PROSIDING
SEMINAR
KEBANGSAAN
SAINS, TEKNOLOGI & SAINS SOSIAL

27 ~ 28 MEI 2002
HOTEL VISTANA, KUANTAN, PAHANG

Anjuran :

Universiti Teknologi MARA
Cawangan Pahang

Dengan Kerjasama

Kerajaan
Negeri Pahang Darul Makmur

JILID 1

MODENAS ENTERPRISE WEB-BASED SYSTEMS (MEWS) FRAMEWORK FOR E-COMMERCE SOLUTIONS IN MODENAS

ZAILANI ABDULLAH, MD YAZID M.SAMAN, MUSTAFA M.DERIS AND POUZI HASSAN
Department of Computer Science, College University Science and Technology Malaysia (KUSTEM), 21030 Mengabang Telipot, Terengganu.

ABSTRACT

This paper is part of the Enterprise Web-based System (MEWS) proposal for Motosikal Dan Enjin Nasional Sdn Bhd (MODENAS). The main focus of this paper is on the conceptual model of e-commerce environment and an introduction to the terminology associated with the technology. The e-commerce model has been chosen due to current market trends and it is believed to be the right strategy for participation in worldwide markets globalization. Thus, a proper infrastructure and readiness of web-based applications is essential to ensure that the company is on the right track before the AFTA 2005 implementation. There are two web-based applications considered as e-commerce systems, namely Electronic Excise System (EES or e-excise) and Electronic Procurement System (EPS or e-procurement). Generally, EES will focus on the finished product (motorcycle) handling whereas EPS will concentrate on raw material purchasing (motorcycle spare part). All the topics covered here will give an overall idea of the MEWS project framework and how it rationalizes MODENAS' heterogeneous environment. Successful modeling of the complete e-commerce environment will become the benchmark and starting point for development of our own e-procurement system in the near future.

Keywords: *e-commerce, web-based application, e-procurement and heterogeneous environment.*

INTRODUCTION

Internet technologies and application have grown more rapidly than anyone could have envisioned just five years ago, opening up new frontiers and interaction between consumers, business and trading partners (11). Electronic commerce, or e-commerce, is a very broad term. Generally, e-commerce conducted between businesses differs from that carried out between a business and its consumers. The universal definition of e-commerce can be summarized as the buying and selling of goods and services via electronic means such as the Internet (3). E-Commerce uses computer technology to automate and streamline the complex processes in an effort to reduce operational costs and create greater profit margins (7). Instead of merely reducing costs (administrative and overhead), it also provides many of the same benefits for groups of enterprises and individual consumers as business transformation within the enterprise, including the elimination of delay and error (13).

The transactions undertaken in e-commerce usually involve buyers, suppliers, and information service providers (ISP) (18). The technologies used for e-commerce include electronic data interchange (EDI), e-mail, electronic bulletin board systems, electronic catalogs, electronic forms, finance and banking technologies, smart cards, fund transfer, and digital cash.

EDI emerged as an important aid to transact business electronically in the 1980s. EDI means the computer-to-computer exchange of business transactions, such as purchase orders, invoices and payment advises within large industrial communities or government. There are two major families of EDI standards, which are X12 and EDIFACT (5). Usually, EDI is made up of application programs, network software, and translation software (4). Although EDI is an integral part of the digital economy, over the course of more than 20 years, only a small fraction of the business world adopted EDI. Problems such as lack of an open global infrastructure and powerful applications to link every aspect of a business relationship have continued to plague EDI and similar IT inter-organization (2).

Security in e-commerce is extremely crucial. The firewall is a multiple authentication method to control data access particularly because hackers are often persistent and ingenious in their efforts to gain unauthorized access. This device (e.g., a computer) is placed between an organization's network and the Internet (6). The firewall will inspect all communication passing between the Internet and the private network and either pass or drop the communications depending on how they match the programmed policy rules (16). There are two approaches to secure transmissions over the Internet, Secured HTTP (S-HTTP) and Secure Socket Layer (SSL). S-HTTP acts on the upper application layer to provide secure

communication mechanisms between an HTTP client/server pair, to enable spontaneous commercial transactions for a wide range of applications. SSL is an encryption protocol and rapidly became the preferred method of securing transmissions across the Internet. Both S-HTTP and SSL support digital signatures, digital certificates, and secret-key encryption algorithms, but the open and nonproprietary nature of SSL makes it the ideal choice for TCP/IP application developers to secure data (15). The users can determine that which have come across to the secured web pages by looking at the browser's web site address. This web site address will start with "https://" rather than the usual "http://". Their browser will also likely display a "closed lock" or other symbol to inform that SSL has been enabled.

Digital certificates are in effect virtual fingerprints that authenticate the identity of a person or thing absolutely, positively. The certificate itself is simply a collection of information to which a digital signature is attached. The digital signature is attached by a Certificate Authority (CA) – a third-party authority that is trusted by the community of certificate users (17). Digital certificates are based on public/private key technology, the same technology used to protect nuclear missile sites. Each key is like a unique encryption device. No two keys are ever identical, which can be used to identify its owner. Keys always work in pairs, one called the private key, and the other called the public key. What a public key encrypts, only the corresponding private key can decrypt, and vice-versa (9).

The paper proposes the MODENAS Enterprise Web-based System (MEWS). It will discuss a framework and the practices of implementing e-commerce in this company. This framework will also touch on redesigning the business model and introducing a scalable e-commerce solution at affordable cost. Some of the uncertainties and problems while developing and implementing the e-commerce system have been resolved through the MEWS framework. Thus, the idea and solution proposed is an important factor to be reviewed by this company in order to provide a competitive edge and better services to their business partners.

MATERIALS AND METHODS

This research has been carried out since the middle of 2000 until late 2001 and implemented at MODENAS, Gurun, Kedah. Generally, IT infrastructure can be described as those production and maintenance support for major applications, data warehousing and support for e-commerce system. In the MEWS framework, most of the technology and components used are free or at least at minimal cost.

Currently, the related MODENAS business processes are not fully integrated with our business partners due to the weaknesses in setting up and configuring the web server. Even though the new infrastructure for web-based applications is already in place, the company is still unable to utilize the existing infrastructure to provide a complete e-commerce environment to suppliers as well as dealers.

The discussion on the first e-commerce system at MODENAS called e-procurement will cover indirectly, Supply Chain Management (SCM). Basically, SCM is one of the areas applied by an e-commerce model (8). E-commerce and SCM are closely inter-related since integrated business transactions are recognized to yield substantial value to sellers and customers (1). SCM aims to provide advantages, cost reduction, quality improvement and flexibility enhancement (12).

The e-procurement system (or EPS) was deployed by MODENAS in early 1998. It was provided by Singapore Network Services (SNS) for publishing procurement information in MODENAS's Intranet. Basically, MODENAS sends procurement data in flat-file format to SNS. Once it is received, SNS will just publish all this information in the web page. Suppliers or vendors will then access their related information when they logon into the system.

The objective of a new e-procurement system is to enhance competitive edge and best practice for doing business with suppliers. MODENAS will prepare the list of parts that have been ordered in the Material Resource Planning (MRP) system. Users are not required to printout the purchase order and manually send them to the supplier. Normally, by the end of the day, the procurement data in the predefined flat-file format will be generated and sent manually to SNS for publishing the following day.

The supplier will notice any new purchase order from MODENAS by logging into the E-procurement system. They will then download the data into Microsoft Excel spreadsheet format for reference. SNS will charge them based on the item (parts) listed in the "purchase order" appearing in the Excel spreadsheet.

Basically, this system has 7 modules that can be used by vendors, namely Purchase Order, Delivery Schedule, Receiving DO Report, P/O Data Inquiry, Outstanding P/O, Invoices Detail Summary and Account Payable Checklist.

Based on the analysis, current e-procurement activity is not cost-justified and rather expensive both to the company and suppliers. For the year 2001, most of the vendors have not paid SNS charges (approximately around SGD 30,000).

MODENAS

Items	RM/Year
Sunrock Service fee	36,000.00
HAS Sunrock Server Operation fee	102,000.00
SNS Server Operation & Maintenance fee	18,000.00
EDI/WEB Transaction fee	24,000.00
TOTAL	180,000.00

Supplier

Items		RM/Year
Subscription fee		1,200.00
User ID		480.00
Transaction Fee	2.50 per message	
TOTAL	Min	2,520.00
	Max	8,520.00

Table 1. SNS E-Procurement Charges

Table 1 shows that the company has to spend yearly RM 180,000 and the supplier has to allocate between RM 2,520 to RM 8,520 annually to enjoy the service.

The second e-commerce system at MODENAS is Electronic Excise System (EES). Generally, this system will cover the electronic data interchange between MODENAS and Jabatan Kastam dan Eksais Diraja (JKED). The EES is based on a dedicated leased line "Extranet" connection provided by Dagang*Net Technologies Sdn Bhd, linking MODENAS with *Jabatan Kastam dan Eksais Diraja* and *Jabatan Pengangkutan Jalan (JPJ)*. The system would facilitate the electronic submission and endorsement of Excise 7 document, and automation of excise duty payments, thus leading to online vehicle registration. The details of estimated yearly charges by using EES can be shown in Table 2.

Items	Estimated RM/Year
Operating Cost - RM 0.70 per KB. Normal message size is 1.3 KB - Storage charges RM 2 after 5 days (per KB, per day) - Estimated usage is 450 KB for 400 bikes - Estimated delivery 100,000 per annum	70,000.00
Subscription fee	2,160.00
Annual Renewable License Charges	525.00
TOTAL	72,685.00

Table 2. Dagang*Net EES Charges

Even though most of the EES is already in place, MODENAS still has to fax manually Excise Receipt Release documents to the respective dealers after payments have been made. EES reduces the time required for the approval process and replacement of an existing Excise 7 document upon registration with JPJ. Currently, MODENAS still has to courier the motorcycle *invoices* to dealers and fax Excise Receipt Release documents to dealers.
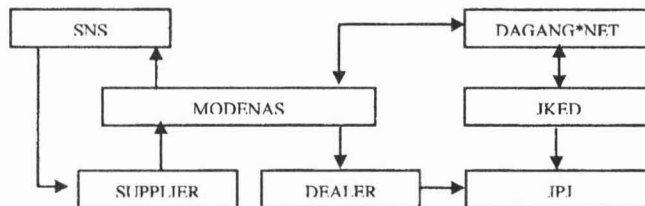

Figure 1. Overview of MODENAS Business Model

The business model is shown in Figure 1. This business model is a major constraint for MODENAS in using fully the advantages of e-commerce. After conducting a few rounds of research on the present

environment, this business model can be improved by restructuring and reconfiguring the web-server. The detailed explanation of this business model is shown in Figure 2.
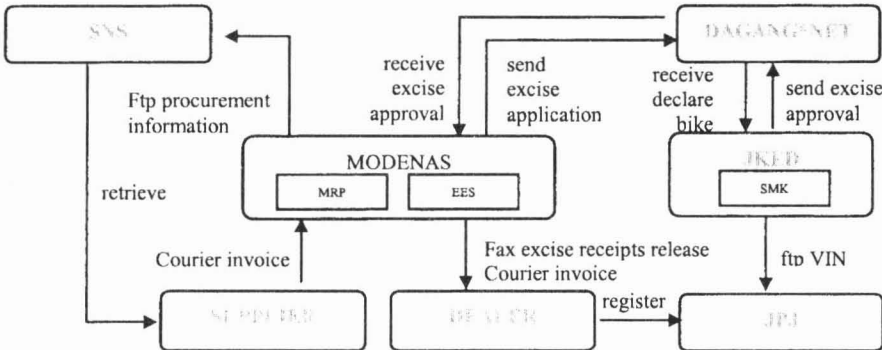

Figure 2. Detailed of MODENAS Business Model

Virtual Private Network (VPN) is a new technology that allows secure remote access to a private network via a "privacy" tunnel installed within an existing infrastructure. A secluded (private) tunnel is created inside an already existing larger public network, and from the user's perspective, it appears (virtual) to be operating within a distinct and independent system of interconnecting lines or channels (network) (14).

Currently, all the branches are connected to a web server through a VPN tunnel. In practical terms, VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies. In other words, VPN turns the Internet into a simulated private Wide Area Network (WAN).

VPN technology has been used for connecting the company's applications residing in internal LAN rather than DMZ area. The current diagram for the entire LAN and Internet Infrastructure is shown on Figure 3.
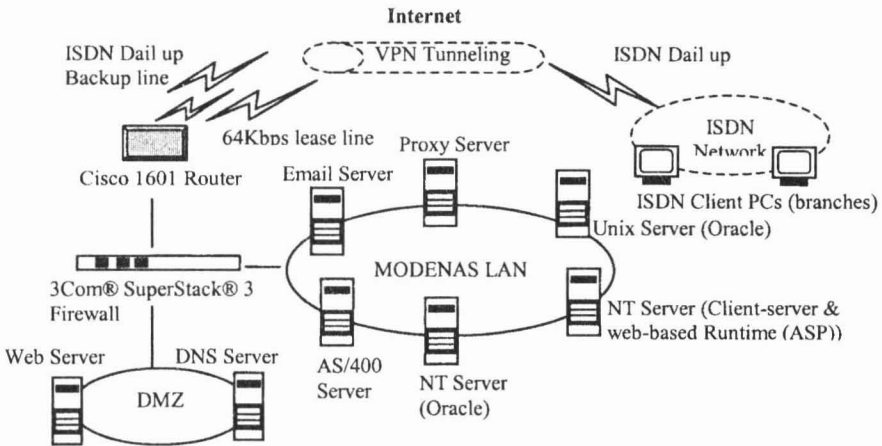

Figure 3. LAN and Internet Infrastructure

138

Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. The DMZ network can also be used to host public servers, such as Web servers, that should be protected from the Internet, but isolated from the company LAN for security reasons (10).

The original business model and configuration of the IT infrastructure discourages MODENAS from implementing the e-commerce system in the near future. The web-based server and IT infrastructure need to be reconfigured in the best manner and this is where the MEWS solution fits in.

RESULTS AND DISCUSSION

In the early stage of e-procurement implementation, MODENAS was constrained to provide the web-based infrastructure as well as internal expertise. In the middle of the year 2000, the connection between web development technology and DB2/400 database was successful regardless of the AS400 version. For this exercise, the author used Hits OLEDB server as a middle-ware (data link) between this database and *Active Server Pages (ASP)*. The author identified the business-critical databases at MODENAS as DB2/400 and Oracle (Unix or NT platform). After successfully connecting all these databases (located in internal LAN) using ASP technology (located in DMZ), the new business model can be derived as in Figure 4.
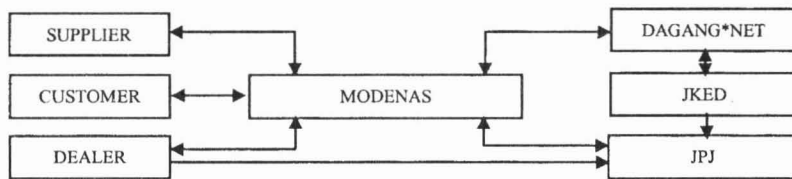

Figure 4. Overview of MEWS

From Figure 4, the SNS entity has been removed and the dealer or supplier will have two ways of communication to MODENAS. An additional entity called "customer" is also included to show that customers are enabled to perform business dealings directly with MODENAS. Otherwise, the rest of the flow remains unchanged especially with regards to JKED.
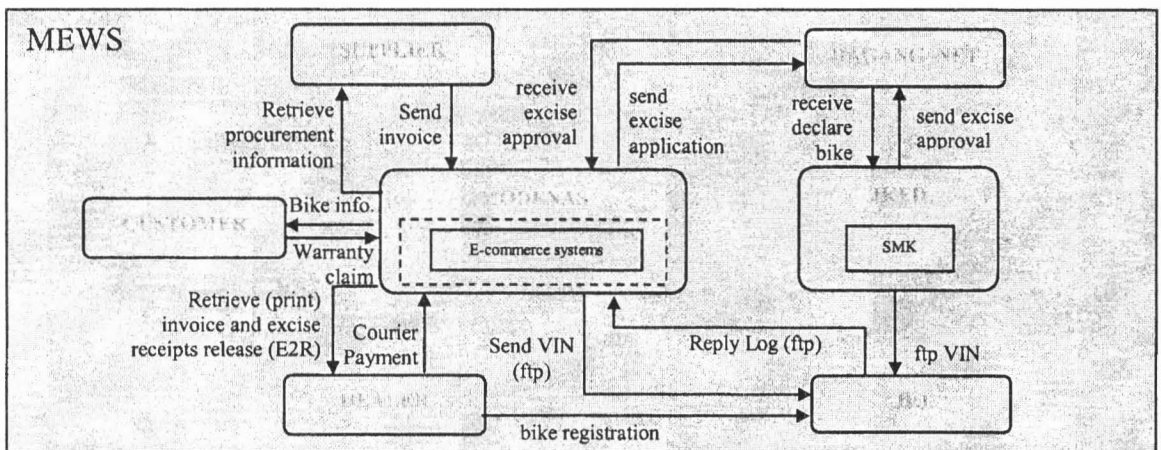

Figure 5. Detailed MEWS Framework

The detailed proposal for a MODENAS business model can be viewed in Figure 5. The successful implementation of MEWS will become the catalyst for e-commerce efficiencies. The obvious impacts are cost reduction about RM 180K per year for e-procurement system (in-house development) and full business integration.

Generally, the business model will show only the basic flow of business processes conducted among the business partners. The overview diagram bellow will show how we are going to implement MEWS proposal based on software, hardware and networking architecture.

The firewall is a combination of hardware and software used to implement a security policy governing the network traffic between two or more networks, some of which may be under our administrative control (e.g., organization's networks) and some of which may be out of user control (e.g., the Internet). Based on Figure 6, dual virtual firewalls are created by using a single firewall providing different security policies for each attached interface in the firewall.
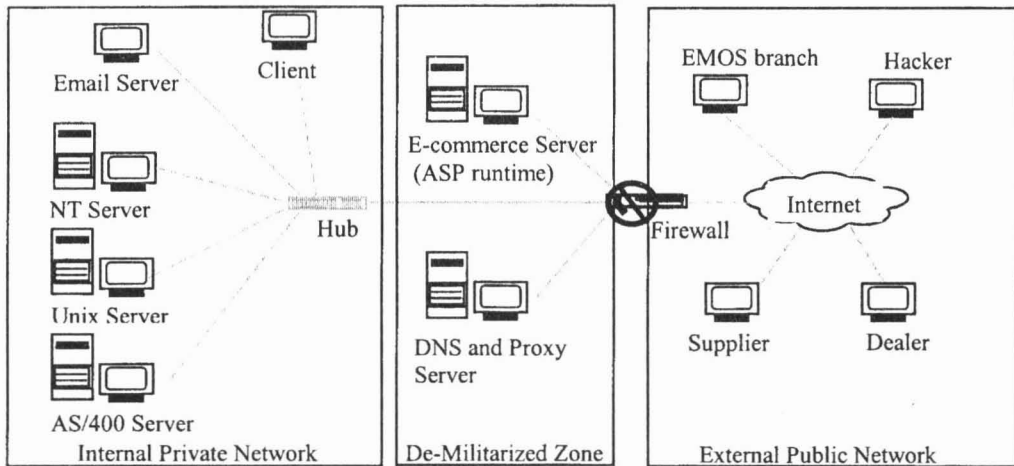

Figure 6. Detailed MEWS Technical Diagram

Currently, all MODENAS service center branches are connected to the company's applications through VPN. These branches use ISDN facilities rather than PSTN to dial into the Internet Service Provider (ISP). Since the integration between two network areas (DMZ and internal LAN) has been resolved, the company could use normal Internet tunnel rather than VPN tunnel.

As mentioned in the middle of this paper, IT staff were unable to resolve connectivity between two networks. They proposed connecting the critical databases by using the mapping method. An author found that this method is not suitable and also would expose our internal network to hackers. The "hidden tunnel" would be created automatically by deploying the above method. Based on the study, this networking connectivity could be established by configuring "route" at the firewall level and "default gateway address" at database - operating system level.

At the moment, MODENAS is using Oracle database running on RISC/6000. The author would like to recommend MODENAS to upgrade Oracle 8.0.4 database in Unix Server to Oracle 9i in NT Server. The existing RISC/6000 server is really unstable and the yearly maintenance fee is very expensive (RM 80K). For the DB2/400 database, the upgrading cost is very expensive and involves upgrading the AS/400 machine itself (estimated 1 million). It's better to stick to the AS400 original version.

Based on the model in figure 7, in terms of security, it is more secure since the public or hacker can only enter the DMZ area and no more tunnels have been provided to go inside our LAN. If the Web Server at DMZ area is corrupted, the NT administrator will just restore the operating system (Windows NT), Internet Information Server (IIS) and ASP runtime. Company data is still under control and safe from irresponsible users. When the e-commerce server is located in DMZ area, the company must apply digital certification in order to provide secured online transmission between business partners and the company. For example, *Excise Receipt Release* is one of the confidential and legal documents to be delivered to dealers. By implementing digital certification, MODENAS can ensure that confidential documents are protected from interception and viewing by unauthorized busybodies.
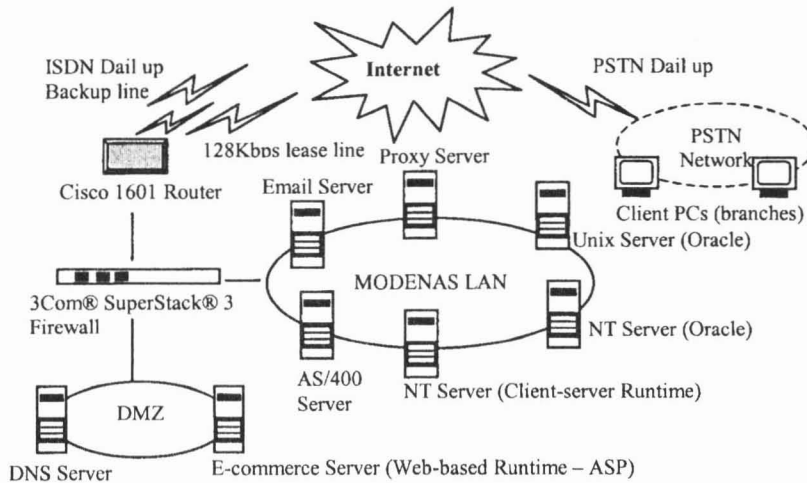
Figure 7. LAN and Internet Infrastructure for MEWS

The advantages of the new LAN and Internet infrastructure as shown in the Figure 7 are:

- *Cost Saving*: MODENAS service center branches can dial into the Internet by using the Public Switched Telephone Network (PSTN) rather than Integrated Services Digital Network (ISDN). Normally, the charge of calling Internet using PSTN is half of ISDN cost.

- *Better Performance*: The response time will be better since the branches are not using Virtual Private Network (VPN) method for connecting to the application server. No encryption and decryption is required for our data during transmission process.

- *Security*: It is more secure to put the web-based application in DMZ area in order to prevent unauthorized users from hacking into any connected PCs or Severs in our LAN area.

- *Securing the network*: Capable of controlling the kinds of legitimate connections, to let outside hosts into the company's e-commerce server, and which kinds of connections internal hosts can make to the e-commerce server.

The MEWS framework can be seen as a key ingredient to ensure significant efficiencies and effectiveness in implementing e-commerce solutions at MODENAS. By re-engineering the business model and IT infrastructure, it will tremendously improve the information flow and enable the company to break the old rules as well as create a new way of interacting with business partners. What is significant know is that the company has found the capability to develop its own e-procurement system and also can exploit the web as a powerful business channel in the near future.

ACKNOWLEDGEMENT

REFERENCES

1. Alt Rainer, Fleisch Elgar, Osterle Hubert "Electronic Commerce and Supply Chain Management at ETA Fabruques d'Ebauches SA" Journal of Electronic Commerce Vol2, Number 3, 2000

2. Anetesh Barua, Andrew B.Whinston, and Fang Yin. Internet Watch (May 2000). Value and Productivity In The Internet Economy

3. Bontis Nick. The first world Congress on the Management of Electronic Commerce: review and commentary. 2000. Volume 10 Number 5:pp. 365 – 373

4. C,Sawyer Stacey, K.William Brain, E.Hutchison Sara(1999), Using Information Technology: A Practical Introduction To Computers & Communications (Brief version), Irwin McGraw-Hill companies, Inc., USA

5. Ford Warwick, S.Baum Micheal (1997), Secure Electronic Commerce: Building The Infrastructure For Digital Signatures And Encryption, Prentice Hall, Inc New Jersey

6. G.Mckeown, T.Watson Richard (1997), Metamorphosis: A Guide To The World Wide Web & Electronic Commerce, John Wiley & Sons, Inc. Canada

7. Held S Jonathan, Bowers R. John (2001), Securing E-Business Application and Communications, Auerbach Publications, CRC Press LLC, 2000 N.W Corporate Blvd, Boca Raton Florida USA. p3

8. Hinkkanen, A., Kalakota, R. , Saengcharoenrt P. Stallart, J., and Whinston, A.B (1997), Distributed Decision Support Systems for Real Time Supply Chain Management Using Agent Technologies, Addison Wesley Publishing, pp. 275 – 291

9. How Digital Certificate Work
http://home.nestcape.com/security/techbriefs/certificates/hoecerts.html?cp=stbmid

10. Instagate EX2 - DMZ (Demilitarized Zone)
http://www.esoft.com/products/iex2/dmz.cfm

11. Internet Watch. May 2000, Anitesh Barua, Andrew B. Whinston, Fang Yin. Value and Productivity in the Internet Economy

12. Jenkins, G.P., and Wright, "Managing inflexibility Supply Chain"), International Journal of Logistic Management, Vol 9, Number 2 pp. 83 – 90

13. Messerchmitt G. David (2000), Understanding Networked Application: A first course, Morgan Kaufman Publishers, Inc., San Francisco, CA USA

14. Network Magazine 10/01/98: Virtual Private Network by Lee Chae
http://www.networkmagazine.com/article/NMG20000727S0029/1

15. Oracle Magazine November 2000: Industry Standard: Introduction to SSL by Doug Obeid
http://www.oracle.com/oramag/oracle/00-nov/index.html?o60ind.html]

16. Strebe Matthew, Perkins Charles (2000), Firewalls 24 seven, Subex Inc., Alameda, CA

17. VeriSign White Paper: Encryption and Digital Certificates
http://www.verisign.com/whitepaper/enterprise/overview

18. Y.Shee Daniel, Tang Tzung-I, Modeling the Supply Demand Interaction in Electronic Commerce, Journal of Electronic Commerce Research, Volume 2, Number 3, 2000