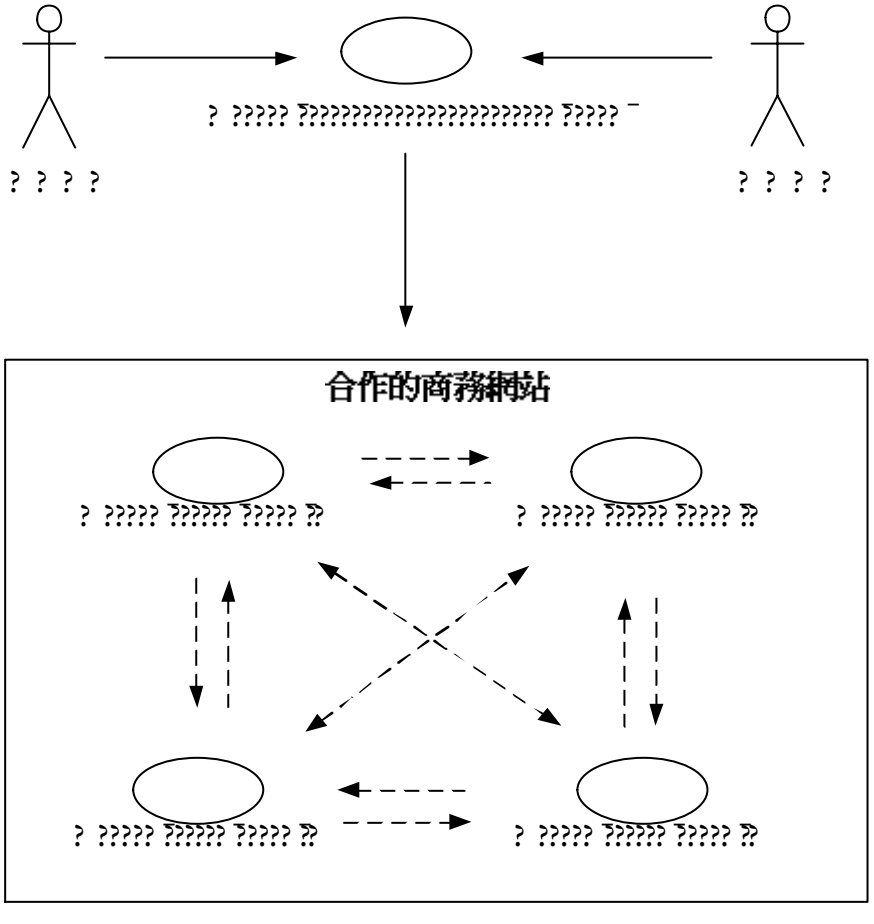


圖15：企業間認證交換平台的使用案例圖，[資料來源：本研究]

就企業間認證交換平台的使用案例圖的相關行為者、使用案例目標及流程說明，如表7說明如下：

表7：XML IEF使用案例圖表

使用案例名稱	認證交換平台架構
相關行為者	UserA、B，WSIEP，WSPA、B、C、D
使用案例目標	使用者A、B可經由WSIEP取得認證憑證互通於合作的商務網站WSPA、B、C、D間。
流程說明	1. 使用者A、B在WSIEP中登錄相關使用者的資訊。 2. 經由WSIEP認證許可後，取得相關帳號憑證。 3. 該核發之帳號憑證為合作之WSP互相認可之憑證。 4. 藉由該憑證，使用者A、B就可在合作的商務網站間取得所有WSP所提供之商務服務。

〔資料來源，本研究〕

本認證平台架構〔XML IEF〕的設計目標如下：

一、提供Web Services 認證的通訊模型，建置一個安全的認證網站服務互通架構，讓合作的網站服務〔WSP〕之間可以無障礙又安全地進行溝通。

二、提高企業間網站服務以XML 為基礎訊息之互通性，降低企業導入電子商務之阻礙和企業間資訊交換系統之間的建置成本。

三、為使用者與企業間電子商務服務環境提供一致性的認證架構基礎，此架構是與商業交易內容無關的，商業交易內容可由依企業服務內容需求不同而設立。

四、藉由ebXML 安全標準與Web Services 的資訊技術，提供企業間建立一個開放式的整合認證合作平台。

五、詳細地說明ebXML 安全技術之間的整合互動，以呈現出XML 安全技術的標準程序做法與功能性，讓ebXML 安全技術更容易為大眾所瞭解與應用。

貳、循序圖

循序圖可表示各項類別之間動態關係，供作進行系統開發及程式撰寫之參考準則。在繪製循序圖時，首先須先確定相關之引用類別有哪些。在本研究之定義中，一個完整之資訊認證交換平台是由數個以上資訊元件所組成，各個元件有各自不同獨立存在目的與訊息處理行為，因此在定義系統規格時，也需要將各元件分開加以考慮其中之資訊互動與通訊行為模式。在表達的過程中，除了根據使用案例的架構說明外，尚須根據電子商務所存在之網際網路環境加以考量其他必要的條件因素。就XML IEF使用案例延伸的循序圖，如圖16所示：

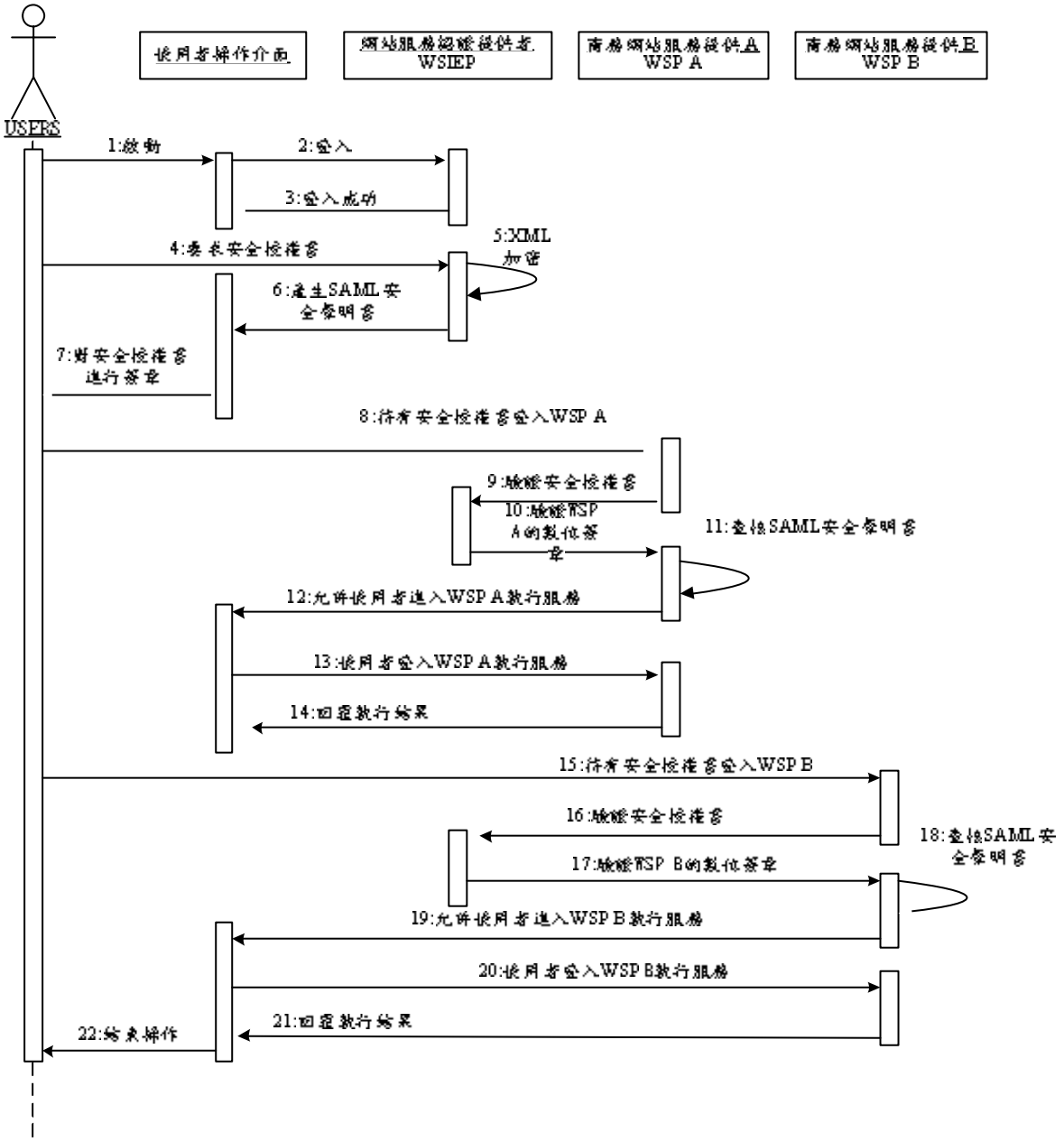


圖16：XML IEF**循序圖，〔資料來源，本研究〕**

使用者登錄到網站服務認證提供者〔WSIEP〕**，為特定交易商務服務要求產生所需的安全授權書。主要應用是**ebXML **安全技術：**XML Encryption、XML Signature、SAML。**而數位簽章驗驗證所用的密鑰都是交由公正第三者依據**XKMS **規範建立**XKMS**伺服器來代為管理。當服務**

提供者﹝WSP﹞接收到使用者所持有的安全授權書，服務提供者對使用者所持有的安全授權書進行驗證程序，這些驗證功能模組是歸屬於服務提供者的ebXML 安全檢驗服務範圍。就XML IEF 的流程依循序圖表示如下步驟：

Step1. 使用者向WSIEP 送出登錄身份的請求，WSIEP 的網站服務處理驗證成功之後，WSIEP 會呈現交易服務列表給使用者，使用者選取交易服務並且產生基本交易資訊，結合使用者相關交易資訊封裝成XML 格式的安全授權書。

Step2. WSIEP 使用ebXML 安全服務為該安全授權書進行加密與簽章保護，先使用XML 加密對證書檢查碼進行加密，並且為該使用者交易需求產生一份符合SAML 規範的認證與授權聲明，並針對該份安全授權書進行簽章。

Step3. 使用者點選WSIEP 網站上所提供的服務提供者WSP A 的超連結，然後傳送證明書的識別ID 通知該WSP 的XML 安全檢驗服務，進行驗證後並通知WSIEP 傳輸證明書，並將使用者導引到WSP A 的網站上進行執行服務。

Step4. WSP 網站上的ebXML 安全檢驗服務會先檢驗證書中的WSIEP 的數位簽章與傳輸此證明書的網站簽章，若兩者簽章正確無誤， SAML 驗證通過後，就將WSP 的網站服務提供給使用者。

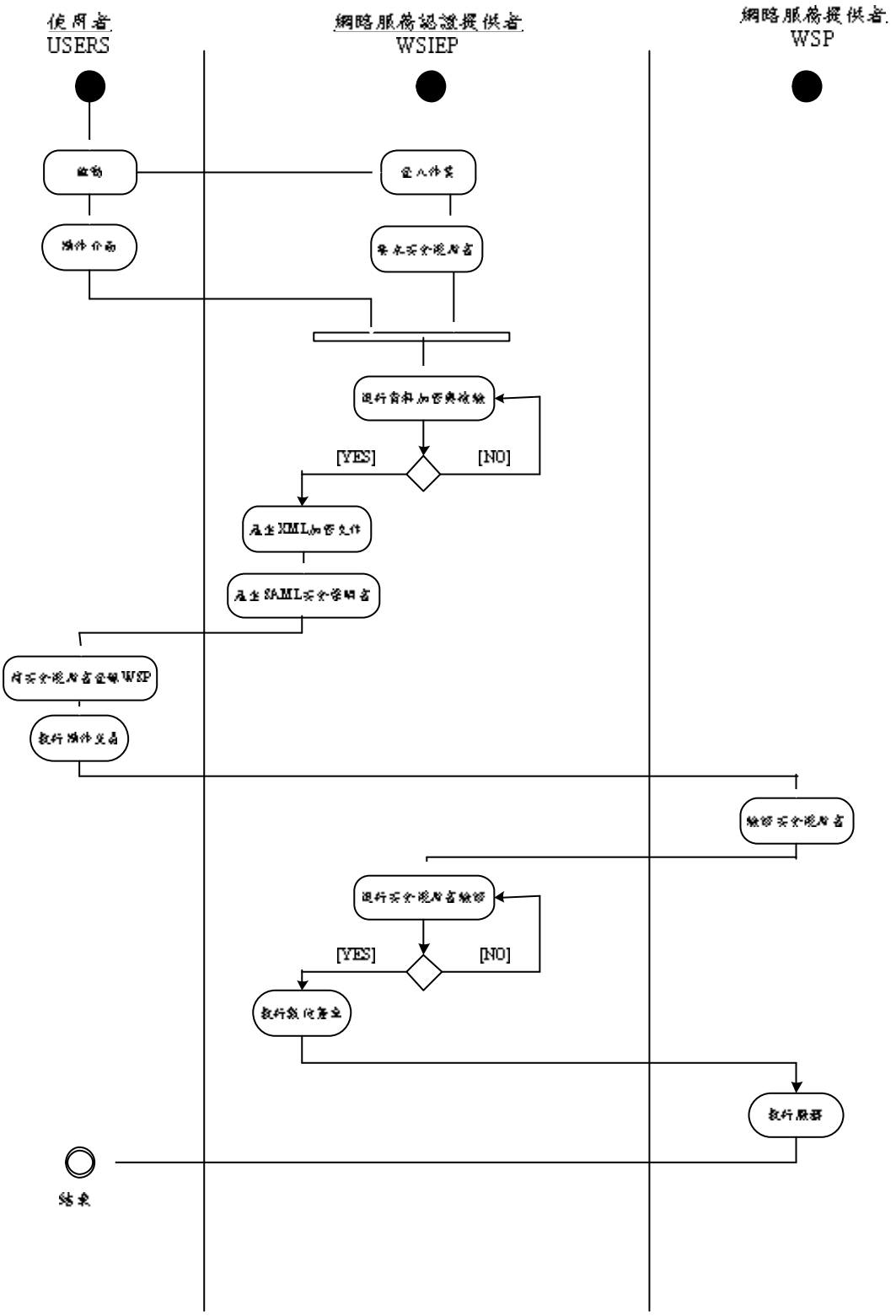
Step5. 使用者與服務提供者交易完成後，要將交易資訊寫入到證明

書之前，要先透過XML 安全檢驗服務向WSIEP 的ebXML 安全服務取得寫入授權碼，將授權碼與交易記錄綁定結合在一起進行加密保護。

Step6. 使用者再點選WSP 網站上其他合作網站的超連結如：WSP B，再將使用者與他持有的安全證書再導引到新交易WSP B 網站，繼續執行網站服務交易。

參、活動圖

為了更進一步清楚地了解各資訊元件間之傳遞行為，進行改良之為“活動圖”。在繪製XML IEF架構的活動圖時，首先根據使用者案例中所定義之三者行為者：使用者、網站服務認證提供者及網站服務提供者，以“游泳水道”加以區隔，以對各行為者之行為做明確的區隔，資訊認證交換平台所進行之處裡行為也將使平台開發人員更了解其資訊傳遞的方式。在活動圖中之表達方式中，可依據循序圖中所定義之資訊傳遞行為由上而下進行處理，也可利用活動圖中所提供之決策單位表達不狀況下之訊息傳遞路徑，圖為XML IEF的活動圖：


使用者
USERS
網路服務認證提供者
WSIEP
網路服務提供者
WSP
[YES]
[NO]
[YES]
[NO]
結束

就 XML IEF 的最終目的而言，其實就是要提供一個企業間單一登錄的認證交換平台；在單一登錄方面來考量，目前提供單一登錄的聯盟團體有 SUN 等多家企業的自由聯盟計畫〔Liberty Alliance Project〕[22]與微軟公司的 Passport 服務，SUN 為聯邦式的做法，Microsoft 則為單一陣營的集中式做法。如圖 18 所示，這兩個兩個陣營不僅就資訊技術或是商業角度都是對立的，若是全球各區域的商務網站都如此的作法，形成各自對立聯盟，使用者最後還是得記住多個特定聯盟的會員帳號與密碼，此結果只是局部的做到單一登錄而已，而不是真正的讓使用者只要記住單一會員帳號與密碼進行單一次登錄動作。

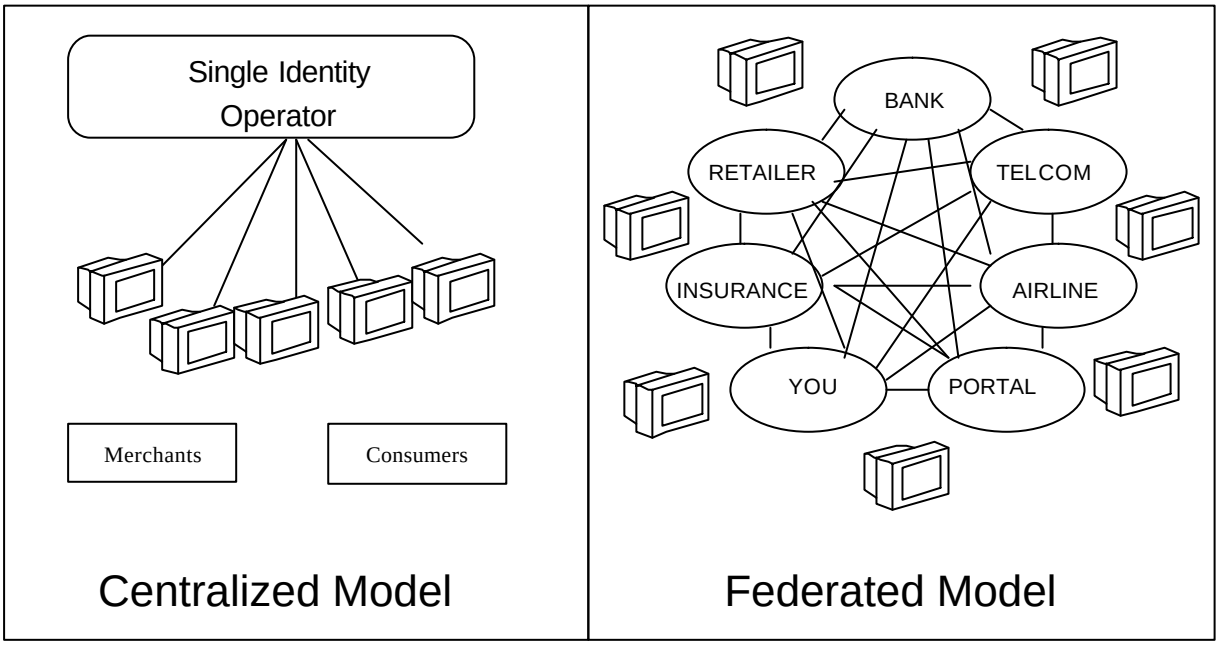


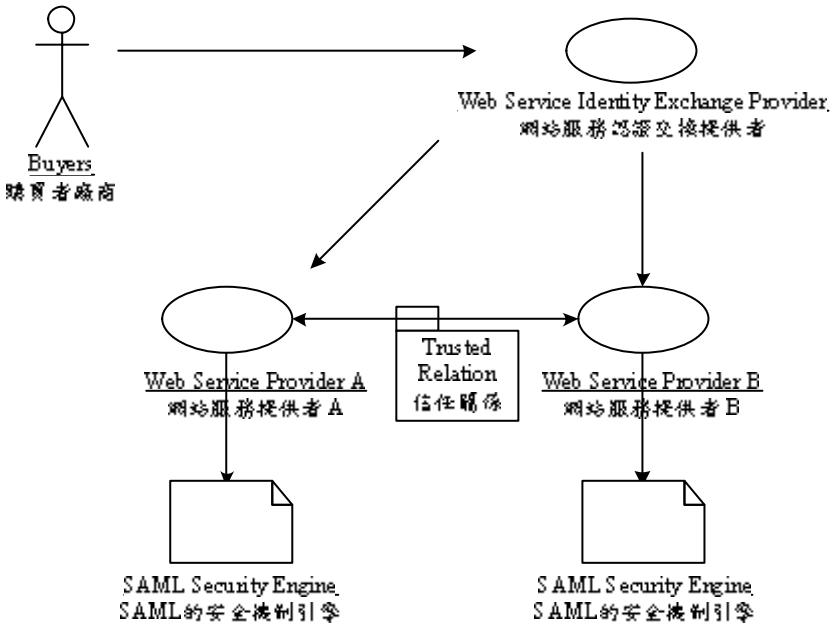
圖 18：Microsoft 與 SUN 企業認證交易商業模式圖，

〔資料來源，本研究整理〕

XML IEF **架構強調的是除了聯盟自己本身的溝通之外，還可以依據聯盟與聯盟之間的結盟，讓使用者真的只需要單一帳號與密碼，就可以在各聯盟之間進行認證與交易，更可應用於企業內或企業間的電子供應鏈整合。**

第三節、單一電子交易環境的採購模式

就單一電子商務的單純商業採購模式，可應用XML IEF **架構，針對相關的聯盟廠商間進行認證交換，採購者即可在聯盟的商務服務提供者間，執行商務服務內容，單一電子交易網採購流程步驟如下圖說明：**



WSIEP 請求發給交易授權書，購買者持著本授權書向聯盟廠商進行商務交易。

Step 2. 當購買者廠商持著WSIEP 所發給的交易授權書到供應商網站，經過供應商網站驗證通過，供應商網站提供下單訂購服務給購買者廠商，供應商會購買者廠商所訂購的交易資訊寫入到購買者廠商持有的交易授權書中。

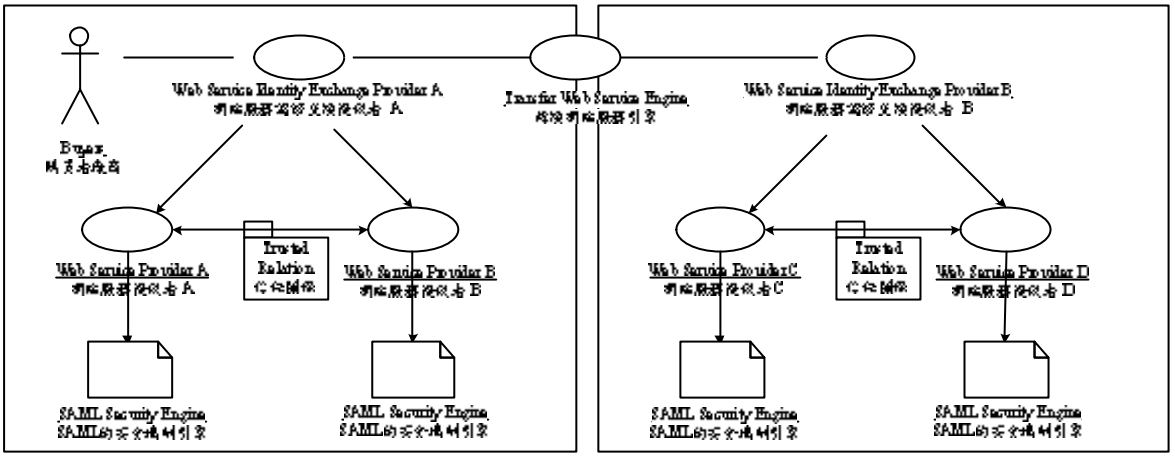
Step 3. 購買者廠商再藉由聯盟供應商網站的連結，依據所持有WSIEP 所發給的交易授權書，與其他的聯盟供應商進行商務交易。

Step 4. 購買者廠商於交易結束之後，將記載的交易資訊授權書攜帶回WSIEP，WSIEP 會判讀與驗證本交易授權書中所記載的交易內容，並將交易內容的資訊製成購買者廠商所需要的電子文件票據，讓他持有此證明票據，可以與聯盟供應商們進行進一步的後續交易處理。

第四節、兩個以上電子交易網環境的採購模式

這個模式是原本架構模型的延伸發展，假設現在有眾多個網站聯盟採用XML IEF 架構來整合網站之間的商務資源，首先就要要在各個聯盟網站的網站服務認證提供者上新增轉換網站服務引擎（Transfer Web Service Engine），它負責驗證跨聯盟網站的安全授權書，並依據該安全

授權書的規範來為使用者產生新的安全授權書，使用者持著新的安全授權書於該跨網站聯盟進行商務交易。就兩個以上電子交易網採購流程步驟如下圖說明：



Step 3. 當購買者廠商持著WSIEP B 所發給的交易授權書到供應商WSP C，經過供應商WSP C 驗證通過，提供下單訂購服務給購買者廠商，購買者廠商所訂購的交易資訊，供應商WSP C 會將此資訊寫入到購買者廠商持有新的交易授權書中。

Step 4. 購買者廠商再藉由供應商網站WSP C 所提供的其他供應商網站的連結，依據所持有的WSIEP B 所發給的新交易授權書，去與這些供應商進行交易。

Step 5. 購買者廠商於交易結束之後，將記載有交易資訊的新交易授權書攜帶回WSIEP B，並將交易內容的資訊寫入到原本購買者廠商帶來的WSIEP A 所發行的交易授權書中，讓購買者廠商帶回到WSIEP A 做進一步的交易訊息處理。

Step 6. 最後購買者廠商攜帶回記載有交易資訊的交易授權書到WSIEP A，並將交易內容的資訊製成購買者廠商所需要的電子數位票據，並將交易內容的資訊製成購買者廠商所需要的電子文件票據，讓他持有此證明票據，可以與聯盟供應商們進行進一步的後續交易處理。

本章小結

就本章所提出的企業間電子商務認證交換平台法展程序，我們從第一、二節的系統架構到流程塑模，都是在證明提出一個較可被企業所接受的商業模式，進而應用資訊科技的技術與工業、企業的標準，整合提

出一解決方案。就本章的三、四小節進一步的驗證說明單一及兩個以上的電子採購流程的做法，就以上可歸納出以下幾點，應用XML IEF建置企業的認證安全平的優勢：

一、更多選擇的供應商的機會：讓廠商可以有更多選擇下單訂購原料的供應商，避免原本供應原料的廠商缺貨時，要購買的廠商急需要原料但是無法取得原料，讓購買者廠商有更多替代選擇供應商方案，讓這樣的情境降低。

二、購買者廠商不必與各家供應商建立高成本的電子資料交換系統：藉由認證資訊平台的建立，購買者廠商可不必花費高成本建立企業間的電子資料交換系統，可縮短並減低了整體供應鏈的交易成本。

三、單一帳號的便利性：購物廠商只要記住單一帳號與密碼，就可以與眾多聯盟的供應商進行商務交易，免去各別與供應商建立眾多信任帳號與密碼的麻煩。

四、提供合作廠商之間供應鏈參考模型：讓廠商的下單網站服務之間可以便利與安全地進行互動，讓廠商有個參考建置環境，更容易建置起自己的供鏈環境。

第五章結論與建議

第一節研究結果

從緒論到文獻探討等章節可得知企業用於電子商務引進日趨複雜的階段可由傳統資訊技術模式進到整合資訊技術及標準模式，隨著Business Model 交易的複雜化，企業間電子商務的往來也愈趨複雜，針對每一商務發展於資訊技術程序架構，我們了解到商務交易模式及行為是何其複雜，在企業資訊運用及整合上又何其需求迫切。進一步為了解決達康公司〔 .com〕的電子商務認證與交易往來連結。本研究針對企業間未來在聯盟網站的網路服務協同合作下，運用Web Services 的資訊技術與ebXML 的安全技術與規範書，架構網站服務聯盟時所需要的安全認證交換機制。

就XML IEF 的企業間認證交換平台架構應用上，做SWOT 分析作為本研究之結果，下表8為SWOT 分析表：

表8：企業間電子商務認證交換平台發展程序SWOT分析表

<table>
<tr><td rowspan="5">企業間電子商務認證交換平台發展程序 SWOT 分析</td><td>Strength　強勢</td><td>Weakness　弱勢</td></tr>
<tr><td>1.便利性：提供 Single Sign On</td><td>1.多用在於企業的入口網站〔Portal〕建置</td></tr>
<tr><td>2.延展性：提供網站聯盟的聯結互動</td><td>2.國內尚未有聯盟式的商務網站或組織</td></tr>
<tr><td>3.開放性：依循 ebXML 的企業開放標準</td><td>3.完全依循 ebXML 標準建置的網站未普及</td></tr>
<tr><td>4.相容性：可透過 Web Services 資訊協定整合</td><td>4.依照 Web Services 資訊協定建置的網站不多，整合不易</td></tr>
<tr><td>5.安全性：藉由 XML Security 技術保護相關資訊訊息</td><td>5.企業尚未針對 XML Security 相關的安全技術標準加以應用</td></tr>
<tr><td>Opportunity　機會
1.新的資訊技術開發
2.新的資訊技術應用
3.資訊需求〔IT 輸出〕的增加
4.工業、企業標準化的整合
5.企業間的協同合作
Threat　威脅
1.企業間信任度〔Trusted Relation〕高低
2.網路環境與聯盟網站的實體架構穩定性
3.各國對於電子商務的法令限制
4.各國間的 PKI 認證機構未整合
5.市場規模的大小</td><td colspan="2">歸納結論：

電子商務固然可以改變企業運作模式與增進效能，但是國際貿易之危險與困難度不僅止於資訊交換或認證而已。就實體貿易與虛擬貿易上，結合資訊技術與標準是一種趨勢，就亞太地區電子商務發展而言，目前已經有合併官方及民間的交易標準與認證程序，建立單一的入口『Mega Portal』服務網站，提供與世界相關的商務網接軌連結。
利用電子商務進行國際貿易時必須要考慮地區的特性，不同地區對於不同的產品喜好程度亦有所不同。從一個較為宏觀的格局來檢視電子商務與國際貿易發展，電子商務所涵蓋之範圍不應僅僅於網路上之商務交易，而應著眼於全球運籌體系之形成。</td></tr>
</table>

〔資料來源，本研究歸納整理〕

第二節研究建議

隨著電子商務的普及發展，建立安全及可信賴的電子認證機制，確保資訊在網路傳輸及儲存過程中之安全性，並賦予電子簽章及電子文件之法律效力，保護使用者的權益，是電子交易能否普及應用的關鍵。

就上述的研究結論提出兩個研究的建議方向：

一、針對未來電子商務發展趨勢的研討：可以預期的是，未來將會有越來越多的企業利用電子商務系統來進行交易。因此針對企業應用電子商務於網路的資料交換、資訊安全、法律制度等議題，身為資訊人不得不有所警覺與認知。因為，電子商務成功之關鍵不在於系統的共通性，而係繫於系統能否符合特定顧客群之需求，以及能否為顧客創造出更好的附加價值。

二、針對未來資訊技術發展趨勢的研討：近年來電子商務發展的重心一直為系統的整合與標準化，此種具有單一整合的觀念除了影響電子商務技術層面之發展，或多或少也影響了企業在運用電子商務拓展商機之基本商務觀念。針對 Web 的相關資訊技術與工具發展上，利用網際網路來進行資訊之交換與系統建置，並降低企業的資訊投資，有效進行資訊之管理，以達到資源最佳化的境界。

第三節研究貢獻

本研究利用ebXML 安全技術來建置Web Service XML 的電子商務架構，及利用XML IEF 架構為基礎，進而延伸到單一及兩個以上的企業電子採購的流程塑模結果，讓我們瞭解到ebXML 安全技術應用於Web Services 資訊技術架構下的電子商務商如何整合用與認識。就本研究的貢獻提出下列幾點看法：

一、探討新興的ebXML 安全技術標準作為系統架構基礎，讓ebXML 安全技術可以很容易地被企業所瞭解並加以推廣應用。

二、建置以ebXML 安全技術為基礎的可擴展整合性的Web Services 網站服務，提供給企業一個網路服務的安全機制參考方案。

三、藉由UML 的技術，針對企業內或企業間的資訊系統整合，提供一個流程塑模的模式，讓企業未來應用於整合企業的資訊資源上有一個參考的依循方法。

四、XML IEF 架構為聯盟網站提供一個合作模式的參考整合方案，進而提供在企業間進行交易架構中，說明了不同網站間的網站服務的安全互動方式，提供單一登錄的聯盟網站認證服務機制。未來更延伸應用於國際間的供應鏈整合〔Global SCM〕。

第四節後續研究

本研究提出之企業間認證交換平台發展程序，在過程中上有許多未臻完善之處，進而在後續的研究發展上，可針對下列幾個方向進一步探討：

一、參照未來ebXML 安全技術標準的發展，來加強XML IEF 架構的安全性與便利性。由於ebXML 安全相關規範書是近年來才正式公佈，因此，ebXML 安全技術輔助軟硬體工具都還未成熟地開發出來，導致架構上還是有部份有待修正與加強。

二、就開發Web Services 的資訊技術工具使用上，無論是採用J2EE 或 .NET，要如何慎選開發工具，則需要兩大陣營Microsoft 及 Sun Microsystems 的合作與整合，因此研究出一個可整合兩大系統架構的發展工具或是資訊技術，也是一項未來值得研究的技術課題。

三、資訊模式互通的課題裡，語意層與語法層，即 UML 與 XML 或 UML 與 JAVA 相關技術，如何透過物件層進行交換與互通，可作為後續研究。

四、以目前的企業間電子商務發展，本研究提出一認證平台發展程序，對於各項系統元件所組成條件，如何將其模組化進而設計

開發出來，並讓其可快速應用於不同的聯盟電子商務間，達到整合化的目的。

參考文獻

一、中文部分

[1] 王柳鋐編譯(1999)[民 88]，Microsoft 之電子商務解決方案.網站技術篇，碁峰資訊。

[2] 吳仁和、林信惠，系統分析與設計理論與實務應用，滕智文化事業有限公司，2002 年。

[3] 陳志昌編譯，UML 技術手冊，美商歐萊禮股份有限公司台灣分公司，1999 年。譯自 UML in a Nutshell，原著 Alhir, S. S.。

[4] 蔡桂芳、萬洪濤 著(2000)[民 89]，e-marketplace—B2B 虛擬商場完全經營手冊，商周文化。

[5] 查修桀、連麗真、陳雪美 譯(1999))[民 88]，電子商務概論。

[6] 于千智等，電子商務總論，智勝文化事業，台北市，1999 年。

[7] Mougatar, W., 萬象翻譯公司譯，電子商務致勝策略，跨世紀電子商務出版社，台北市，2000 年。

[8] 何經華，製造業電子化國際高峰論壇，2000 年，9 月。

[9] 孫三才，“整合開發應用 HailStorm 實作 Passport Single Sign-In 及 Alert Service 介紹”，Microsoft Visual Studio .NET 研討會，2000。

二、英文部分

[10] Booch, G., Rumbaugh, J. and Jacobson, I., The Unified Modeling Language:User Guide. Addison-Wesley, Reading, Massachusetts, 1999.

[11] Gates Bill , Business@the speed of though : Using a digital nervous system , William H. Gates , III , 1999.

[12] Imamura, Takeshi, et al., “XML Encryption Syntax and Processing ,” W3C, 2002/3.

[13] Moses, Tim and Prateek Mishra, et al., "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML)," Organization for the Advancement of Structured Information Standards(OASIS), 2002/4.

[14] Turban, E., Lee, J., King, D., & Chung H. M., Electronic Commerce: A Managerial Perspective, New Jersey: Prentice-Hall, 2000.

三、網站部分

[15] **製造業電子化** eB **服務網，**http://www.ebmfg.org.tw。

[16] **經濟部動電子簽章法計劃，**http://www.esign.org.tw/。

[17] **經濟部商業司，電商務導航，**http://www.ec.org.tw/ecpilot。

[18] **經濟部網際網路資訊情報中心，**http://www.find.org.tw。

[19] **數位簽字—公開金鑰認證機構介紹，**
http://stlc.iii.org.tw/publish/infolaw/8511/851109.htm

[20] Sun Microsystems, "How to Implement Network Identity", SunMicrosystems, Inc., 2002, http://www.sun.com/sunone/identity.

[21] http://www.broadvision.com/OneToOne/SessionMgr/home_page.jsp

[22] http://www.projectliberty.org/

[23] http://www.microsoft.com/

[24] http://www.sun.com/index.xml

[25] http://www.oasis-open.org/home/index.php

[26] http://xml.coverpages.org/saml.html

[27] http://www.omg.org/uml/

[28] http://www.w3c.org.