B2B in using the Dynamic E-Commerce Trading Architecture that integrates XML and SET ---with Taiwan for example

Heng Ma, Chin-Yang Tai, and **Wei-Neng Hsu**

Department of Industrial Engineering and Management
Chung-Hua University
Taiwan
E-mail: tai@chu.edu.tw

Abstract

With the rapid development of Internet and the advanced technologies, the Internet becomes the most important of information and marketing propagation media up to the present time. The application of Electronic Commerce is not only increasing the convenience of purchasing, but also bringing about corporate competitive advantages. The key factors of doing business on the Internet are trust and security. Through the digital certificate signing from certifying authority, the regulations of electronic signature made e-commerce transaction legal. And the two major security mechanisms used are Secure Socket Layer (SSL) and Secure Electronic Transaction (SET).

Electronic Data Interchange (EDI) was introduced to manage many business operations, such as storage, delivery, and payment. But due to the high costs of applying EDI, more time and human effort are required, and complexity of data interchange standards, we suggest replacing EDI with XML, which is more user-friendly and costs less. Using XML to integrate the e-commerce application among corporations and adapting the ring model to handle the different business needs.

1 Introduction

1.1 Study Background

According to the investigation of E-commerce application promotion center in "The Present Internet Application Condition of 2000 Top Enterprises in Taiwan area", it shows that the network on-line popularity of the internal top enterprises reach 95.6%; in

the on-line network enterprises, 42.8% of the staffs had more than three years on-line experience. As for the specific industry, network linking popularity in the service industry has begun earlier, while the rest industry is the financial industry and manufacturing industry orderly; but, along with the growing importance and popularity of internet application, such as E-commerce and the network bank etc., the manufacturing industry and finance industry are also rising and following closely behind, and we can learn this from the proportion of specific industry enterprises with the network linking within these two or three years. Manufacturing industry occupies 31%, finance industry occupies 27% and service industry occupies 21%.

With the rapid development of Internet, enterprises market is no longer restricted to some certain area. Through website construction, the customers from any place of the world can browse in the enterprises website at any time to choose the commodities goods or services that is needed; the development of Internet is not only the scientific revolution but also an intense commercial competitiveness. In 1997, World Commerce Conference shows that Electronic Commerce, EC is the electronic accomplishment of the entire trading activities, its range covers: each business transaction party, who executes his trading through electronic trading method, not any kind of commercial trading through direct face to face trading or the trading in the presence of the relevant parties, such as commodities trade, service, advertisement, information providing, financial trade, market information etc., that is to integrate the financial flow, logistics and the flow of information and accomplish the traditional trading mode with electronic transmit method through Internet. In E-Commerce trading, the most familiar trading is the Business to Business, B to B, B2B trading and Business to Customer, B to C, B2C trade).

1.2 Study Motivation

According to the prediction of Forrester Research, current global E-Commerce total value is approximated to 57 billions US Dollars and in the year of 2004, the global electronic commerce total value will substantially increase approximately to 6.8 trillion US Dollars and from this, we can foresee that there will be a large number of enterprises joining in the Internet E-Commerce Trading in the future. According to the survey of 2000 large enterprises made by domestic The Economist Magazine in the end of year 2000, it shows that enterprises think that the key factors to success in the Electronic Commerce application are arranged as follow according to its importance order:

And now the e-commerce relevant application of enterprises industry is still in the initial stage, and there are still more than 70% of enterprises that still have not constructed E commerce system. The main reason is because enterprises still somewhat doubt about the security of trade information and enterprises generally think that if the E-commerce is to be successful, it has to have safe and authentic network trading environment as its first and foremost condition.

1.3 Study procedures

The study procedures executed in this paper are as shown in Figure 1.

1.4 Electronic Signatures Law

Network trade is executed through

electronic records; therefore, during network information sending, the confirmation message about sender's status and the request to check on whether information content has been changed will be produced to avoid disclamation or denial happening after the trade. So the status identification mechanism of "Digital Signatures" has become more and more important.

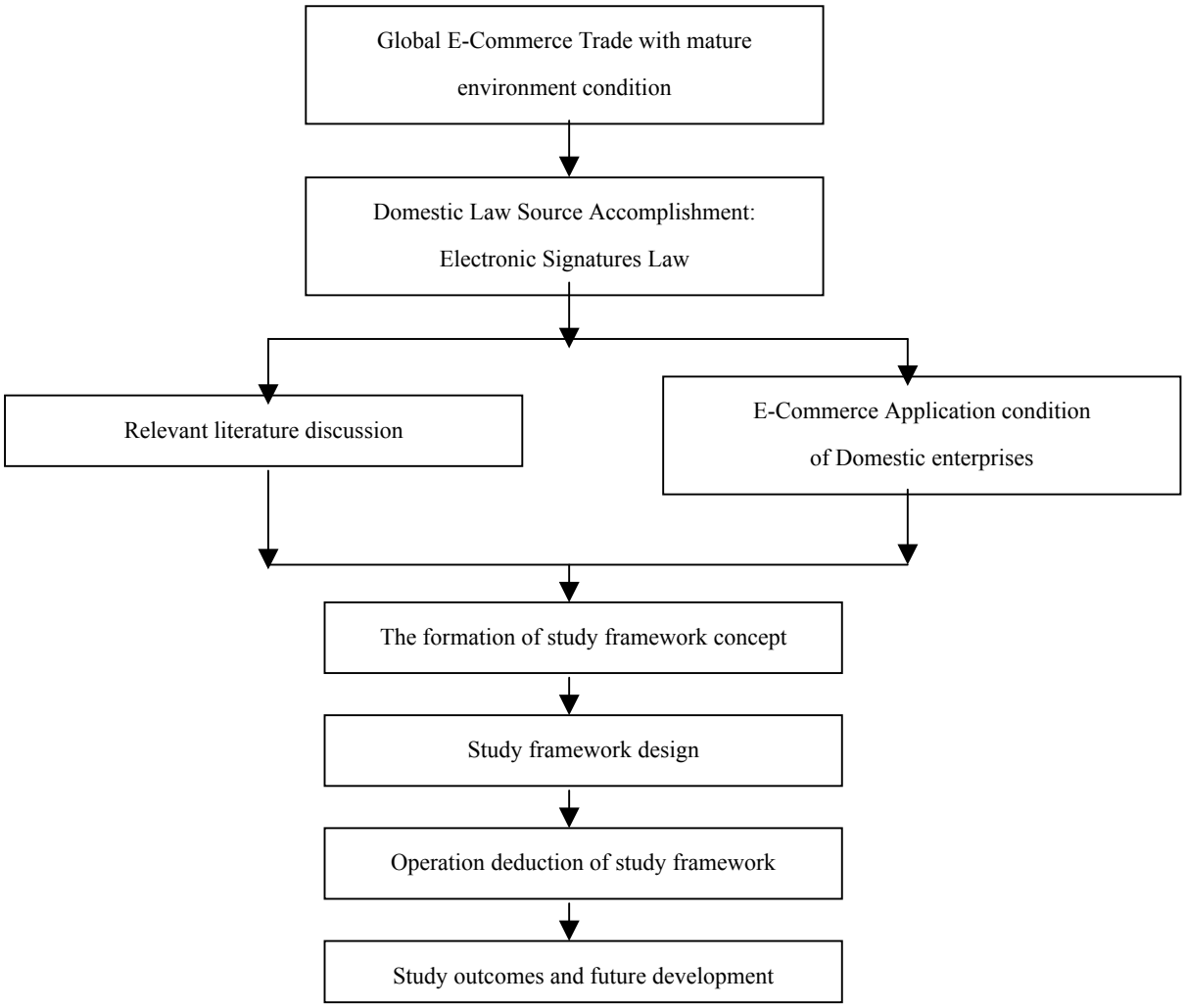

Global E-Commerce Trade with mature environment condition
Domestic Law Source Accomplishment: Electronic Signatures Law
Relevant literature discussion
E-Commerce Application condition of Domestic enterprises
The formation of study framework concept
Study framework design
Operation deduction of study framework
Study outcomes and future development

Figure 1.

To operate in coordination with the increasing vigorous development of digital economy activity, each country in the world are making efforts in promoting the relevant legislation work of electronic signatures to establish safe and authentic E-commerce environment, and application popularity of E-commerce, such as Germany (August of 1997), Malaysia (1997), Italy (March of 1997), Singapore (August of 1998), Korea (July of 1999), Hong Kong (January of 2000), Japan (May of 2000), United States (June of 2000), each member of European Union has completed the relevant law criterion of electronic Signatures Law (before the July of 2001).

To establish the security and credible network environment, our government ensures the information during network transmission cannot be easily counterfeited, altered or stolen, and the status of both trading parties can be distinguished, and this can also prevent the parties from denying the fact of the accomplished trade. To promote the safe electronic transaction system, government and the enterprises in the non-government circles make every effort in using modern cryptographic technology to establish each digital certificate system, to provide status certification and trade certification services, to promote users' confidence and the universal application of electronic trade. To ensure the security of electronic trade and to promote the development of electronic government and electronic commerce, the President proclaimed the full text of Electronic Signatures Law on November 14th, 2001 and is executed on April 1st, 2002. The passing of Electronic Signatures Law, it is for the definition of Electronic Signatures and to normalize its law efficiency, and to extend the handwriting signature in the past into electronic signatures and to normalize the essential condition that the certificate providing service unit should have in providing the basic electronic trade security.

2 Literature discussion

2.1 The brief introduction of Cryptology (Symmetric Cryptosystem, Asym-metric Cryptosystem)

In the Electronic Commerce system, trade security is the most important factor to prevent a third party from intercepting, and knowing the data that is transmitted through network. Under many conditions, the information encryption is the only measure to assure the information confidentiality. An encryption procedure is based on certain mathematical calculation that combines the common data (Plain text) with a succession of number (key) to generate the Cipher Text that is incomprehensible by other people. So even if a third party intercepts the data (Cipher Text), he is unable to change it into plain text because he does not have the key. Therefore, it assures the confidentiality and security of the information, while the receiver can restore the Cipher Text into Plain Text through the correct key. And each kind of the mechanism of the Cryptology is mainly used to provide four kinds of requests that are needed by information security: that are 1. Status identification, during communication, both parties can ascertain the status of the other party; 2. Data confidentiality, to ensure the content of data is not known by a third party during the data transmittance process; 3. Correct data, this can let receiver assure that the data transmitted through network has not been altered by a third person; 4. Non-repudiability, when a controversial issue is happening in the future, sender or receiver

should have been able to submit the certificate of this data transmittance procedure. According to the key properties, the encryption calculation can be divided into Symmetric Cryptosystem and Asymmetric Cryptosystem.

2.2 Secure mechanism of E-Commerce Trading (SSL, SET, Non-SET)

To execute commercial trade on the Internet, the most important is the security problem. At the present day, there are three most familiar electronic commerce secure trade protocols, the first is SSL (Secure Socket Layer), the second is SET (Secure Electronic Transaction), and furthermore, the last one is Non-SET, the one that is more suitable for financial industry.

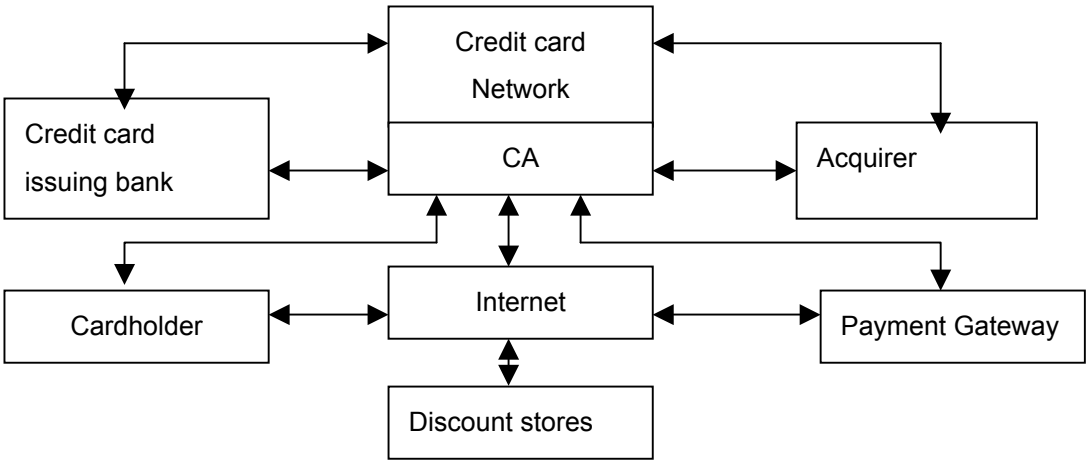
SSL is developed by Netscape, and it is the specifications that is used to protect the trade security during using browser on the network. Since its function is supported by each browser, it is the protocol that is most widely used on network. The information that is transmitted by SSL is encrypted with the key and although a third party may be able to intercept the information, it will be hard to read the information content, and the completeness of encrypted information can be maintained and will not be altered or damaged. Therefore, SSL has the function of data encryption, status identification, data checking, etc. But there are still some problems to overcome, such as: the deficient in certification mechanism, it is unable to confirm whether the consumer is the cardholder, stores and acquirer are in lack of standard transmittance interface, the data integration is hard to do, credit card data is transmitted to stores hence the information may be used illegally by the stores.

In the commercial trade that is executed on network, the most important factor will be the insecurity. Since the payment method of customers on the network during trading are always using the credit card to pay the bill directly. In this moment, the data with confidentiality such as credit card number, and password will be easily intercepted by other intended people and consumer's credit card will be furthered used for theft if it is not adequately security protected. To let consumer feel at ease in using credit cards, Visa, Master card, Netscape and Microsoft, etc. jointly originate a kind of secure trade mechanism – SET. The first version of SET was publicized in January of 1996, and the last confirmed SET specification was publicized in May of 1997.

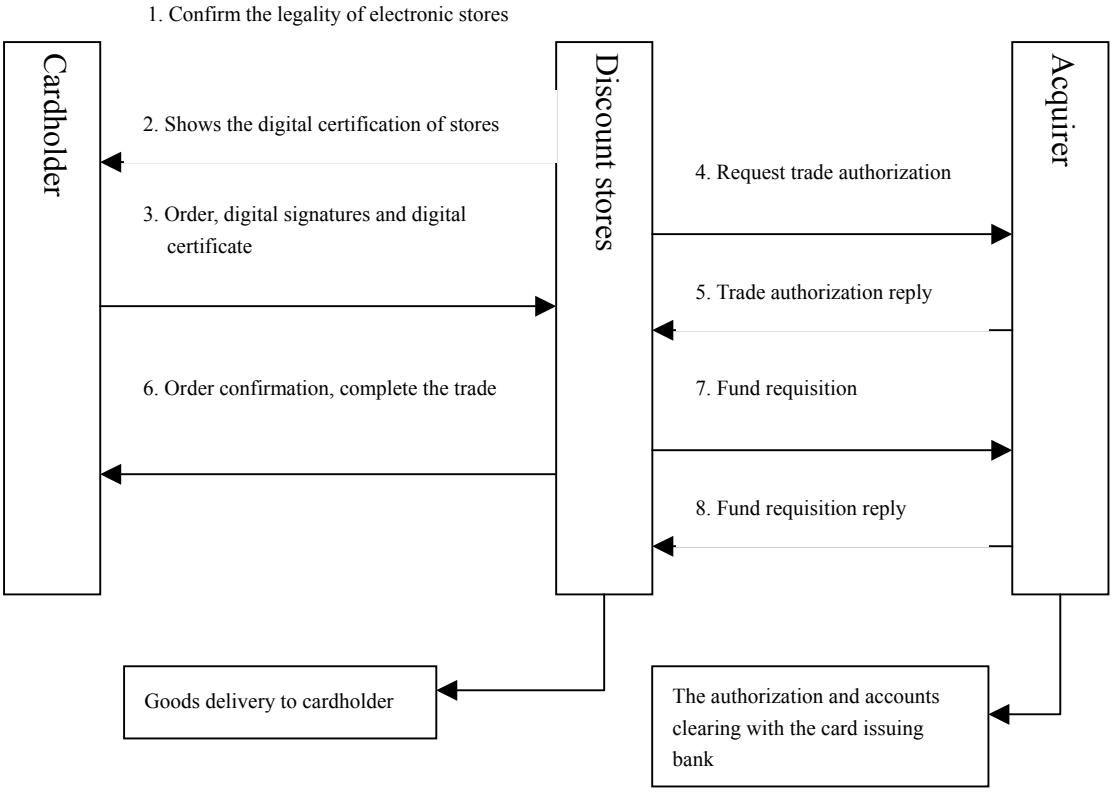
SET is an Internet secure electronic payment protocol that is with credit card as basis, and its purpose is to transfer the trading method of credit card at stores to computers. In the SET mechanism, a complete on-line shopping trade includes request, status identification, debit authorization, and payment acquirement and trading condition inquiries. Through the above-mentioned mechanisms, it can let consumer, network stores and bank feel at ease to execute electronic commerce activities on the network. At present, SET trade mode will involve the individuality including (see the figure below): credit card holder, discount stores, acquirer, credit card issuing bank, Certificate Authority, CA.

Since the SET specifications is very complicated, financial company develop a new "Non-SET network bank certification system" separately in accordance with the authorization requirements of some banks. The certification function that is provided by Non-SET network banks certificate system can also satisfy the certification requirements of order on network of Taiwan

Stock Exchange at the same time.



SET Trade Flow path



As for the differences between SSL, SET and Non-SET (see the table below), the main difference is that SSL is a kind of secure technology standard. Since it by no means force the user end to carry out status certification, it is easily developed into a kind of mechanism that is commonly used. It is commonly used as the certification of server on network and as the encryption of on-line data transmittance. In the initial stage of E-commerce, most of the shops are using this method to implement the security protection.

In the aspect of trade secure mechanism, after the consumer's application has completed, no matter it is SET or Non-SET, the certification mechanism will issue the digital certificate that is called the private key and as for the bank, it will have the public key. So when a consumer is implementing the trade, it should operate the private key and public key in coordination before he is able to enter the account. Since during making digital certification, consumer has to input random codes that reach 40 (orders) bytes, and then the password is set; with the type of private key that is floppy disk or IC card, hackers will not be able to produce the same private key and is unable to hack the account as long as the private key is properly kept.

	SLL	SET	Non-SET
Digital Signatures	None, during information transmittance, it only confirms the message source in accordance with encryption and decryption. The message itself does not have digital signatures; the authority of responsibility is not defined.	Yes	Yes
Digital Certification	None	Yes (Network account)	Yes (Identification Number)
Certification mechanism	None	TAIWAN-CA.COM Inc.	TAIWAN-CA.COM Inc.
Term of certification	None	One year	One year
Certificate fee	None	Has not yet determined	Has not yet determined
Non-Repudiability	None	Yes	Yes

2.3 Supply Chain Management (Supply Chain Management, SCM)

Supply chain management, SCM is a set of commercial policies that "provides the biggest benefit for the consumers or clients with the minimum supply chain cost through the close cooperation with business partner".

The purpose of supply chain management in a word is to let enterprises can effectively manage their suppliers information, orders, contracts, payment method, quality control, product data, product research and development, sample, product catalogue and product prices and finally conclude a transaction. And through the predominance of network science and technology, SCM system can connect the suppliers and ordering dealer that are not originally familiar and with each different geographical features and different culture background, language, and currency, to effectively cut down the trading time, space, distance and trade cost of the both parties.

2.4 Electronic Data Interchange (EDI)

The basic concept of Electronic Data Interchange (EDI) is: firstly, determine the form of data. Enterprises use the standard form to interchange electronic files between them through network and the files are directly transmitted from the computer system of the information sender to the receiver's computer system. The receiver's computer system will automatically process the data through the application of the appropriate information system and the entire process does not need the interference of mails, facsimiles communication or manual interference. The basic principal part of EDI is determined by fixed data form, and these data forms are defined by Organization of Standards, such as ANSI (American National Standards Institute) and UN/EDIFACT etc. Except for the defined data field, field order and field length, data form also includes the commercial rules (rules of data processing). In general, the steps leading into EDI are as below: Two enterprises that want to execute data interchange should come to an agreement.

1. Two enterprises that want to execute data interchange choose the added value network in common.
2. Buy or construct software system and transform the original data form into EDI form and the data form of the other party.
3. If there is another new enterprise joining in, the above-mentioned steps have to be repeated once again.

After completing each of the steps mentioned above, the operation of actual EDI data interchange will then begin; while the entire data interchange process should need three main essential factors to complete: that are Standards, Translation and Transmission Media.

The main advantages of EDI are: common standards for industry field, the defined management procedures, standard publicized, data interchange environment with security and legality, that it can bring benefits to the introducer industry has been proved, the benefits include: decreasing trade flow path error, reducing the cost of paper operation, shortening the time needed for trade completion, increasing the data cognizance degree of business operator that can be contributive to policy making and indirectly increase the finance flow rate.

While the EDI restriction and deficiency can be mainly categorized as below: the standard establishment is slow, multi-standard, the alteration of standard version involves the changes of the system, EDI

application cost is too high and is unable to attract small sized manufacturers, the application consumes too much time and the effect towards the available system is too big, fixed commercial flow path is in lack of flexibility.

2.5 Extensible Markup Language, XML

Extensible Markup Language, XML is a kind of language form and statement that can make the documents easily readable by people and at the same time, easily identifiable by the computer program. It has been recommended as the recommended specifications by the "Global Information Network Organization of Standards"in the February of 1998. XML is able to let homepage programmer construct his own tag and provide more hyperlink functions and more perfect hyperlink functions, including the files content that can be directed to multi-document or be dynamically embedded into the linking homepage, etc.

The properties of XML can be briefly described as below:

- XML is the language that is used to construct and describe the structured data markup language.
- The form that is not related to data.
- Open up to public access, it can let public read the data form and it looks like HTML.
- It can prevent the browser or other intermediate software from adding certain HTML tag by itself.
- With extensibility and is not like the HTML with fixed form.
- Be contributive to the data transmittance between server, browser, and applied program.
- Through DTD (Document Type Definition) establishment, it can be used to define the relevant language of other domains (such as figures, chemical, music etc.).
- XML is the subclass that is produced by SGML as the result of WEB optimization.
- XML allows the option and the tag of identification document form on Web.
- XML is the architecture that writes the structured document in the form of tag.
- XML can establish the statement or rules of markup language by itself.
- XML is used to describe data, and its key point is consisted in the organization of data content. And HTML is used to present the data and the key point is the presentation method on the browser.

2.6 Ring Architecture Model

In 2001, from the theory of Ring Architecture Model, Insoo Khil, Jiseon Kim, Ingoo Han and Jaecheol Ryou had submitted that electronic commerce could actually be taken as a succession of transmittance and interchanges of electronic items, such as the purchase order, contract, electronic products, payment, and receipt and etc. Electronic transmittance operation involves the asynchronous dispatch and receiving of some items so the secure standard establishment should be considered. Except for the consideration of trade security, how to ensure that each participant obtains his own requirement through the electronic transmittance method of fair trade is also the important topic for discussion. On the whole, fair trade includes six demands below: effectiveness, fairness, timeliness, Non-Repudiability, trade can be proved by TTP (Trust Third Party), and trade can be recovered through TTP.

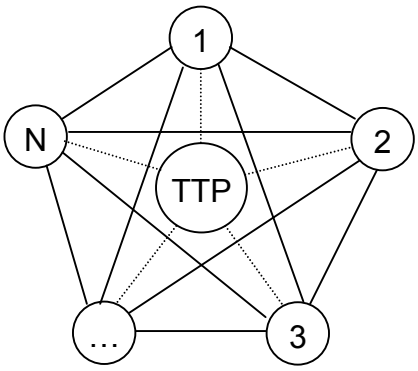
Since the traditional fully meshed model

involves too much information transmittance during trading, it makes the electronic trade have to execute repeated trade or cancel trade etc. because of the influence of exceptional condition, and the procedures of recovery operation are too inextricable and complicated, which result in the waste of resources. Therefore, to correct the shortcomings of fully meshed model and improve the whole effectiveness of multi-direction electronic trade, this ring architecture model is submitted as the improving program. The entire ring architecture model should be composed by trade participants, and it is the temporary cooperation architecture and also can be changed according to the different needs of enterprises. Ring Architecture Model contains a Trust Third Party (TTP) and N number of trade participants. Each trade participant is given a fixed serial number order, and TTP is decided by each trade participant through agreement and the linkage with each participant is starting from the participant number one (initiator). Although there is no direct contact, the trade in the ring architecture model is the same as the trade in meshed model. It can communicate with each participant. Each participant takes or consigns the communication information of his own needs in the flow of trade information.

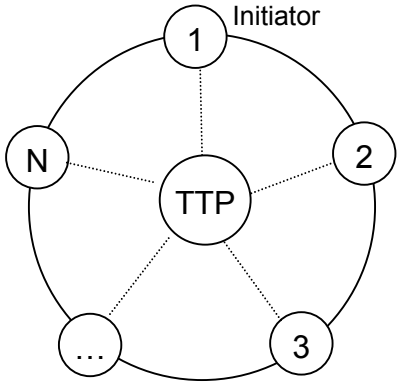
3. Study Model Establishment

3.1 The dynamic trade architecture concept that integrates SET and XML

Since the fund amount of E-commerce trading between manufacturers is larger, the trade security needed will also be more conscientious and careful; besides, whether the trade between upstream manufacturer and downstream manufacturer is successful or not, it will also have the decisive effect to its commercial credit. Therefore, the B2B electronic commerce trade standard between manufacturers should normalize the Non-repudiability of its trade. Although current SSL is more popular due to its convenience in application, enterprises should take the risk that the other party does not admit the trade after receiving order. And SET provides the status identification of both parties for cardholding enterprise and discount stores in advance before contract execution. This can ensure the money paying method of the both trading parties, such as the actual trading method in the market of today Authorization procedures utilize the electronic form to identify the status, such as digital certificate that Visa member banks issue to cardholding enterprises and discount stores. SET also uses public key encryption technology to protect the individual privacy



Fully Meshed Model



Ring Architecture Model

or the privacy of financial institution. Through SET, enterprises card data will be protected during the transmittance to financial institution. At present, there are two main kinds of method in the electronic data interchange between enterprises; that is EDI and XML. However, since the standard of EDI is complicated, the fixed cost of the application is too high and it has larger effect towards the available system of enterprise and etc, these factors make the actual implementations of EDI be considerably difficult. At present, each circle recommends to use XML instead of EDI as the electronic data interchange method.

In May of 2001, through the cooperation of the Organization for the Advancement of Structured Information Standards (OASIS) and United Nation Centre for Trade Facilitation and Electronic Business (UN/CEFACT), and the participation of each large units and organizations, the "ebXML standard" is issued as the new index of industry field. The new ebXML standard includes the technology architecture, the specifications of commercial flow path, registration service and information interchange and etc. It replaces Electronic Data Interchange with on-line trade as the leading and establishes the open, coordination, the standard for providing the intercommunication of heterogonous networks. And the enterprises can directly interchange the information between them. It lets the industry of different field determine its own XML standard and vocabularies and can further executing the trade and data interchange on the network. And through the assistance of ebXML standard, enterprises can also adopt the cheaper XML software architecture with more flexibility and reduce the cost of enterprise.

3.2 The dynamic trade architecture design that integrates SET and XML

Since the amount of one single trade of manufacture industry is large, it is significantly inapplicable to SSL trade mechanism and it needs the SET with stricter certification mechanism to be the trade standard to assure the non-repudiability of the trade. Furthermore, since there are numerous of small and medium enterprises in Taiwan, using traditional EDI to be its electronic data interchange method will cause heavy burden to the capitalized cost of the small and medium enterprises. After application, the impact that it causes on the original system of enterprises is also bigger and there is a certain difficulty in implementation. Therefore, the ebXML with cheaper construction cost, easily programmed, and rich meaning expression is adopted to be the electronic data interchange mechanism. In addition, there is consideration key point such as goods delivery term, payment time limit, and stock control, etc. existing in between the manufacture industry and upstream, downstream stores, so to look after the rights and interests of both side, Ring Architecture Model can provide a fair electronic commerce environment, which let the payment of funds and the receipt acquiring can be executed synchronously.

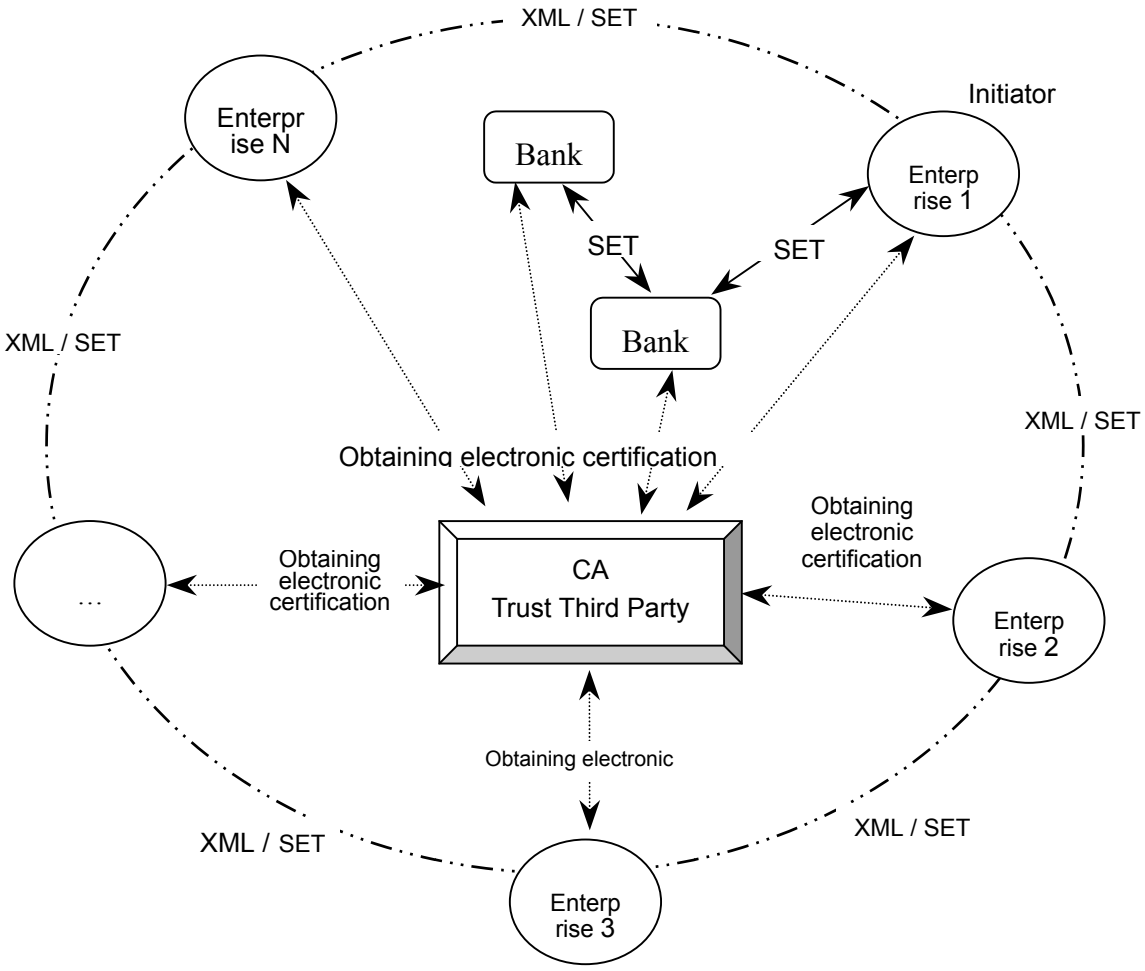
Integrating each point of consideration that is mentioned above, this study recommend to use the XML method as electronic data interchange standard and apply SET electronic transaction standards to integrate the upstream, middle stream, downstream stores with Ring Architecture Model, and regarding the trade requirements of enterprises, to dynamically find certain manufacturers to participate in the trade

activity, and form the dynamic trade architecture that integrates SET and XML (as shown in the figure below).

The characteristics of this architecture are:

1. The guarantee of trade fairness
2. Virtual trade network architecture
3. Conscientious and careful authentication process
4. Low application cost
5. Trade non-repudiability

The dynamic E-commerce trade architecture model that integrates XML and SET



3.3 The dynamic trade architecture operation description that integrates SET and XML

The upstream, downstream dealers of manufacturer industry transmit electronic commerce documents such as price estimation sheet, order sheet, funds requisition sheet, receipt, products delivery details and etc through XML. In the XML, each document and each element is regarded as an object and it can be defined and tagged according to the enterprise needs. And the link in XML is applied to add the relationship between two or more data objects in expanding the expression content of the document.

After the common consensus between enterprises has been achieved, the SET trade flow path is as following by way of the trade execution of SET electronic commerce trading mechanism.

1. First, the enterprises that are participated in the network trade should obtain the digital certificate from the Certificate Authority, or contact its card issuing bank in advance, complete the registration procedures and obtain the Digital Certificate and Electronic Wallet.

2. Upstream manufacturer will transmit the order of downstream manufacturers to the electronic wallet of downstream manufacturers through secure transmittance method.

3. If the downstream manufacturers confirm this trade in the electronic wallet, electronic wallet will sign it with its digital certificate, and then transmit the credit card data to the on-line trade system of upstream manufacturers through the encryption method.

4. The on-line trade system will send this encrypted credit card data and the signature of digital certificate of upstream manufacturer to payment gateway for further process.

5. After payment gateway receives the trading data, it will forward the data to acquirer (the bank of upstream manufacturer). Acquirer will request the credit card issuing bank (the bank downstream manufacturer) to transfer accounts.

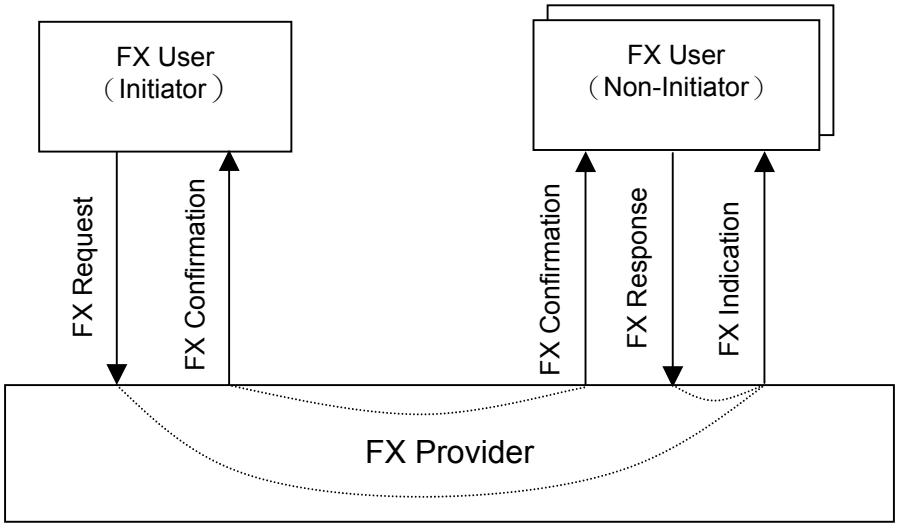
6. At last, the acquirer will send the information whether the accounts transfer is successful or not to payment gate. Payment gate will then transmit this information to upstream manufacturer through Internet. Then upstream manufacturer will reply to the downstream manufacturer through XML, and at the same time, inform the downstream manufacturer of the relevant affairs of stocks delivery. No matter whether the trade is successful or not, the on-line trade system of upstream manufacturer and the electronic wallet of downstream manufacturer will keep this trading record.

In the dynamic trade architecture that integrates SET and XML, the most important characteristics consist in the integration of upstream, middle stream, and downstream manufacturer into one system. When the enterprise has trading needs, it will then send out demand on the trade network as initiator and send it to other manufacturers according to their order. The information needed will be taken by each manufacturers itself and by using the public key, each manufacturer can only get its own information that is given by the initiator but is unable to read the

information for other manufacturers. In addition, this architecture is generated in the answer of enterprises trade needs, so when enterprises have different needs of trade, the enterprises that participate in the trading combination will change accordingly. And the vertical integration with its own relevant industry or the horizontal cooperation relationship with other industries will be achieved and forms the virtual enterprise integration effects. With the rapid widespread of Internet, the enterprises domain is also spreading unlimitedly.

In the communication protocol of dynamic trade architecture, a fair-trade agreement performs the fair trade services to support the trade execution of each party (as shown in the figure below). To assure the fairness and the security of trade execution, multi direction fair trade includes some services mentioned below:

- FX Request — Fair trade demand is initiated by initiator, all of the information related to the trade executes its individual communication through the different protocols (such as HTTP (Hypertext Transmission Protocol), FTP (File Transfer Protocol), or Email).
- FX Indication — The trade provider sends out the trade indication to each participant in the dynamic trade architecture other than the initiator to inform each party to start carrying out the trade and waits for the trade response message.
- FX Response — Each participant that receives the trade indication send out the reply and the trade reply contains two kinds of reply, that is “Agree” or “Disagree”.
- FX Confirmation — The trade final result is informed by trade platform protocol and the trade result confirmation may be “Aborted”, “Failed” or “Success”.



FX Communication Protocol may have some message classifications as below: Normal message, Abort Message, Complaint Message, Retry Message, Retry Ack

Message, Retry Nack Message, Affidavit Message.

4. Study Model Implementation Example

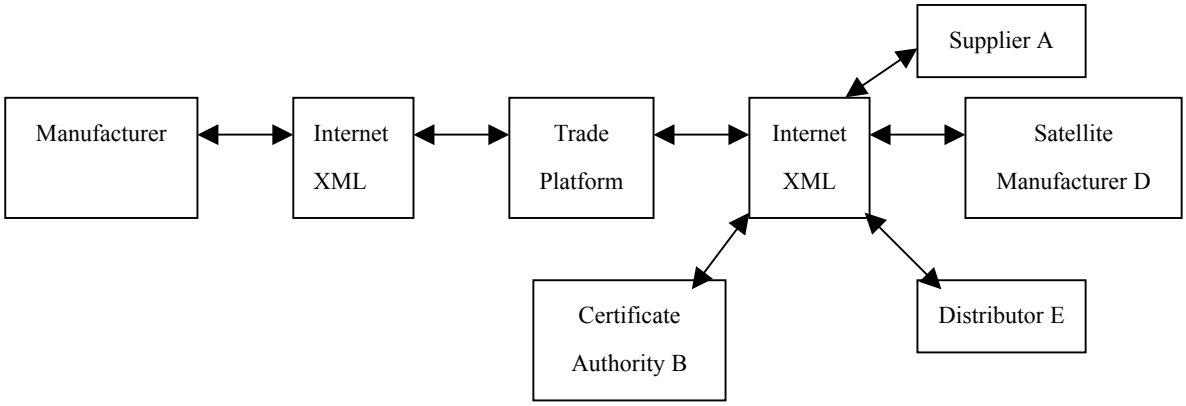
During executing the dynamic trade architecture that integrates of SET and XML, it can be described respectively through each section listed below. We make assumption that there is a manufacturer C, and its upstream supplier A, Certificate Authority B, cooperation satellite manufacturer D, and other downstream dealers, the marketing channel dealer E, F for example to explain the operation model of each manufacturer under the dynamic trade architecture that integrates SET and XML.

4.1 XML document form establishment and information interchange

From the description of each section mentioned above, we know that using the XML with adoptable open platform, the user can define his own document language control tag in accordance to the users' work field, and has the characteristics that any application program can read the homepage content and etc. XML has changed the internal architecture of browser, and the current IE5.0 now can read XML document or to be more precisely said that the browser in XML language can read the document of the program such as Word, Excel and etc. Therefore, XML provides an integrated document form for the same kind of application between each enterprise, and also the integrated data form for the different application between computers.

Before executing the B2B E-Commerce Trading between enterprises, an integrated document form has to be established in advance (such as shown in the figure below) to supply the need of information communication. In its XML document form design, there are some points below that have to be noticed:

- The common of data architecture, to contain the data category of different enterprises.
- Data input and description management
- Using search and index to effectively check trade record.
- From the record that is acquired in the search, users can clearly achieve the message needed and the information presentation method can be self determined.
- Construct the series connection architecture between different trade systems.
- For the consideration of system security control, to distinguish the users with different status, includes the management and the control of information acquisition level.



- The information that is needed by the trade between enterprises can advance the interchange and the storage in accordance with each kind of different needs.

Through XML, each manufacturer in the trade architecture can advance the information communication in the same forms. For example, manufacturer C can use a certain form to give clear indication of the information such as the specifications of product needed, type number, quantity, price, delivery date and etc, and the purchase request that is sent out to supplier A. And when the supplier receive the order, it can transform the purchase request information that is sent by the opposite party directly into the form of its own enterprise for follow-up prices negotiation, signing and check, or the needs of delivery or production. After the supplier decides to carry out the trade, it can also use the same form to return the related information of the final determined trading product that is indicated in the original purchase order and carry out the operation procedures such as goods delivery, check on delivery, payment and etc. with this information.

4.2 SET Security Trade Operations

Continuing the example of the previous section, when manufacturer C and supplier A conclude a transaction, the trade will be processed through SET E-Commerce Trading mechanism. Its SET trade procedures are as below:

1. First, the Manufacturer C and the Supplier A has to obtain the digital certificate from the Certificate Authority, or contact its card issuing bank in advance, complete the registration procedures and obtain the Digital Certificate and Electronic Wallet.

2. The Supplier A will transmit the order of Manufacturer C to the electronic wallet of Manufacturer C through encrypted secure transmittance method.

3. If the Manufacturer C confirms this trade in the electronic wallet, electronic wallet will sign it with its digital certificate, and then transmit the enterprise credit card data to the on-line trade system of Supplier A through the encryption method.

4. The on-line trade system will send this encrypted credit card data and the signature of digital certificate of Supplier A to payment gateway for further process.

5. After payment gateway receives the trading data, it will forward the data to the bank of Supplier A. And the bank of Supplier A will request the bank of Manufacturer A (Manufacturer C) to transfer accounts.

6. At last, the bank of Supplier A will send the information about the account transfer, whether the accounts transfer is successful or not to the payment gate. The payment gate will then transmit this information back to Supplier A through Internet. Then Supplier A will reply to the Manufacturer C through XML, and at the same time, will inform the Manufacturer C of the relevant affairs of stocks delivery. No matter whether the trade is successful or not, the on-line trade system of Supplier A and the electronic wallet of Manufacturer C will keep this trading record.

4.3 Dynamic Ring Trade Architecture

When Manufacturer C sends out the Trade Request, and relevant information such as clear indication of its trade content, quantity, delivery date restriction and etc. to each manufacturer in the trade architecture due to the demand of business affairs, this kind of trade demand will start from Manufacturer C. And the message will flow through the whole ring system and flow through its upstream Supplier A, Certificate Authority B, Satellite Manufacturer D, and downstream market, dealer E and F, and etc. And the manufacturer, supplier or dealer who wish to participate in this trade can add the encrypted message of its own enterprise behind the message content, such as the quotation of prices, trade content consultation and discussion and etc. Since the information that is sent out has gone through the encryption process, the encryption process can assure the information security that the information can only be read by target receiver enterprise, while the other enterprises are responsible for the message transmittance only. Similar to the cooperation relationship of Manufacturer C and Supplier A, the trade relationship between Manufacturer C and its satellite Manufacturer D or with its Distributor E can also be executed through the message transmittance of ring architecture.

And since the ring trade architecture executes the information communication through a kind of series method, so when enterprise (such as manufacturer C) has some certain kind of trade needs, its trade content can be described through XML and the manufacturer with the status of initiator will send out the trade request. When any related upstream, middle stream, and downstream manufacturer in the architecture (for example Supplier A, Satellite producer D, distributor E) is interested in this trade, it can add its response on the message that is sent by Manufacturer C. The response part will be encrypted to ensure that only Manufacturer C can read it to prevent the happening of opportunistic trade and the condition of losing negotiation ability. Besides, in the ring architecture, the enterprise can send out the trade request to request for the joining and the cooperation of the enterprise interested only when it has the needs. After this trade is ended, the cooperation relationship will also be ended. Therefore, enterprises can dynamically choose and cooperate with the different manufacturers in accordance to their different needs. And this can expand the range in finding cooperation partner and can also find the most suitable manufacturer for cooperation and it is unnecessary to maintain the perpetual fixed relationship with upstream enterprises and downstream enterprises.

4.4 E-Commerce Trading Secure design

In the E-Commerce Trading environment of SET, except digital certificate, electronic signatures and etc., there are also some other related secure items. The messages of enterprises will flow through every link, so how to assure the trade related information could only be read by the right user will be a very important topic for study. Except for the alteration operation such as access, additions and deletions and etc that has to be executed by appropriate authorizer, the management of digital certificate annulment list should also be carefully executed; the so-called annulment list of digital certificate is the digital certificate that is annulled before the original valid date is due. There are some reasons that cause the annulment of digital certificate, such as

the private key is probably stolen or the private key is only used by certain staff in the enterprise, for example the private key that uses formal name like 「Kris Ma, director general of XYZ Company」. So when Kris Ma resigns or quits or is transferred to other occupational duty, XYZ Company may not wish that he uses only this private key to sign or reply to messages. Therefore, XYZ Company may put this private key on the annulment list of digital certificate to ensure the effectiveness of all signature keys.

5 Conclusion and future development

5.1 The application procedures of SET network certificate

At present, TAIWAN-CA. COM Inc. is the only domestic certificate authority that constructs credit card network certificate authority. Each Visa and MasterCard credit card issuing mechanisms and acquirers in Taiwan can authorize the company to serve as their credit card network certificate authority (cardholder certificate authority, network stores certificate authority). In the past, credit card mechanism users has to submit the certificate application to foreign companies through domestic agents, which always result in the disclosure problem of domestic users certificate and identification data to foreign mechanisms. And now this problem is solved.

For example TAIWAN-CA.COM Inc., the application procedures of enterprise SET network certificate are as below:

1. Client (network stores) submit the application to bank, fill out the registration form and provide relevant documents such as identification papers and etc (such as basic information of stores, business operation registration certificate and etc.) to register.

2. The bank will provide electronic wallet software, application manual and identification data for certificate application to the client.

3. The client installs the electronic wallet by itself.

4. Link to the website of TAIWAN-CA.COM Inc. to apply for certificate. After the network store submits application registration to the acquirer, it can enter the certificate application system according to the characteristics of the operation system platform and certificate application interface software. And input the basic information of network store and the status identification data, and submit the certificate application to the company through Internet.

5. After the certificate application is approved, network store can link directly to the bank or the

website of other network stores to carry out relevant trade.

5.2 The SET stores development condition of domestic network E-Commerce at present

According to the data of TAIWAN-CA.COM Inc., it shows that the domestic network stores (are shown as below) that possess SET certificate are mostly the stores of service industry.

Kind of industry	SET network stores
Department stores, markets	■ Taiwan Biznet ■ Taiwan GCnet ■ Taiwan EMall ■ Postal Stamps Mall Taiwan ROC ■ Central master Co., Ltd. ■ Heim ■ OHOT ■ BUT NET ■ CityGo ■ Victradco Ltd (Giftnet) ■ Webcity ■ Acer Internet Services, Inc. ■ EBay Taiwan ■ CTS Inc. ■ Music.com.tw (Fashionow) ■ Unalis on line
CD Exclusives	■ Cdclub ■ Rock Records
Books Exclusives	■ Amazon ■ Yuan-Liou Publishing Co., Ltd.
Network information	■ Your internet solution) ■ Vitek (Media net) ■ Oget ■ Funcity Co., Ltd ■ Digi Life ■ Cyberlink Co., Ltd. ■ Easy Top ■ Infopro ■ HiTrust Inc. ■ Kingnet ■ Wise Technology Co. ■ TWV
Tours and Hotels	■ Dynasty travel ■ Protour ■ Everlight Travel Service Co., Ltd. ■ Caesar Park Hotel
Telecommunications	■ Mobitai Communication

	■ Giga Media Ltd.
Insurance	■ Taian Insurance Co., Ltd.
Food products	■ I-Mei Foods Co., Ltd.
Public Service	■ Taipei Water Department ■ Taipei Rapid Transit Co.
Foundations	■ Te-Tao Cancer caring Foundation
Farmers' Association	■ Tao Yuan County Government Bureau of Agriculture

5.3 Future development and contributions

The influence of XML has extended to the macrocosm development of information system. XML future development will not only be limited to the tag language but will also involve in the automatic interchange, data process domain and play the important role in the mechanism. It will stride across the operation system environment, the target of transmission protocols and each kinds of other limitation, to arrive at data transform mechanism, and further completing the substantial reciprocal function of communication. Looking in the future, XML will complement the deficiency of EDI and the deficiency of Extended Intranets. Along with the mature development of XML related technology, the investigation of Zona Research shows that the application of XML in Electronic Commerce (E-Commerce) will raise from the 0.5% of the initial stage in 2000 to 40% in 2003.

As for the current condition of commercial procedures mechanism and Multi-tier Architecture application of nowadays, many vertical industries start applying XML technology to be the data form and the procedures standard of its industry, such as the RosettaNet and ebXML that are leading in the industry of electronic components; NewsML of publication industry, aecXML and LandXML of construction industry and Schemas, the retail information for retail business, and other industries such as Petrochemical industry, real estates industry, food products service industry and manufacturer are also starting to use the XML standard.

Using the dynamical ring trade architecture that integrates XML and SET will have some important effects towards the E-Commerce of manufacturer industry, and they are mentioned below:

- Supplier Management: to reduce the order management cost and procedures frequency with XML as the information interchange method between enterprises and to apply less manpower in managing more number of orders.
- Inventory management: Electronic Commerce can shorten the procedures and the time of order placing, delivery and payments collecting and it can reduce and improve the inventory management problem to avoid running out of stock.
- Distribution Management: Electronic Commerce can improve the sending condition of relevant documents such as funds requisition sheet, order sheet, freight bill and document for clearance of goods etc., and it can assure the correctness and validity of the documents and data.
- Channel Management: Dynamic trade mode can let enterprise find the most suitable cooperation partner and can transmit the operation condition that is changing to cooperation enterprises rapidly. It not only reduces the considerable quantities of labor cost but also

ensure the correctness and the sharing of information.

- Payment Management: SET E-Commerce secure trade method can link the company of suppliers and distributors and let the payment operation can be received and transmitted through electronic method. And this not only reduces the man-made error, assures the revenue and expenditure condition of fund, but also improves the speed of company accountant in bills calculation and reduces the trade cost and expenses.

But when current enterprise applies for the SET electronic commerce trade certificate, network certificate authority company will only request the enterprise to give clear indication of the information such as basic information of store, business operation registration certificate and etc. and this can only confirm the actual existence of the enterprise. While its credit data such as payment ability, goodwill assessment and etc. is not requested, so we recommend that in the future, certificate authority company should consider whether the payment of each individual enterprises is paid on time, whether there is delay record in the date of delivery, and etc before issuing certificate, and carry out enterprises credit assessment to assure the trade quality of enterprises that participate in the electronic commerce.

Nowadays, there is only TAIWAN-CA.COM Inc. that is network certificate authority unit in Taiwan. In the future, along with the rapid development of electronic commerce, the demand for certificate authority unit will also substantially increase. We suggest that each industry should have its own exclusive network certificate authority unit in the future. In this way, when the certificate authority unit issues network certificate to the enterprise of the industry, the certificate authority unit can effectively give the assessment of the enterprise credit since it knows more about the enterprise environment. This kind of industrialized method of certificate authority can also let the enterprise rapidly find the suitable cooperation enterprise under different commercial needs and improve the efficacy of electronic commerce.

References

1. Andrew B. Whinston, Dale O. Stahl, and Soon-Yong Choi, “The Economics of Electronic Commerce”, 1998, Prentice Hall.

2. Insoo Khill, Jiseon Kim, Ingoo Han and Jaecheol Ryou, “Multi-party Fair Exchange Protocol Using Ring Architecture Model”, Computers & Security Vol.20, No.5, pp.422-439, 2001.

3. Mitzi Montoya-Weiss and Anne Massey, “The Reality of Global Virtual Teams”, E-Commerce Learning Center, North Carolina State University.

4. David Simchi-Levi, Philip Kaminsky, and Edith Simchi-Levi, “Designing and Managing the Supply Chain：Concepts, Strategies, and Case Studies”, Irwin/McGraw-Hill, 1999.

5. Michael Meehan, “EDI, ebXML Groups Agree to Cooperate”, Computerworld, July 2, 2001.

6. Alexandros Moukas, Giorgos Zacharia, Robert Guttman, and Pattie Maes, “Agent-Mediated Electronic Commerce: An MIT Media Laboratory Perspective”, International Journal of Electronic Commerce, Volume 4, Number 3 (Spring, 2000).

7. Judith Gebauer and Michael J. Shaw, Guest Editors, “Introduction to the Special Section: Business-to-Business Electronic Commerce”, International Journal of Electronic Commerce, Volume 6, Number 4 (Summer, 2002).

8. Boris Padovan, Stefan Sackmann, Torsten Eymann, and Ingo Pippow, “A Prototype for an Agent-Based Secure Electronic Marketplace Including Reputation-Tracking Mechanisms”, International Journal of Electronic Commerce, Volume 6, Number 4 (Summer, 2002).

8. Asokan, N., “Fairness in Electronic Commerce”, Waterloo University, Canada, 1998.

9. Janice Reynolds and Roya Mofazali, “The Complete E-Commerce Book: Design, Build & Maintain a Successful Web-based Business”, CMP Books, October 2000.

10. Khalid Sheikh, “Manufacturing Resource Planning (MRP II) with Introduction to ERP, SCM, and CRM”, McGraw Hill, June 15, 2002.

11. Brett McLaughlin, “Java & XML, 2nd Edition: Solutions to Real-World Problems”, O'Reilly & Associates, September 2001.

12. Pierangela Samarati, Michael K. Reiter, and Sushil Jajodia, “An Authorization Model for a Public Key Management Service”, ACM Transactions on Information and System Security, Vol.4, No.4, November 2001.

13. Shai Halevi and Hugo Krawczyk, “Public-Key Crytography and Password Protocols”, ACM Transactions on Information and System Security, Vol.2, No.3, August 1999.

14. William Hillison, Carl Pacini, and David Sinason, “Electronic Signatures and Encryption”, The CPA Journal, August 2001.

15. Andres Torrubia, Francisco, J. Mora, and Luis Marti, "Cryptography Regulations for E-Commerce and Digital Rights Management", Computers & Security, Vol.20, No.8, 2001.

16. YuLun Huang, Shiuh, and Fu-Shen Ho, "A Generic Electronic Payment Model Supporting Multiple Merchant Transactions", Computers & Security, Vol.19, No.5, 2000.

17. Duen-Ren Liu, I-Chin Wu, and Sung-Ting Hsieh, " Integrating SET and EDI for Secure Healthcare Commerce", Computer Standards & Interfaces, Vol.23, 2001.

18. Institute for Information Industry (III)http://www.iii.org.tw/

19. E-commerce Application Promotion Center of III http://www.find.org.tw/

20. Industrial Development Bureau, Ministry of Economic Affairs http://www.moeaidb.gov.tw/

21. Guiding Promotion Project of Automation and Electronic Commerce by Ministry of Economic Affairs http://edi.tca.org.tw/

22. "Electronic Signatures Law" Promotion Project by Ministry of Economic Affairs http://www.esign.org.tw/

23. TAIWAN-CA.COM Inc. http://www.taica.com.tw/

24. Visa Taiwan. http://www.taiwan.visa.com/

25. ebXML. http://www.ebxml.org/

26. XML Taiwan Website。 http://www.xml.org.tw/

27. Peter Workroom, 2000 "Super Wild-angle e-Commerce Victory Guidance", Key Hold Information Co., Ltd,

28. Yeh Nai-chin, Chen Shih-wei, 2001, "The Latest Edition of Internet Summary", Kings Information Co., Ltd.

29. Wei Tsui-chi, 2000, "The Un-lack Role in e-Commerce—Research and Study on Legal Matters of Internet Payment and Certification", Master Thesis, Department of Laws, Soochow University

30. Teng Yu-pin, 2001, "Research on Applying XML on the Data Exchange and Integration in e-Commerce", Master Thesis, Department of Industrial Engineering and Engineering Management, National Tsing Hua University

31. Liang Yung-ju, 2000, "Practical Research on the Supply Chain Data Exchange System", Master Thesis, Department of Management Information System, National Chung Cheng University