A study on building of a common gateway for secure exchange and transmission of electronic business message

Ruey-Kei Chiu and Shiao-Ping Yu
Department of Information Management, Fu-Jen Catholic University, Taipei, Taiwan, Republic of China, and
S.C. Lenny Koh
Management School of University of Sheffield, Sheffield, UK

Abstract

Purpose – To present a research model attempting to build an innovative common gateway complaint with Rosettanet Standards for the secure message exchange between electronic businesses under this age of internet economy. The use of Rosettanet Standards is to achieve the effectiveness and efficiency of message exchange and consequently gain mutual benefits by means of agile response for cross-organizational co-operation.

Design/methodology/approach – The common service gateway is modeled by taking the advantages of transmission comply with the standard model specified by RosettaNet among business trading partners involved in supply chain system. A prototyping system compliant with the model presented is built and installed as a gateway interface of digital firms and seamlessly integrate to the firm's backend information system to conduct the message exchange with its business trading partners. The prototype is also implemented to prove the feasibility and effectiveness of this proposal of innovative model.

Findings – Through the practical experiment, the service model provided can really assist the firms using this service gateway to conduct its peer trading partners with having same gateway installed may streamline their flow of business data and create a higher value of supply chain between them in terms of communication and operation costs.

Research limitations/implications – More experiments and trials of the prototyping system need to be conducted in different test cases in order to make a concrete conclusion of this paper.

Practical implications – The adoption of international standard model is easier to implement a supply chain system and the business value is also can be achieved if the electronic data exchange is carried over the internet.

Originality/value – The system model presented in this paper can be a valuable reference for further similar development to build an electronic business to achieve the low cost, high efficiency, high security message exchange for digital firms at this internet era.

Keywords Electronic commerce, Internet, Electronic data interchange, Value chain, Supply chain management

Paper type Research paper

Benchmarking: An International Journal
Vol. 14 No. 3, 2007
pp. 306-319

1463-5771
DOI 10.1108/14635770710753130

Introduction

Voss *et al.* (1997) collected data from 660 managers and found a positive relationship between benchmarking and operational performance. According to these authors benchmarking improves performance by helping a company to identify best practices, set challenging performance goals, and implement decisions based on existing needs. He found the improvements in purchasing performance should have a positive effect on business performance. Whyte (2001) describes the technical architecture and components that can be integrated in order to provide a comprehensive and robust infrastructure on which to build successful e-Business. The highest profit activity in electronic business is undoubtedly that conducting "buying and selling things on the web" with supply chain partners. Supply chain system (Supply-Chain Council, 2002) can effectively solve trading problem among digital firms by means of fast data transmission and agile electronic data interchange (EDI) (Housley, 1999). It is a sort of most commonly used approach to gain competitive advantages and enhance the business value in this digital economy age. Bakos (1991) mentioned the systems between trading-partner firms may run on different platforms and/or use different data formats. Hence, during the conduction of data interchange one needs to integrate legacy data residing in each firm's existing applications and transfer of business information, based on a collection of standard message formats, has provided businesses with a way to exchange data via any electronic messaging service. This is known as electronic data exchange. However, adoption of EDI implies certain tasks and procedures must be agreed, in that companies must conduct an analysis to determine precisely how they are going to move their business data to and from the predefined EDI formats. Moreover, Webber (1998) suggested the combination of EDI and XML technologies (XML/EDI Group, 2003) to build the exchange message could efficiently support interaction and cooperation between various types of companies, while the required functionality is delivered over the internet. The system can efficiently support communication with companies that have their own legacy, EDI-based, enterprise systems. All types of interaction with such systems do not affect the traditional working methods of the related companies. In addition, the standard also involves the flow of data between business partners. The standards specify how a business with its trading partners may leverage the standards to build dynamic, flexible trading networks to enhance the inter-operational efficiency, and gain business performance.

In considering this achievement, we believe that with the aids of using XML/EDI documents and ResettaNet International Standards (2003), the tedious tasks of business message exchange through the internet and web can actually be reduced and the business performance can then be really achieved because of its characteristics of standardization to handle cross platform of data transmission, therefore. Besides, these, the security issues are always concerned to conduct the EDI over the internet by most of practitioners. In the past few years, there were many security solutions were proposed accompanying with the developing the services of conducing the EDI over internet. Among these security solutions, the ones commonly taken along with using electronic mail to transmit the business information are S/MIME (Secure/Multipurpose Internet Mail Extensions) (Ramsdell, 2001a), PGP (pretty good privacy)/MIME (Balenson, 1993; Zimmermann, 1994) and privacy enhancement protocol (PEP) for internet electronic mail (Kaliski, 1993; Linn, 1999; Kent, 1993). Hence, business EDI may be carried out on the internet with lower risk but higher efficiency.

In this research, we adopt the XML-based e-Business model (Figure 1) developed by RosettaNet Organization (RosettaNet Standards, 2004) to take the advantages of transmission comply with a standard model among business trading partners in a

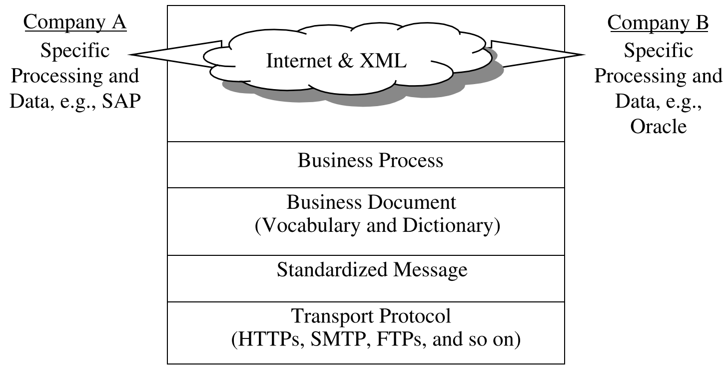

Figure 1.
XML-based e-business model

supply chain by creating a framework of common gateway service. A prototyping system based on this service framework is also implemented to examine the feasibility and effectiveness of this proposal.

Issues of business electronic data exchange

Data security

In general, there are three common categories to encode secure EDI messaging on the internet. The first one is Symmetric Key Coding System (SKCS), another one is Asymmetric Key Coding System or called as Public Key Coding System (PKCS) or commonly called as Public Key Infrastructure System or is called as PKI for short (Adams and Farrel, 1999), and the third one is Key Escrow Coding System or Key Recovery Coding System (Kaliski, 1993; Ramsdell, 2001a). Normally, two or more of the above coding systems are combined to achieve a higher level of security in data transmission.

For the security consideration of data transmission, nowadays the messaging encapsulation which is most commonly seen in practice to conduct the electronic commerce has two approaches. One is by the transmission of using e-mail with S/MIME (Ramsdel, 2001a; Crocker, 1995), which encapsulates the encrypted business documents using one of the coding systems mentioned above in an internet mail. The other one is by using web application services with HTTPS (Hypertext Transfer Protocol Security with Secure Socket Layer), which securely transfer the encrypted documents using Secure Socket Layer between user and web server. The S/MIME is the combination of MIME and the secure encoding systems of PKCS No. 1, PKCS No. 7 and PKCS No. 110 (Housley, 1999). It has been continuously revising and updating during the last couple years. The latest one released is the third version, which we call it as S/MIME V3. Its relevant major request for comments (RFCs) include RFC 2630 (Housley, 1999), RFC 2631 (Rescorla, 1999), RFC 2632 (Ramsdel, 2001a), RFC2633 (Ramsdel, 2001b), RFC2634 (Hoffman, 1999), and so on. In S/MIME V3, the X.509 method (Adams and Farrel, 1999) is adopted to be the basis of certification for users. It means through the process of certification authority (CA) that the approval, confirmation and cancellation of certificate can be effectively conducted. These RFCs are briefly described in Table I.

The hash code of RFC 2633 can be generated from MD5 (Message Digest 5) or SHA-1 accompanying with the use of Rivest-Shamir-Aleman calculation method and

Table I. A brief description of relative RFCs of S/MIME V3

RFC No.	Main themes
RFC 2630	Describes the standard methods of encryption and decryption including digital signature, signature time, signature calculation method, code key management calculation method, key agreement calculation method, key transportation calculation, etc.
RFC 2631	Describes the Diffie-Hellman calculation method
RFC 2632	Describes the S/MIME certificate handling standard. It clearly indicates that the certificate handling of S/MIME follows the standard of X.509
RFC 2633	Describes the S/MIME message format including standard hash code of sending and receiving agency program and signature confirmation
RFC 2634	This specification can be added optionally. It mainly explains four types of services including signed receipts, security labels, secure mailing lists, and signing certificates to strengthen the security level of S/MIME V3

the private key of the sender used to conduct the signature encryption for the document. As to the information encryption, RC2 (40 bits) and triple DES calculation method are used to conduct encryption of message. It means that the encryption of message script can be done by adopting RC2 or triple DES calculation method (Ramsdell, 2001b).

EDI over internet

Because traditional EDI using a private network to conduct the business data interchange has the problem of higher data transmission cost, time and restriction on geographic domain whereas the transmission of message through the internet can greatly reduce these problems, scholars and practitioners started to conduct research on how to carry out EDI overt internet when the internet brought to the attention of the public in last decade. This phenomenon was commonly called EDI over internet or called EOI for short. As far as our understanding, practically we can illustrate the transmission fee spent by using traditional EDI and EOI, respectively, which is shown as Figure 2.

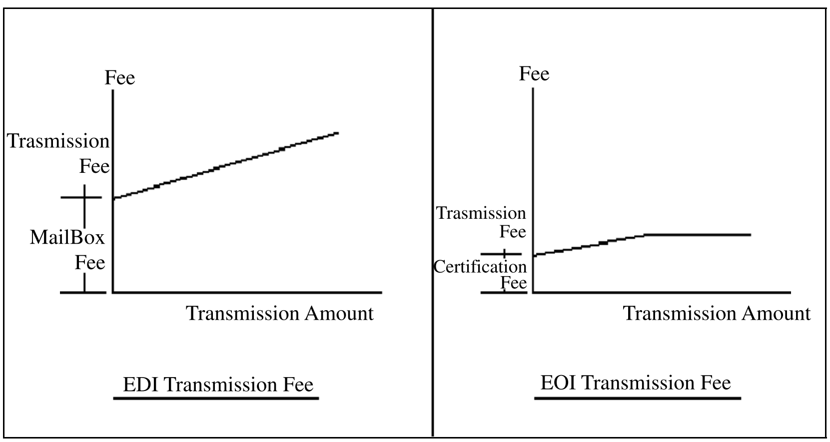

Figure 2. Comparison of transmission fee of traditional EDI and EOI

The Figure 2 shows the comparison of transmission cost of using traditional EDI and EOI, separately. This cost is only regarded as the daily operational cost for each method. At the left-hand side of Figure 2, the traditional EDI needs to rent mailbox from EDI service providers, which is traditionally called as a value-added network (VAN) center, to store and forward the trading messages exchanged over a private network among trading partners. In additions, under the use of the traditional EDI each firm needs include the fee of renting a dedicated communication line in order to establish the connection to the VAN center. Because the traditional EDI goes through an impartial third party under control by a dedicated and private network, the certification process used to certify the firm's identity is usually not necessary. Therefore, the certification fee (cf) paid for the identity certification from the CA can be omitted. Therefore, the overall operational fee (Opr fee of EDI) during a period of time paid for data transmission of adopting traditional EDI can be computed as the mailbox rental fee (mrf) plus the data transmission fee (dtf) and where the dtf is equal to the unit fee for data transmission (ufdt) multiplied by the units of data transmission (udt). Or we can express this computation in the form of equation like:

$$\text{Opr fee of EDI} = \text{mrf} + \text{dtf}, \quad \text{Where dtf} = \text{ufdt} \times \text{udt}.$$

At the right-hank side of Figure 2, it shows the daily Opr fee of using EOI. Because all trading partners may directly exchange and transmit their trading messages each other through the internet mail without being aided by an EDI services provider, therefore it may save the mrf from the EDI services provider but the firm needs to pay for the cf in order to certify the identity of trading firms and authorize the rights to trading firms before they may conduct the EDI over the internet. However, because this certification process is only performed one time before a series of transactions starts, it is counted as a fixed cost. So, the fee spent for certification is much lower than that of renting a mailbox in traditional EDI. As to the transmission fee, because EOI uses an open and sharable public network like the internet while traditional EDI uses a private and dedicated business network, EOI pays a much lower transmission fee than that is paid by using a traditional EDI as the increase of data transmitted. Today, the fee paid for the internet connection and access provided by network services providers is fixed to a firm. When the data transmission amount for business trading is low, it may have an increasing transmission fee as the data transmission increases for each unit of data transmission. While the amount of data transmission increases beyond a certain amount, the transmission fee will increase slowly to a near-flat line. Hence, the overall Opr fee (of EOI) paid for data transmission of adopting EOI can be counted as the cf plus a slowly-increasing slope of dtf. Or we can represent this fee like:

$$\text{Opr fee of EOI} = \text{cf} + \text{dtf}.$$

In summary, we can see from Figure 2 that overall daily operational fee spent of using the traditional EDI is much higher than that of using EOI for data transmission regardless the amount of daily data transmission. Therefore, from this standpoint of view of operational fee, we may always say EOI has better cost effectiveness than EDI.

In addition, according to our survey carried out to ten companies in Taiwan which had implemented the system for EDI by end of year 2002, the overall costs spent for hardware and software installation for traditional EDI and EDI over internet separately are summarized in Table II.

Cost items	Types of EDI Traditional EDI	EDI over internet
Hardware installation cost (one time charged, a fixed cost)	$2,000 to 5,000 for EDI workstations installation. (usually dedicated use)	$5,000 to 10,000 for EOI (mail or web) servers and workstations installation. Sharable with firm's other services
Software cost for EDI/EOI implementation (a fixed cost)	$2,000	$3,000
EDI translation software cost (a fixed cost)	Requires a specific conversion software to convert firm's business document into standard EDI document	Requires a specific conversion software to convert firm's business document into standard EOI document such as XML/EDI document. Usually higher than the use of traditional EDI
Maintenance cost (variable)	Low	High
Communication cost (a variable cost)	Connection establishment cost to VAN center. Dedicated use for EDI. High	Connecting establishment cost to the internet services provider. Share with firm's existing connection. Low and may be negligible

Table II.
The hardware and software cost spent by traditional EDI and EOI separately

From the data and cost figures shown in Table II, the traditional EDI seams to have the lower hardware and software installation and maintenance costs spent than those spent in EOI. Nevertheless, the hardware and software installed and used in EOI are sharable by firm's other applications, but those are dedicated to be used by the traditional EDI. In additions, the EOI has a lower communication cost, hence in the long run, it can reduce a large amount of transmission cost. Above all, we may conclude the total cost of adopting EOI is counted to be much lower than those spent for traditional EDI.

Standards of RosettaNet

RosettaNet Standards (2003) of supply chain management developed by RosettaNet Group. The standards specify how a business with its trading partners may leverage the standards to build dynamic, flexible trading networks to enhance the inter-operational efficiency, and gain new business opportunities. The RosettaNet Standard provides a common global e-business language that aligns processes between trading partners. It enables seamless and secure, real-time business-to-business transactions through system-to-system integration between customers and suppliers. One key advantage of RosettaNet is its ability to build reusable interfaces throughout an industry characterized by multiple trading partners. The standard is promoted by the organization of RosettaNet which is a non-profit consortium including more than 400 of the world's leading companies in the industries of Information Technology (IT), Electronic Components (EC), Semiconductor Manufacturing (SM), and system integration services providers joining together to implement and promote the open e-business process standards. RosettaNet Standards offer a robust nonproprietary solution, encompassing data dictionaries, implementation framework, and XML-based electronic business message scheme and process specifications, for e-business standardization. During the last decade, there are more and more practical examples which make used of this standard to build the integration of enterprise applications. Intel Information Technology White Paper (2003) demonstrates how Intel and Fujitsu use the RosettaNet Standard to exchange documents, coordinate business processes, and replace existing EDI processes with RosettaNet automation so that the customer satisfaction, business value, and competitive advantage are significantly increased between them. Arrow Electronics and National Semiconductor celebrated their announcement to create European first with the successful implementation of a RosettaNet-based system that automates the electronic exchange of key design information between them in August 2004 (Arrow Electronics News, 2004). The result is a fully automatic system for the detailed registration of design projects, which simultaneously updates in real time the data held on IT systems at Arrow and National Semiconductor. The initiation will be expected to forge strategic supplier relationships that support improvements in operating efficiencies, streamline the supply chain and, ultimately further enhance the services of Arrow Company offering to its customers.

As Table III shows, RosettaNet Standards are a layer structure which consists of three major parts which include RosettaNet Implementation Framework (RNIF), (Partner Interface Processes (PIPs), and Dictionaries (RosettaNet Standards, 2004).

The RNIF defines the RosettaNet objects and substantially explains how to transmit message between trading partners by using XML-format construction with the security implementation. It also specifies a common transport protocol and based on this protocol a commercial service can be effectively and securely conducted. The RNIF also gives the specifications of setting the agreement between trading partners before the message exchange starts and routing, packaging, and signaling during the message interchange between two firms.

The PIPs are specialized system-to-system XML-based dialogs which define business processes between trading partners; define the document exchange choreography and the XML schemas for the individual business documents involved. The purpose of each PIP is to provide common business/data models and documents enabling system developers to implement RosettaNet e-business interfaces. PIPs are organized into seven clusters, or groups of core business processes, that represent the backbone of the trading network. Each cluster is broken down into segments – cross-enterprise processes involving more than one type of trading partner. Within each segment are individual PIPs. The PIP clusters are briefly described as follows (RosettaNet Standards, 2004):

Table III.
Layer structure of RosettaNet standard

Technical and business dictionaries Message payload *Message choreography* (E.g. dialog process, retrieve, timeout, acts, etc.)	PIPs- Partner Interface Processes
RNIF (E.g. defines XML Construct, methods of security implementation, transport protocols; set the agreement between trading partners; set the routing, packaging, and signaling, etc.)	

- *Cluster 1: partner product and service review.* Allows information collection, maintenance, and distribution for the development of trading-partner profiles and product-information subscriptions.
- *Cluster 2: product information.* Enables distribution and periodic update of product and detailed design information, including product change notices and product technical specifications.
- C*luster 3: order management.* Supports full order management business area from price and delivery quoting through purchase order initiation, status reporting, and management. Order invoicing, payment and discrepancy notification also managed using this Cluster of processes.
- *Cluster 4: inventory management.* Enables inventory management, including collaboration, replenishment, price protection, reporting and allocation of constrained product.
- *Cluster 5: marketing information management*. Enables communication of marketing information, including campaign plans, lead information and design registration.
- *Cluster 6: service and support.* Provides post-sales technical support, service warranty and asset management capabilities.
- *Cluster 7: manufacturing*. Enables the exchange of design, configuration, process, quality and other manufacturing floor information to support the "Virtual Manufacturing" environment.

The dictionaries provide a common vocabulary for conducting e-business and reduce confusion in the procurement process due to each company's uniquely defined its own business terminologies and vocabularies resulting the misunderstanding during the data interchange. The RosettaNet Business Dictionaries designate the properties for defining business message between trading partners and clearly define the characteristics of both buying and selling parties of business. Moreover, the RosettaNet technical dictionaries provide properties for clearly defining products and services. By adopting the standard dictionaries, trading partners can reduce the misunderstanding generated in the trading message flow due to the use of different glossaries between different companies, thus achieving efficient and effective trading among businesses

A common gateway for secure data exchange

The system structure of common gateway

The system structure of common gateway system built in this research for securely conducting business data exchange over the internet is shown in Figure 3. The system structure is divided into four levels which consist of message transmission level, XML-based document conversion level, data storage and retrieval level, and integrated intermediary level. The complete structure with its level interrelationship is shown as Figure 3.

The function of each level in the system structure shown in Figure 3 is briefly described as follows:

- *Message transmission level.* The message transmission level defines the functional components and interfaces used to conduct the business message

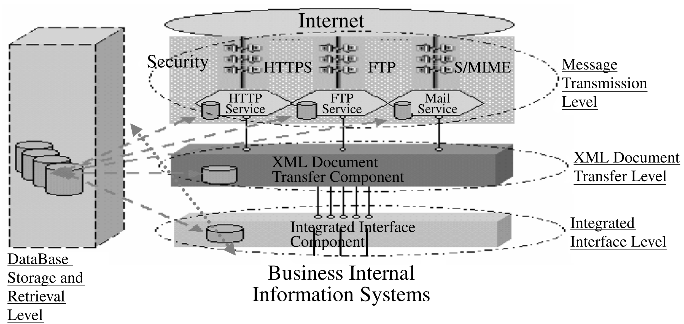

Figure 3.
The structure of common gateway system

transmission and interchange between business partners over the internet. The peer systems of trading partners may thus communicate each other by selectively using one of three message transfer services, including HTTP, FTP, and SMTP/e-mail depending upon the prior agreement which was set before proceeding to the communication. The proper security mechanism is also implemented corresponding to each message transfer service. In this research, the authors only focus on the implementation of SMTP/e-mail services with S/MIME to conduct the business message transmission and interchange. The services of HTTP and FTP can be similarly constructed by extending the implementation from the SMTP/e-mail.

- *XML document conversion level.* The XML document transfer level is implemented into three main functional components. The first component is responsible for conducting the data conversion from non-XML trading document obtained from firm's applications to XML-format document and vice versa, the second component is responsible for certifying and analyzing the accuracy of XML data format, and the third component is responsible for providing XSL style sheets for converting each XML document received from a peer trading partner into a readable screen-formatting output. The system-to-system communication is implemented to abide by the process specified in RosettaNet's PIPs.
- *Database storage and retrieval level.* This level consists of a group of protocol data storages corresponding to each transmission protocol used for transmission and an inter-level storage bank. The main purpose of these protocol data storages are used to provide the variety of data manipulation, utilization and visualization needed by different transmission protocols. The inter-level storage bank maintains different intermediary data stores for the communication purpose between two adjacent communication levels.
- *Integrated interface level.* The main purpose of this level is to interface the firm's back-end information system with the XML document transfer level by means of an intermediary data storage which is the part of database storage and retrieval level. At each side of all trading partners, two interface programs are separately installed and bounded with the XML document transfer level and the business backend information system. Through the aid of the intermediary data storage and interface programs, the trading data can be effectively transmitted

between firm's internal backend information systems and the XML document transfer level. Meanwhile, the common gateway service may be seamlessly integrated with business backend information systems such as business procurement/ordering systems.

An experiment of the system

To evaluate the effectiveness of the system developed in this research, we experiment this common gateway service by actually installing to a computer network equipment manufacturing company which bases in Taipei City, Taiwan. The company is a medium-scale company in the network equipment manufacturing industry in Taiwan. It has three main manufacturing factories separately locating in Taipei City and Hsingchu City of Taiwan and Don-Kowng City of Kwong-Don Province of China. It produces hundreds of computer-related network and communication equipments including hubs, switches, routers, cable modems, and ADSL modems, and so on. Before year 2002, the company major purchasing activities were mostly through telephone, facsimile, and generic e-mail. It also partly used a traditional EDI system to deal with some of its suppliers who had the same traditional EDI system installed. In the early of year 2002, the company started to implement an enterprise resource planning (ERP) system provided by Taiwan's local ERP software vendor. The main parts of ERP system were successfully implemented in the fall of year 2002. As the use of the internet became popular companywide, the company attempted to transfer its traditional EDI to on the internet. Therefore, the common gateway system developed by the research was introduced for experimentally used as a front-end system of its newly implemented ERP system. Figure 4 shows a simple peer-to-peer interoperable relationship between the company and its suppliers. Both the company and its suppliers can play the roles as both the sender and the receiver during the data exchange is conducted. The common gateway service is separately installed at both sides as a front-end data transmission and exchange services.

As the services of common gateway described as above sections, at the sender side, if its business backend information system has business document intend to be transmitted to its trading partner. It makes use of the common gateway service through the integrated intermediary interface level. The business document taken from business information system by the interface level will be passed to the data storage and retrieval level and stored into its prescribed data storage. Afterward, the service component of XML document conversion level corresponding to the type of each business document stored in the data storage will be activated to convert the document

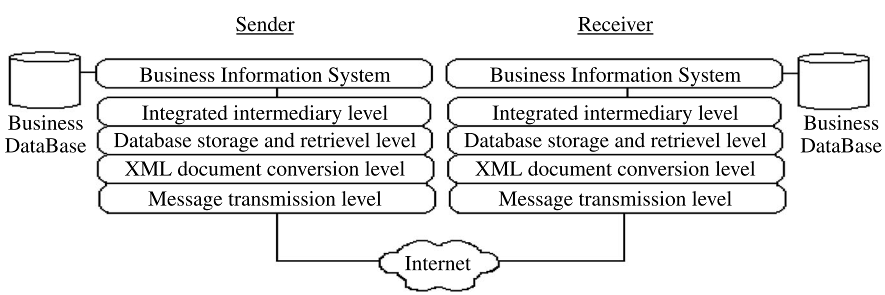

Figure 4. The peer-to-peer relationship of the common gateway

into its corresponding form in XML format specified in RosettaNet Standards. These forms are such as 3A1 (i.e. Price Inquiry Form), 3A4 (i.e. Order of Purchase Form), 2A2 (i.e. Product Data Inquiry Form), and so on. The service component of the XML document conversion level will base on the types of document to decide which types of standard form to be transformed. The message transmission level will then be activated to take the XML-format document to conduct further security installation and message encapsulation before it is transmitted out to its peer trading partner.

At the receiver side, once the XML-format message is received by the component of the message transmission level, the component will first verify the integrity of the message by a security verification procedure. If the integrity of message is successfully verified, it is then handed to the XML document conversion level to convert into a user-visible document. Regardless of the result of verification for the integrity of the message received, a return message must be returned to the sender to notify the message receiving status so that the sender can decide whether to retransmit the message or not. Before conducting the message conversion, the XML document conversion level at first needs to examine whether the message conforms to its corresponding document type definition (DTD) specified in RosettaNet Standards. If it does not conform to the DTD specified, then it will be deemed as a message of invalid and shall then be abandoned. When it conforms to its DTD, the XML document conversion level will then conduct the message conversion. After the message is converted into a user-visible document, it is then handed to the database storage and retrieval level. Subsequently, the database storage and retrieval level stores the document received into its prescribed intermediary data storage. The business back-end information system may periodically activate the integrity intermediary interface level to pick up the document stored in the data storage and pass it to the business back-end information system to process the document. The integrity intermediary interface level also may periodically and proactively scan the intermediary data storage, pickup the document, and pass it to the business back-end information system. At the receiver side, any error resulting from the message error in message conversion or cannot be recognized by the receiver's business back-end information system, an error message ought to be returned to the sender within a prescribed time period to respond the error status of message, so that the sender can understand the problem and decide whether to retransmit the message or not.

Analysis and discussion of experiment

During a six-month period of experiment, we collect the turnaround time spent on the data transmission and propagation over the internet is about 40 seconds on the average. In fact the average response time of completing a transaction forth and back may be completed within one minute. This time spent is acceptable to most users who participate in this according to our survey to the company's and supplier's major users.

Furthermore, each supplier uses a dedicated line such as ADSL (512 Kbps downlink/64 Kps uplink) or T1 (1.544 Mbps) connecting to the company through its internet services providers to form a supply chain network for data exchange. Because each supplier only shares partial bandwidth from its existing internet connection for business data exchange, the cost of using the communication line for data transmission can thus be negligible, but this cost needs to be counted under the use of traditional

EDI since a dedicated line s used. Meanwhile, traditional EDI also needs pay an additional fee around US $150 per month to pay for renting the EDI mailbox from the EDI services center for message store, management, and delivery. Therefore, it is apparently seen that the cost for transmitting data over the internet using a common gateway is much lower than the traditional EDI.

Although the use of traditional EDI has the cost advantage of hardware and software installation and maintenance costs shown in Table II, in the contrary it needs pay more for its variable costs of renting a dedicated transmission line and for the services of VAN center. Taken as a whole, in the long run, the use of EDI over internet has much more advantages over the use of traditional EDI.

Conclusion

This paper presents a lower cost and high security of common gateway services for business data exchange between trading firms in a supply chain system. The system is built intending to meet the four security principles of electronic business in the aspects of identity confirmation, privacy, accuracy and non-repudiation. At the same time, the RosettaNet Standards specification is adopted as a major basis to build this common gateway service system. Through an actual implementation in a company's purchasing and ordering system, it can prove that the cost spent and benefits gained from conducting EDI over the internet leveraging the common gateway presented in this paper is much lower than that of employing traditional EDI. In additions, according our experiment, the results show that the use of the XML/EDI format electronic business model specified in RosettaNet Standards to implement the system can be easier to achieve higher effectiveness and security to conduct the electronic business under this information age. The result of this research also can provide a valuable referential model for a firm to create a similar supply chain system with its trading partners under this era of digital economy.

References

Adams, C. and Farrel, S. (1999), "Internet X.509 public key infrastructure certificate management protocols", RFC1421 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Arrow Electronics News (2004), "European first for RosettaNet implementation", Arrow Electronics (UK), available at: www.electronicstalk.com/news/arr/arr145.html/ (accessed 30 August)

Bakos, J.Y. (1991), "Information links and electronic marketplaces: the role of inter-organizational information systems in vertical markets", *Journal of Management Information Systems*, Vol. 8 No. 2, pp. 31-52.

Balenson, D. (1993), "Privacy enhancement for internet electronic mail. Part III: algorithms, modes, and identifiers", RFC1423 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Crocker, D. (1995), "MIME encapsulation of EDI objects", RFC1767 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Hoffman, P. (1999) Enhanced Security Services for S/MIME, RFC2634 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Housley, R. (1999), "PKCS#7: cryptographic message syntax", RFC2630 of Internet Engineering Task Force (IETF), RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Intel Information Technology White Paper (2003), "Collaborative RosettaNet implementation", available at: www.intel.com/techtrends/trends/rosettanet/implementation.pdf

Kaliski, B. (1993), "Privacy enhancement for internet electronic mail. Part IV: key certification and related services", RFC1424 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Kent, S. (1993), "Privacy enhancement for internet electronic mail. Part II: certificate-based key management", RFC1422 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Linn, J. (1999), "Privacy enhancement for internet electronic mail. Part I: message encryption and authentication procedures", RFC1421 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Ramsdell, B. (2001a), "S/MIME Version 3 certificate handling", RFC2632 of IETF RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Ramsdell, B. (2001b), "S/MIME Version 3 message specification", RFC2633 of IETF RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

Rescorla, E. (1999), "Diffie-Hellman key agreement method", RFC2631 of IETF, RFC-Editor RFC Document Database, available at: www.ietf.org/rfc.html/

RosettaNet Standards (2003), "RosettaNet overview", available at: http://xml.coverpages.org/RosettaNet.html

RosettaNet Standards (2004), "Technical reports: RosettaNet", available at: http://xml.coverpages.org/RosettaNet.html

Supply-Chain Council (2002), "SCOR overview", available at: http://supply-chain.nidhog.com/default.htm/

Voss, C.A., Ahlstrom, P. and Blackmon, K. (1997), "Benchmarking and operational performance: some empirical results", *International Journal of Operations & Production Management*, Vol. 17 No. 10, pp. 1046-58.

Webber, D. (1998), "Introducing XML/EDI frameworks", *Electronic Markets*, Vol. 8 No. 1, pp. 38-41.

Whyte, W.S. (2001), *Enabling eBusiness – Integrating Technologies Architectures & Applications*, Wiley, New York, NY.

XML/EDI Group (2003), "Introduction to XML/EDI", available at: www.xmledi-group.org/xmledigroup/xmledigroup.htm/

Zimmermann, P. (1994), *PGP User's Guide*, Massachusetts Institute of Technology, Cambridge, MA.

Further reading

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

About the authors

Ruey-Kei Chiu is an Associate Professor of Department of Information Management, Fu Jen Catholic University in Taiwan. He received his first master degree in computer science from Brigham Young University, Provo, Utah, USA, his second master degree in computer science and PhD degree in management science from the University of Iowa, Iowa City, Iowa, USA.

He has conducted a long-term research on Healthcare and Medical Informatics since 1994. Since, then, he has guided a research group to assist the Department of Health and Center of Disease Control of Taiwan's Government to conduct the implementation of advanced and innovative information technologies. His research interests are in the areas of healthcare and medical informatics, supply chain management with performance evaluation especially in the areas of building data warehousing systems, decision support systems, and electronic data interchange systems to effectively enhance the business value of supply chain.

Shiao-Ping Yu, once was a scientific researcher of SCM/ERP research group at the Department of Information Management of Fu Jen Catholic University in Taiwan from year 2000 to 2003. Currently he is working for Taiwan government's custom as a computer engineer to aid the organization to innovate its legacy EDI systems which have run for ten years. He holds a master degree in information management from the Department of Information Management of Fu Jen Catholic University. His research interests are in the area of supply chain management, electronic data interchange, decision support systems for public organization sectors. Shiao-Ping Yu is the corresponding author and can be contacted at: yu@im.fju.edu.tw

S.C. Lenny Koh BEng (Hons), PhD, MIEE, MCMI, MIOM, is a Deputy Director of MBA in EcoBusiness and a Lecturer in Quantitative Methods and Management at the University of Sheffield, Management School, UK. Her research interests are in the areas of production planning and control (particularly in MRP, MRPII and ERP), uncertainty management, modern operations management, logistics and supply chain management, e-business, e-organisations and sustainable manufacturing. She has published widely in various international and national academic journals and conferences. She is the Associate Editor of the *International Journal of Operational Research*, an editorial board member of the *International Journal of Logistics Systems and Management* and *Benchmarking: An International Journal*, serves as a chair and on the board of committee of various international conferences, and a referee for several international journals in these disciplines.