Report on EDI and Security Standards (Draft)

Source: Expert Group B - EDI & Security Standards
Working Group 2 - Information & Services

Group Leader: Mr. K. K. Suen, Hong Kong Article and Numbering Association
Members: Mr. Cranfond Yu, Traxon Asia
Mr. Eddie Wu, Hong Kong & Shanghai Bank Corporation Ltd
Mr. Eldon Yeung, Tradelink Electronic Document Services Ltd
Ms. Rosa Chan, Hong Kong Article and Numbering Association
Mr. Thomas Lee, Hong Kong Article and Numbering Association
Mr. Ray Lai, CargoNet Transportation Community Network Ltd
Mr. Philip Wu, CargoNet Transportation Community Network Ltd

Submitted to: Working Group 2 - Information & Services
Task Force on Technical Standards
Information Infrastructure Advisory Committee (IIAC)

Date: 1 December 1997

Contact Person: Mr. K. K. Suen, HKANA
Tel: 2863-9711
Fax: 2861-2423
Email: hkanedi@ibm.net

Standard Needs Addressed: Part I - EDI Standards
Part II - EDI Security

Nature of Document: Draft for comment

Part I
Report on EDI Standards

(DRAFT)

Prepared for

Working Group 2 - Information & Services
Task Force on Technical Standards
Information Infrastructure Advisory Committee (IIAC)

Prepared by

Expert Group 2 - EDI & Security
Working Group 2 - Information & Services

1 December 1997

Table of Contents

EXECUTIVE SUMMARY

Background

Recognizing the increasing demand for improved efficiencies, effectiveness and timeliness, increasing numbers of companies have started to incorporate electronic commerce applications in their overall business operations. Electronic Data Interchange (EDI), as a key building block of electronic commerce, is used to streamline business processes by reducing paperwork and increasing automation.

Purpose of Study

To ascertain the effectiveness of Hong Kong's businesses in implementing EDI, it becomes a necessity for Hong Kong to endorse an internationally accepted EDI standard. In response to this uprising need, the Expert Group on EDI and Security Standards was established under the Information Infrastructure Advisory Committee for the purpose of recommending the most appropriate EDI standard for the Hong Kong business community.

Besides focusing on identifying an EDI standard, the scope of the Expert Group also includes the identification of EDI security standard. The outcome of the study on EDI security standard is presented in a separate report.

History of EDI Standard Development

The practices of electronic data interchange can be traced back to the late 1960's when EDI was done by agreeing on proprietary format between two trading partners. Industry specific standards were then gradually developed to meet the particular need of individual sectors. Even with industry standards in place, the development of national standard became apparent at the time of cross-industry trading. Later the need of having an international multi-industry EDI standard was also recognized due to the increasing volume of global trade.

Existing EDI Standards and Implementation Guidelines

There are currently five levels of EDI standards in place: proprietary, industry, national, continental, international. However, only two standards are widely recognized, which are the UN/EDIFACT and ANSI X12 standards. Studies on existing EDI standards and implementation guidelines indicate that majority of the EDI standards communities are moving towards conformance with UN/EDIFACT. And EANCOM is increasingly used as an implementation guideline of UN/EDIFACT due to its clarity and simplicity.

EDI Related International Organizations

The development of EDI standards is supported by many organizations throughout the world. Seven major organizations were identified to provide an overview of the emphasis being placed on the facilitation of EDI standards.
These organizations are:

- UN/EDIFACT Board
- Asia EDIFACT Board
- EAN International
- American National Standards Institute (ANSI)
- Uniform Code Council (UCC)
- Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.)
- International Air Transport Association (IATA)

EDI Development in Other Countries

The adoption level of EDI varies from countries to countries. The goal of this section is to give a better understanding of the EDI development and the standards being used in some major areas of the world. The countries/regions being studied are the U.S., Europe, Asia & China. Some of them may serve as role models or references for Hong Kong in EDI implementation.

EDI Development in Hong Kong

EDI Service Providers in Hong Kong
Studies on four major Hong Kong EDI service providers were carried out to provide a macro view of the overall EDI development in Hong Kong. The studies also provide information on the EDI standards currently being used and the level of EDI adoption in Hong Kong.

EDI Standards in Different Industries
This section aims to identify the EDI standards being applied in different industries/sectors in Hong Kong. The industries/sectors being studied are apparel, air cargo, retail & distribution, healthcare, banking, electronics, government & transport. Although varieties of standards are currently adopted in different industries, trends are towards compliance with UN/EDIFACT, and EANCOM is widely used as the implementation guideline for UN/EDIFACT.

Future Direction of EDI

New EDI concepts such as Lite EDI/Simpler EDI, Open EDI, New EDI are being developed at an international level. The aim of these new concepts is to ease the efforts involved in EDI implementation, which is believed to be helpful in facilitating the worldwide adoption of EDI.

Recommendation

The achievement of a single universal EDI standard is a long-term goal which would make

EDI implementation more efficient and would minimize the aggregate costs of use. Base on the study we conducted on EDI standards, we strongly recommend the United Nations/EDI For Administration, Commerce and Transport (UN/EDIFACT) standard be adopted for EDI implementation in Hong Kong. And EANCOM is recommended to serve as the implementation guideline for UN/EDIFACT. We feel that cooperation among all the EDI service providers will be the key towards the interoperability of EDI among different commercial sectors in Hong Kong.

Introduction

Objective

To identify a common standard to facilitate and enhance the interoperability of Electronic Data Interchange among different commercial sectors in Hong Kong.

Background

Businesses today face with demand for improved efficiencies, effectiveness and timeliness due to the increasing competition in both local and international community. To sustain their business growth or in some cases just to stay in business, companies need to maximize their productivity while keeping delays and costs to a minimum. Electronic commerce, a modern business methodology that addresses these needs, is being considered globally as a new way of doing business.

Every day, businesses generate and process a large volume of paper documents. These range form purchase orders and invoices to product catalogues and sales reports. One of the goals of electronic commerce is the integration of telecommunications, data management, and security services to allow business applications among different organizations to exchange information automatically. Electronic Data Interchange (EDI) serves as a key building block of electronic commerce in streamlining business processes by reducing paperwork and increasing automation. It is used worldwide in manufacturing, shipping, warehousing, utilities, pharmaceuticals, construction, petroleum, metals, food processing, banking, insurance, retailing, government, health care, textiles and other industries.

EDI is the transfer of structured data, by agreed message standards, from one computer application to another by electronic means and with a minimum of human intervention. In order for computers or, more accurately, computer applications to be able to accept EDI messages directly, the input information must be structured in a pre-defined format(s), according to specified rules and using standard abbreviations. In other words the data must conform to an EDI standard.

EDI standard is independent of the hardware, software and communication medium. EDI only specifies a format for business information; the transmission of the information is covered under other standards. Through the use of EDI message standards, data may be communicated quickly, efficiently and accurately irrespective of users' internal hardware and software types.

The development of standards plays a critical role in the evolution, acceptance and market penetration of EDI. One of the greatest difficulties organizations face is the different standards being adopted by groups of businesses, also known as proprietary standards. Without thought of the longer-term consequences once members of the group need to expand their trading activities outside the original circle, issue of incompatibility arises. If EDI implementation is to remain cost-efficient, trading partners must share a common language for their businesses and commercial messages.

History of EDI Standard Development

Early electronic interchange practices can be traced back to the late 1960's. At that time EDI was done by agreeing on proprietary format between two trading partners. Much of the early work on EDI was driven by particular industrial sectors, such as transportation, pharmaceuticals, groceries, automobiles, and banking. Each sector developed its own set of data elements and messages to meet its particular needs, with the result that the various sectors were not able to exchange messages.

Even with industry standards in place, organizations involved in cross-industry trading still faced a number of barriers, and consequently the need for national standards became apparent. A number of national standards were then developed and were widely adopted in the specific countries. Although these different national standards generally meet the domestic needs, they nevertheless were creating difficulties for international transactions. It became clear that if the EDI standardization efforts were to meet the requirements of the global business community, an international multi-industry EDI standard was needed.

By the mid-1980's, the development of an EDI standard began taking shape within the United Nations Economic Commission for Europe (UN/ECE) in the working Party for the Facilitation of International Trade (WP.4). In 1987, the syntax or grammar of this common business language, known today under the acronym UN/EDIFACT, was approved as ISO standard 9735. UN/EDIFACT or United Nations Electronic Data Interchange for Administration, Commerce and Transport comprises a set of internationally agreed standards, directories and guidelines for the electronic interchange of data. Over 60 countries and many international organizations, such as the European Commission, IATA, International Chamber of Commerce, ISO, International Chamber of Shipping and EAN International, are represented at the UN/ECE WP.4.

Existing EDI Standards & Implementation Guidelines

Although today there are many existing EDI standards, only two are widely recognized: UN/EDIFACT and ANSI X12. However, UN/EDIFACT is the only EDI standard endorsed both for national and international use by the governments of major trading nations, including the USA and most of the European countries.

The following levels of EDI standards are currently in place:

1.Proprietary	Standards that one or more trading partners develop to suit their specific situation.
2.Industry	Standards that an industry group develops for it's specific transaction processing requirements (e.g., TDCC for the transportation industry).
3.National	Standards that address different industry types within one country (e.g., X12 in the United States and Tradacoms in the United Kingdom).
4.Continental	Standards that are usually more widely accepted across an entire business community (e.g., X12 in North America and EDIFACT in Europe).
5.International	Standards that have been developed to facilitate trade among all industrialized nations in a world marketplace. (EDIFACT is the most widely accepted international standard.)

UN/EDIFACT

UN/EDIFACT (United Nations Rules for Electronic Data Interchange for Administration, Commerce, and Transport), which is slowly being accepted as a truly universal set of document translation standards, is a joint project between International Standards Organization (ISO) and United Nations Economic Commission for Europe. ISO is responsible for developing syntax rules and the data dictionary while the later responsible for the development of the document standards.

UN/EDIFACT incorporated much of the existing standards and is aiming to become widespread throughout the world. The concept of UN/EDIFACT revolves around a single international standard flexible enough to meet the needs of transmitting messages across industries, across country boundaries for both government and private sectors. It is fast gaining recognition and acceptance as the global EDI standard.

UN/EDIFACT covers standardization in five main areas:

- The syntax rules;
- The data elements;
- The segments;
- The messages;
- The codes;

EANCOM

EANCOM is an easy-to-use implementation guideline of the UN/EDIFACT standard messages. UN/EDIFACT messages are often complex and users may easily misunderstand the principles and original intentions of message designers. A subset of UN/EDIFACT messages, EANCOM aims to provide clear definitions and explanations which allow trading partners to exchange commercial documents in a simple, accurate and cost effective manner.

In 1995 the total number of EANCOM users was 7305. It was increased to 12750 in 1996, an increment of 75%. The figure is forecasted to increase again in 1997 by approximately 60%. EANCOM standards are currently used in 86 countries worldwide.

EANCOM was recently endorsed by the Asia EDIFACT Board as the EDI standard for procurement in the Asia region. Within the Asia EDIFACT Board Purchasing Work group, twelve economies have either adopted, or committed to adopt, EANCOM for their trading message requirements. The economies are China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Philippines, Singapore, Sri Lanka and Thailand.

In Europe there has been a marked increase in EANCOM usage in countries where national standards existed before EANCOM. An example of this migration is France where GENCOD-EAN France reported 3000 users of EANCOM in 1996. According to the 1996 EDI survey done by EAN International, the rate of increase in national standards usage appears to be slowing sharply, from a 46% increase in 1994, a 21% in 1995, to an increase in 1996 of just 13% with 7% expected for 1997. These figures indicate that EANCOM is being preferred over national developments.

EANCOM is currently available in 22 languages, Bulgarian, Czech, Chinese, Danish, English, French, German, Greek, Hebrew, Hungarian, Icelandic, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Spanish, and Swedish. The availability of an international standard in native languages is seen as a major instrument in the promotion and development of EANCOM worldwide.

ANSI X12

ANSI X12 developed by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) is the predominant standard in the United States. ANSI is one of the EDI standards with the largest user base today, not only in the United States, but also in Canada and Australia and for a number of international communities as well.

The development of ANSI X12 has been on an ad hoc basis, with the North American companies concentrating on perfecting ANSI X12 as a national standard whilst ignoring the increasing adoption of UN/EDIFACT in the rest of the world. The differences in the X12 and EDIFACT syntaxes make interoperation impractical, if not impossible. This caused problems with organizations, which traded internationally and so were forced to support two standards, ANSI X12 for domestic trade and UN/EDIFACT for international trade.

As a consequence, the membership of the Accredited Standards Committee has voted to align ANSI X12 with EDIFACT by 1997 with the EDIFACT syntax set already adopted. Many X12 users view switching standards as a cost with little financial return. To appease these users, the ASC X12 committee voted (as of February 1995) to continue the development of X12 standards (i.e. develop both EDIFACT and X12 standards), and to bring this issue to

vote every 3 years. Thus, the vote to continue the development of the X12 standards will be taken again 1998, and so forth.

As North America moving towards EDIFACT (away from ANSI X12) over time, it is expected that they will also adopt EANCOM as their only national standard for EDIFACT implementation under the name called GEDI (Global EDI Guidelines for Retail).

US Global EDI Guidelines for Retail (EANCOM US Subset)

Since 1993, it has become apparent that a growing number of EDI users in the grocery and retailing industries of North America becoming interested in using EDI outside of North America. In response to the increasing interest in global EDI, the Uniform Code Council (UCC) along with VICS EDI Committee have jointly developed GEDI based on EANCOM, a multi-industry subset of UN/EDIFACT. GEDI stands for Global EDI Guidelines For Retail. These guidelines are used by companies in the US which have trading relationship with oversea partners. Hong Kong Article Numbering Association is the coordinator for the GEDI project in Hong Kong. HKANA's role is to facilitate the use of GEDI for Hong Kong companies currently trading with companies in U.S.

GEDI Version UCC001, published in July 1997 contains the following five messages:

- Syntax and Service Report (CONTRL)
- Invoice (INVOIC)
- Purchase Order (ORDERS)
- Purchase Order Response (ORDRSP)
- Purchase Order Change Request (ORDCHG)

GEDI Version UCC002, scheduled for publication in October 1997, will contain two additional messages:

- Price/Sales Catalogue (PRICAT)
- Despatch Advice (DESADV)

Others

Despite the existence of both national document translation standard ANSI X12 and a universal set of document translation standards (UN/EDIFACT) which is slowly being accepted internationally, there are many different ‘semi-proprietary’ standards still being used for the translation of EDI document.

AIAG	Automotive Industry Action Group - the US automotive industry standards;
CargoIMP	Standard for airline/air cargo industry;
DISH	Data Interchange in Shipping - the standards used by a large group of European shippers, forwarders and carriers which, as with many European-based standards, are now moving towards conformance with EDIFACT;

EAGLE	Standard for the hardlines industry. The hardlines industry is composed of hardware and houseware and includes everything sold in a home center.
ODETTE	Organization for Data Exchange by Teletransmission in Europe - the standards used by the European motor industry which are also moving towards conformance with EDIFACT;
SWIFT	Standard used by the overwhelming majority of the world‘s banks for inter-bank reconciliation which are also moving towards conformance with EDIFACT;
TDCC	Transport Data Coordinating Committee - the original EDI standards, which were created by the US transportation industry and which formed the basis for ANSI X12;
UCS	Uniform Communications Standards - the standard used by the U.S. grocery industry and other retail-oriented industry sectors (subset of ANSI X12);
UN/GTDI	United Nations Guidelines for Trade Data Interchange (also known as TDI and TRADACOMS), which is widely used in Britain by the majority of trading companies;
VICS EDI	Voluntary Inter-industry Commerce Standard - the joint standards of the US apparel and general merchandise industry (subset of ANSI X12);
WINS	Warehouse Information Networks Standards - used by public warehouses and their depositor customers in US (subset of ANSI X12);

EDI Related International Organization

UN/EDIFACT BOARD

EDIFACT has established six regional boards as advisors for international standards: Asia, West Europe, East Europe, Pan-America, Australia & New Zealand, Africa. Each regional board has a rapporteur, who initiates and coordinates EDIFACT development work in the geographical area of jurisdiction. A rapporteur is someone who is nominated by a government and appointed by the United Nations Economic Commission for Europe Working Party 4 (UN/ECE WP4) on Facilitation of International Trade Procedures.

In Europe, the Western European EDIFACT Board consists of eight message development groups: trade, customs, constructions, insurance, transportation, finance, statistics, and tourism. In North and South America, the Pan-American EDIFACT Board (PAEB) serves as the coordinating body of Pan-American national EDI standards organizations and provides a forum for Pan-American representation and consensus to the EDIFACT rapporteur. EDIFACT standards development, maintenance, and technical assessment in North America is performed by ASC X12 in the U.S. and by Canadian Government Standards Board (CGSB) and Canadian Standards Association (CSA) Joint Technical Committee on EDI (JTC/EDI) in Canada.

Asia EDIFACT Board

This Asia EDIFACT Board, or ASEB in short, was formed with the mission to guide, stimulate and promote the development and use of the UN/EDIFACT standards in its member countries or economies. ASEB is the representative body taking care of all EDIFACT matters in the Asia region

Since its establishment in August of 1990 with two members: Japan and Singapore, the Asia EDIFACT Board has seen explosive growth, both in the number of its members and in the number of EDIFACT projects in the region. It now has eleven participating countries and one economy: Japan, Singapore, Korea, Chinese Taipei, Peoples Republic of China, Malaysia, India, Thailand, Philippines, Sri Lanka, Iran, and Indonesia. In addition, Hong Kong has been participating in ASEB meetings and activities since 1990 as "observer" economy. Also, Mongolia, Nepal, Burunei Darussarum have attended at the past Board meeting as observers.

The members of the Asia EDIFACT Board are nominees of EDIFACT Committees, or any similar organization, established in a country that is a member of the United Nations or ESCAP (Economic and Social Commission for Asia and the Pacific). Associate members are nominees of EDIFACT Committees, or any similar organization, established in an economy that is not a member of the United Nations or ESCAP.

EAN International

EAN International is an active participant in the UN/EDIFACT development process at national, regional and international levels. EAN is an association managing a worldwide system that allows the identification and communication of products, services, utilities, transport units and locations. It develops and maintains coding standards for all users, and has the aim of developing a global, multi-sectorial standard with the objective of providing a common language for international trade.

EAN and its member Numbering Organizations are not new to the field of EDI. Some Numbering Organizations like EAN Sweden developed sectorial standards as early as 1972, and the EAN Numbering Organization in the UK, ANA, published the highly successful TRADACOMS standard in 1982.

In view of the Numbering Organization‘s activities in EDI communications and in response to a growing demand from their member companies for an international standard, the EAN General Assembly decided in 1987 to launch the EANCOM EDI project. EANCOM was to be developed on the basis of the then emerging international UN/EDIFACT standard and it serves as a detailed implementation guideline of the UN/EDIFACT standard messages.

Several new Numbering Organization EDI projects were launched in Asia and Latin American during 1992 including Argentina, Brazil, Chile, China, Columbia, Hong Kong, Korea and Singapore. The majority of these projects have been launched on the basis of EANCOM as the implementation guideline for the international UN/EDIFACT standard messages for EDI. Many of these Numbering Organizations have begun a process of study and pilots on EANCOM with the objective of obtaining a consensus for its establishment as an operating national standard.

ANSI

American National Standards Institute (ANSI) founded in 1918 as the national coordinator of voluntary standards in the United States, including those related to communications, programming and data management. In, 1979, the American National Standards Institute (ANSI) chartered the Accredited Standards Committee (ASC) X12 to create a set of standards to facilitate the electronic exchange of business information. Its first standard was published in 1983. Known as the ANSI X12 standards, these are generic standards for common business documents, and are used across all industries. X12 membership is open to any individual, company or organization, which may be directly and materially affected by X12 activities.

Uniform Code Council (UCC)

Uniform Code Council, Inc. (UCC), a non-profit making organization in the United States, manages and administers Universal Product Code (UPC) and the following EDI implementation guidelines:

- Uniform Communication Standard (UCS)
- Voluntary Inter-Industry Commerce Standard (VICS EDI)
- Warehouse Information Network Standard (WINS)
- Global EDI Guidelines for Retail (GEDI)

In 1984 UCC began administering the Uniform Communication Standard (UCS), an EDI standard developed by the grocery industry. In 1988, the UCC expanded its support to include the Warehouse Information Network Standard (WINS) and the general merchandise retail standard known as VICS (Voluntary Interindustry Commerce Standard).

With trade increasingly taking place on a global scale, the Uniform Code Council realized something had to be done to bring the North American standard in line with the worldwide standard. After two years of studies, the UCC has endorsed EDIFACT/EANCOM subset for international EDI use. For trade within North America, the UCC will continue to use the UCS/WINS and VICS subsets.

In 1996 UCC published "UCC Global EDI Guidelines for Retail" (GEDI), Version UCC001, which was developed based on EANCOM. While the use of the EANCOM subset within North America is not expected to be large at present, the UCC has predicted that interest among its members will grow rapidly, especially with the new availability of the UCC guidelines for implementing EANCOM.

The Uniform Code Council (UCC) and EAN International are working more closely than ever to provide a common platform for trading partners in North America and the rest of the world.

Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.)

S.W.I.F.T. was formed in 1973 by a consortium of U.S. and European banks with the goal of establishing a set of data processing and computing standards for communications among banks. Today, S.W.I.F.T. operates the largest, cross-border system in the world for exchanging banking-specific electronic messages. The S.W.I.F.T standards are one of the earliest examples of the use of EDI standards. They have their own data dictionary and syntax rules.

S.W.I.F.T currently operates in 130 countries. Everyday it processes an estimated $2.5 trillion in payment instructions among nearly 5,000 banks and other institutions that are co-owners of S.W.I.F.T.

S.W.I.F.T. has announced its intention to support EDIFACT messages for the trader to bank interface. SWIFT is currently serving on the EBES/European Expert Group 4 - Finance (EEG4) as secretariat where Financial EDI messages are developed base on the EDIFACT message standard.

International Air Transport Association (IATA)

IATA's mission is to represent and serve the airline industry. In fulfilling that mission, IATA services four groups interested in the smooth operation of the world air transport system: airlines, the general public, governments, third parties such as travel and cargo agents or equipment and systems suppliers.

IATA standards are one of the earliest applications of EDI standards. IATA has defined a proprietary data dictionary (using specific data elements) and syntax rules. Messages developed by IATA relate to passenger travel, cargo movement and parts ordering.

IATA is responsible for the development of CARGO IMPS, the Air EDI Standard. IATA is also a sponsor of Cargo Community Systems in several countries. These systems electronically link participants in air transport: carriers, customs administrations, air terminals and air freight consolidators.

Over the past few years, IATA has undertaken a major activity to migrate from its own standards to EDIFACT. For instance, the Cargo-IMP series of messages have now been mapped onto EDIFACT (Cargo-FACT). Another key development of IATA has been the development of the IATA Interactive EDIFACT architecture, which is now into its implementation stage.

Global EDI Development

The United States of America

Sectorial initiatives to implement EDI flourished in the United States around the mid 1970's. Pioneering work was conducted in 1975 with the development of EDI for the transport industry and from 1977–1982 in the grocery industry with pilots of UCS (Uniform Communication Standard). Several other EDI initiatives were being developed in the banking, insurance and automotive sectors, to list a few.

In 1978, ANSI (American National Standards Institute) became involved in the initial development of a generic EDI standard, which eventually was designated as X12. However, by the time ANSI X12 was developed and acquired a critical mass of users (1986), several communities already had a head start of several years with a large user base making the migration to the generic X12 standard non-trivial. In 1992, ANSI ballot its membership in order to ascertain whether the users would support a migration to EDIFACT. An overwhelming majority (76%) voted in favor of the proposal. However, the ANSI standard will undoubtedly be maintained for a number of years for the benefit of its users as they prepare for migration.

Current estimates of companies doing EDI range from 40 to 50 thousand in the United States. With the US Government passing the Electronic Commerce bill requiring the US Government to conduct all of its procurement less than US$100,000 using EDI, the US Government alone has identified over 350,000 trading partners with which it intends to do EDI by the beginning of 1997.

In the Federal Information Processing Standard (FIPS) 161-1 for Electronic Data Interchange, the US Government committed to using EDI X12 and EDIFACT standards in the exchange of business information with trading partners already using EDI. On October 26, 1993, President Clinton signed an Executive memorandum requiring Federal agencies to implement the use of electronic commerce in Federal purchases as quickly as possible. As the initial step the President's Management Council (PMC) Electronic Commerce Task Force (ECTF), chaired by the Administrator, Office of Federal Procurement Policy (OFPP), chartered the Federal Electronic Commerce Acquisition Team (ECAT) memorandum. The PMC gave ECAT the task of defining the system and identifying the executive departments or agencies responsible for developing, implementing, operating, and maintaining the Federal electronic system.

Europe

In several European countries, EDI activities began in the early 1970's in the retail and distribution sector under the auspices of EAN Numbering Organizations. EAN Numbering Organizations were approached and entrusted by their member companies to develop a standard communication system, including telecommunication facilities allowing for the exchange of commercial documents with their trading partners. As early as 1972, Sweden had developed the Dakom standard. Similar activities took place in France in 1974 when GENCOD (EAN in France) developed the GENCOD language, in Germany in 1977 when CCG (EAN in Germany) developed the SEDAS Invoice and in 1979 when the ANA in the United Kingdom (EAN in UK) began working on the TRADACOMS standard. Other sectoral activities included the ODETTE (Automotive industry project) and international projects such as IATA (airlines) and SWIFT (banking).

The international co-ordination began in 1986 and led to the creation of the UN/EDIFACT (United Nation Electronic Data Interchange for Administration, Commerce and Transport) syntax implementation and message design guidelines which were endorsed by International Standards Organization (ISO) in 1987 as ISO 9735. A United Nations Trade Data Element Directory also was approved as ISO 7372.

Currently in Europe, the EDI growth has been dramatic to say the least. It is estimated that the EDI growth rate of 35% or more per year will continue well into the year of 2000 with the current user base estimated at around 15,000.

In Western Europe, sustained growth in the implementation of mature national standards was accomplished by an increasing use and interest for EANCOM, both as an EDI standard for international and national communications. In a number of countries such as Denmark, Iceland, Italy, Ireland, Portugal and Switzerland, the EANCOM standard has been adopted as the national standard by the EAN Numbering Organization. In other countries, like Germany, The Netherlands, Norway and Sweden, a full or partial migration form the national standard to EANCOM has begun. As they do so their member companies benefit from the implementation of one standard applicable for national and international communications based on the internationally recognized EDI Standard, UN/EDIFACT.

Asia

The countries in Asia are witnessing rapid economic growth. Seen as a region with highest potential for development and growth, it offers itself as an attractive production base and a potential market where the manufacturing costs are low and the markets are growing. The growth of many of the Asian countries has in fact been characterized by rapid industrialization and growth of the export markets.

One of the trends which has clearly emerged among some of the Asian countries is the use of EDI for the growth of their economies. They have taken the first step in setting up national networks that are targeted to improve the efficiency of business transactions through the handling of trade documentation electronically. Most of these countries have targeted their first EDI applications in the area of international trade, to enhance trade efficiency. There is also an increasing interest among these networks to interconnect to each other and to process the trade documentation between trading partners in each country electronically.

As one may expect, Japan led the way in EDI implementation in Asia followed by Australia. While Japan paid the heavy penalty of being a pioneer thus having to develop most of its messages in proprietary format, Australia adopted the US X12 standard instead. However, both countries are currently major supporters of the international standard EDIFACT.

EDI implementation took a dramatic turn in 1987 when the Singapore Government announced the first nation wide EDI network in the world. The Singapore Government's approach of developing a national EDI network infrastructure then followed by the systemic sectoral development has become a model for most of the Asian countries.

In Asia, due to the smaller base of existing EDI users, the growth rate will probably continue to increase by 2 to 3 folds for the next few years and then tapered off to around 50% increase for the subsequent 2 to 3 years as some of the national projects reached their height of implementation.

A large majority of the Asian countries have adopted the international EDIFACT standard as their official EDI standard. EANCOM is also being actively promoted by the respective EAN association in each country to ensure a consistent way of implementing the EDIFACT standard.

China

China continues to move ahead in its development of EDI, making progress that will impact both the Chinese and worldwide economies. Indeed, the Chinese government has identified EDI as one of the "Three Golden Projects" in the development of the country's information infrastructure. And with a digital data network (DDN) now up and running, companies in many parts of China can take advantage of EDI.

The China EDIFACT Committee (CEC) was set up to oversee the development of EDI and bar coding in China. Under the CEC's jurisdiction is the Article Numbering Centre of China (ANCC), which is responsible for EANCOM-related activities. The China Purchasing Joint Working Group (China-PWG) had also been established for EANCOM message and software development. The China-PWG is to be administered by the ANCC.

In 1994 EANCOM was adopted as the national standard in China. The EANCOM 1994 has also been translated into Chinese and was published in July 1995.

Regarding infrastructure development, the China-PWG has chosen Shenzhen as a pilot area for implementing an EDI system. The project will use the newly adopted purchase order EANCOM message to link retailers and suppliers.

EDI Service Providers in Hong Kong

A number of EDI value added service providers has been operating in Hong Kong over the last six years. International VANs such as AT&T, British Telecom, GEIS, IBM, Infonet, SITA, SprintNet and SWIFT have been providing EDI services in Hong Kong. In addition, a few local EDI networks have also been set up to aim at specific target markets, including CargoNet, EZ*TRADE, Traxon, Tradelink.

With TRAXON offering EDI service to the air-cargo community; CargoNet for the shipping community; EZ*TRADE for the retail, manufacturing and trading industries and Tradelink for the government, Hong Kong is in a good position to leapfrog some of the Asian countries in EDI implementation. The ultimate goal will be the inter-connection of the different EDI network in Hong Kong.

CargoNet

CargoNet, the Hong Kong based global electronic data interchange system for the trade and transportation community, started operations in September 1995. The objective of CargoNet is to serve the Hong Kong business community with an electronic commerce network and information service hub. The solution provides all the complementary technology such as EDI, email, Internet Web, fax, bar coding, scanning, smart cards and communications. Its aim is to speed up the communications between members of the transportation and trading communities in Hong Kong and Southern China.

The local market in Hong Kong includes some 14,000 trading companies, 42,000 manufacturers, 44,000 shippers, 800 freight forwarders and 250 ocean carriers. The Cargonet system uses the UN/EDIFACT and ANSI X.12 standards for its electronic documents. It expects to launch with 12 basic trade and transport message types covering shipping instructions, bills of lading and invoicing, among others and more will be added according to demand.

Since launch in September 1995, CargoNet has offered desktop solutions based on the CargoNet "End-user Package" which enables shippers to exchange documents (such as shipping orders, shipping instructions) with transportation service providers. CargoNet also provides EDI gateways for service providers or large organization to send and receive EDI messages using X.400 mailboxes.

EDI messages exchanged include IFTMIN, IFTMCS, IFTMBF, IFTMBC, IFTMAN, IFTSTA, IFTSTQ, IFCSUM, INVOIC, ORDERS, QUOTES, REQOTE, DESADV, DELFOR, INVRPT, DELJIT. CargoNet also supports central translation services to facilitate migration to UN/EDIFACT.

CargoNet shareholders include: Hong Kong International Terminals (HIT), the Hong Kong Association of Freight Forwarding Agents (HAFFA), Kenwa Communications, a major freight forwarder and ship operator, Global Logistics Systems Ltd. (also known as TRAXON Asia, a joint venture between Cathay Pacific Airways and other airlines), I.T. supplier, EDI Network Services and Commercial and Transportation Software Services, a division of Hong Kong IBM reseller CSSL.

The CargoNet communication service is provided by the AT&T global EasyLink Services in conjunction with CargoNet.

EZ*TRADE

EZ*TRADE is a community EDI service offered by Hong Kong Article Numbering Association (HKANA). HKANA is an independent non-profit making industry organization founded in 1989 by the Hong Kong General Chamber of Commerce under an international charter, to promote and administer the international EAN standards in Hong Kong . HKANA's mission is to increase the competitiveness of Hong Kong companies through the use of IT technologies and international business standards. It is represented by many leading local business associations such as the Chinese Manufacturers' Association of Hong Kong, Federation of Hong Kong Industries, Hong Kong Coalition of Service Industries, Hong Kong General Chamber of Commerce, Retail Management Association and the Textile Council of Hong Kong.

EZ*TRADE, an initiative of the HKANA in collaboration with IBM, is an EDI service that enables companies in the retail, distribution and manufacturing industries to send and receive electronic business documents such as orders, invoices, etc. The objective of EZ*TRADE is to simplify trading processes through the use of EDI. EZ*TRADE is committed in driving the adoption of EDI to make Hong Kong stay ahead of competitors. Besides providing network, software, and helpdesk support, EZ*TRADE offers education and training programs, promotions, consulting services, roll-out assistance and a library for companies to learn about EDI and electronic commerce.

The EZ*TRADE service was launched for commercial use in May 1995 and the service is made available to all companies who are interested in doing EDI with their trading partners. Currently there are about 300 EZ*TRADE users from industries such as retail, distribution, healthcare, and apparel. Users include: Park'n Shop, Wellcome, 7-Eleven, Swire Coca Cola, Wing On Department Stores, San Miguel, Nestle Dairy Farm, Inchcape JDH, Mobil Oil, Garden, Edward Keller, United Soft Drinks, 3M Hong Kong, EAC, Unilever Hong Kong, P&G, Hospital Authority, etc.

All messages developed by HKANA are based on international EDI implementation standards EANCOM. In order to simplify implementation effort for the entire EDI community in Hong Kong, HKANA takes the leading role of defining implementation guidelines for the ten messages chosen by the members. This approach eliminated the issue of having one message format (one implementation guideline) for each customer, as it is the case overseas. Under EZ*TRADE EDI User Committee, a Message Development Sub-committee has been set up to review and define the EANCOM messages to suit Hong Kong's business practice. HKANA also represents at the Asia EDIFACT Board and UN/EDIFACT Board via EAN to ensure users' needs be reflected in the worldwide development of EDIFACT and the most up-to-date information be available to all the EZ*TRADE users.

Tradelink

Tradelink originated as a group of leading Hong Kong businesses and trade associations, which joined forces with Government in 1988 to investigate the feasibility of a community-wide EDI service. Tradelink's 11 current shareholders, which include key members of the trading community and future users of EDI, are:

- Hong Kong Government
- China Resources (Holdings) Ltd.
- Hong Kong Air Cargo Terminals Ltd. (HACTL)
- Hong Kong Association of Freight Forwarding Agents (HAFFA)
- The Hong Kong General Chamber of Commerce
- Hongkong International Terminals Ltd. (HIT)
- The Hongkong & Shanghai Banking Corporation Ltd.
- Hong Kong Telecommunications Ltd.
- Modern Terminals Ltd. (MTL)
- Standard Chartered Bank
- Swire Pacific Ltd.

Tradelink's mission is to contribute towards an improvement in Hong Kong's competitiveness in world markets by simplifying trade procedures through the introduction of new business practices and the use of information technology.

Currently Tradelink has two services available: Restrained Textile Export Licenses (RTEL) application and Trade Declaration (TD) lodgement. There are about 12,000 companies submitting over 800,000 RTEL documents per year while the number of TD lodged per year is over 10 million spread over 70,000 manufacturers and traders.

The Government has announced the closure of its paper-handling counters for RTELs by 31 December 1998 and for TDECs by 31 March 2000. After these dates, electronic submission through Tradelink's services will be the only way to send these messages to Government.

Tradelink currently represents Hong Kong in the Asia UN/EDIFACT Board where it is an observer.

Traxon

Traxon Asia, a joint venture between Cathay Pacific, Japan Airlines and Korea Air provides Cargo systems service with EDI capability for the airlines, cargo forwarders, customs and all other related parties. Parties can use the system to perform transactions among one another using standard message format (CargoIMP).

Participating carriers include:

- Air France
- Cathay Pacific
- Cargolux
- Japan Airlines
- Japan Asia Airways
- Korean Air
- Lfthansa
- Scandinavian Airlines
- Singapore Airlines
- Swissair
- Air Canada

which totally accounts for more than 60% for cargo uplift out of Hong Kong.

In Hong Kong, Traxon Asia currently has 170 freight forwarders and 188 connections. Most of them use the Traxon PC package running on a LAN or standalone environment. As of mid 1996, there are 21 airlines and about 2,000 freight forwarders in 5,000 offices connected with Traxon. Inter-CCS message exchange complies with air cargo standards established by IATA. For those freight forwarders that do not prepare messages in standard format, Traxon will convert their messages to comply with the standard. Primary functions include cargo space availability inquiry and cargo space reservation, shipment status tracking and air waybill data transmission.

Customs Express Consignment Manifest (CUSEXP) message was implemented in October 1996. This message allows freight forwarders to transmit house manifest data to the air cargo terminal so that the airlines can match these data with the master air waybill data for cargo reporting and customs clearance.

Traxon Asia is working together with EXIMNET to provide reliable cargo information communication services that are simple to use and will be implemented in Thailand soon.

Starting operations in September 1991, Traxon Asia is operated by Global Logistic System Asia.

Major Industries using EDI in Hong Kong

Air Industry

The history of EDI in the air transport industry goes back to the 60's when airlines started to exchange structured messages such as AIRIMP related to passengers and CARGOIMP related to cargo. In the IATA standard, CARGOFACT, a subset of EDIFACT designed specially for Cargo and SSIM (Standard Schedule Information Message), is also used widely to update the schedule database of the airline computers.

A transition to open standards e.g. EDIFACT is now occurring in the air industry especially in the cargo area where airlines are gearing to move from CARGOIMP to public standards. However the migration of standard is believed to be slow since CARGOIMP has rooted itself in this industry for a long time and migration towards other standards offer little incentive to the users.

Apparel Industry

The whole apparel business is today oriented toward the satisfaction of the final customers. This involves an effort toward more flexibility and reactivity by all the players. The installation of a short circuit strategy in procurement can only be done if there is an efficient transmission of the commercial, logistical and technical data from downstream to upstream. EDI plays an important role in achieving this goal.

Increasing numbers of Hong Kong companies are pressured by their oversea business partners to improve their business efficiency, and transmitting business document through EDI is becoming a major business requirement. In response to these challenges, Hong Kong Article Numbering Association has initiated an apparel industry project to facilitate the use of EDI, data identification and other automatic data capture technology to enhance the competitiveness of the Hong Kong apparel industry.

In the domestic apparel market, EANCOM standard is most commonly used as the standard for EDI implementation. For international market however, ANSI and EDIFACT are currently the dominating standards.

Banking Industry

EDI with banks, so called Financial EDI, has been implemented in the banking industry for quite a long time, but with local adoptions and standards. EDI offers opportunities for banking industry to handle the settlement of invoices, payments and reconciliation more efficiently. The SWIFT standard is used by majority of the world's banks for inter-bank communication.

At international level, efforts have been put in for the development and standardization of Financial EDI. In 1988 the EBES/European Expert Group 4 -Finance (EEG4) was established by the European Board for EDI Standards (EBES). Its primary task is to develop EDIFACT messages for the communication between financial institutions and their customers in both directions and where appropriate, for communication between banks.

Government Sector

In Hong Kong, as in most other major world trading centers, the Government is committed to phasing out paper submissions of trade information. The receiving counters for Quota License applications, for instance, will be progressively closed by the end of 1998 and those for Trade Declarations by March 2000. With government owning 48 percent of the shares, Tradelink's initial focus is on automating commonly-used Government trade transactions.

Under its franchise agreement with the Hong Kong Government, Tradelink will implement and operate the Community Electronic Trading Service, using EDI and other techniques, to improve and facilitate international trade for the Hong Kong trading community. Tradelink has the exclusive right to provide services for handling a range of Government trade-related transactions for a period of 7 years. Other exclusive services now under planning and development include Certificates of Origin, manifest information, dutiable Commodities Permits and other quota related transactions.

To encourage the rapid adoption of EDI, the Hong Kong Government has instigated a preferential fee structure for RTELs and TDECs submitted electronically, such that the total cost for EDI submission is no more than that for using paper forms, even when Tradelink's handling charges have been added.

According to a Hong Kong Economic Journal report, the Government spent $121m in 1993 to set up and EDI system with the capability of handling 212,000 and 1.61 million applications for Quota Licenses and Trade Declarations, respectively. It is predicted that the existing system will only be able to cope with demand in the first year. Thus, the government plans to further expend $150m for the expansion of the computer system over the coming three years.

All the government related EDI messages are developed base on the EDIFACT standard.

Healthcare industry

The number of health care industry players that have begun to use EDI and automatic data capture (ADC) technology to streamline business procedures and obtain accurate, machine-

readable information has increased dramatically in recent years.

Through the use of article numbering and EDI communication system, significant progress has been made in the medical industry to improve efficiency, especially logistics control and supply chain management. Due to the increasing use of EDI, the European Medical EDI group (EMEDI) is now working closely with EAN International on applying EANCOM messages within the healthcare industry.

In Hong Kong, most of the EDI activities in the health care industry have been centered on the procurement process among the wholesalers and manufacturers of pharmaceutical products. Since December 1996, Hospital Authority of Hong Kong has started employing EDI in their pharmaceutical procurement. Currently, HA is doing EDI with seven of its suppliers which account for more than 70% of their total pharmaceutical supplies. The EDI standard being adopted is EANCOM.

Retail Industry

The retail industry has been one of the most active group in the EDI community both locally and internationally. A general trend is to have bar coding integrated with EDI to facilitate the buying and selling processes of retailers. Major players of the retail industry in Hong Kong, including Park'N Shop, Wellcome, Seven-Eleven, Swire Coca Cola, Jusco and Nestle Dairy Farm, are participants of the Retail EDI project initiated by EZ*TRADE. There are currently more than 200 companies in the retail industry using the EZ*TRADE service.

EANCOM is the prevailing EDI standard being implemented in this sector.

The following table summarizes the EDI standards being applied in different industries in Hong Kong.

Industries	**EDI Standard**
Air Cargo	CargoIMP
Apparel	EANCOM (local), EDIFACT & ANSI X12 (International)
Bank	SWIFT & EDIFACT
Electronics	EDIFACT & ANSI X12
Government	EDIFACT
Healthcare	EANCOM
Retail & Distribution	EANCOM
Transport	EDIFACT/EANCOM

Future Direction of EDI

Lite EDI (EDI to Web)

Lite EDI, or EDI to Web, and vice versa is a growing business for several network providers. The advantage is that all end-users need is a simple PC and a Web browser. Since many users are already surfing the Internet for other purposes, Lite EDI will shorten the learning curve of implementing EDI. A centrally located application allows modifications and upgrades be handled from the central site. However, Lite EDI concept revolves around a man-machine interface, not a machine-machine interface which is the original concept of EDI.

Open EDI

Open-EDI is a version of EDI that can be performed in an open environment. That is, anyone being able to do business with anyone else without the need for prior human negotiation and agreement as to the technical or business details involved

The objective of Open-EDI is to develop a solution that enables two or more trading partners to transact business with no prior arrangements and no human involvement at all - where all parts of the trading relationship can be negotiated, resolved, and implemented entirely by the Business Information Systems of the trading partners involved.

The field of application of Open-EDI is the electronic processing of business transactions among autonomous multiple organizations within and across sectors (e.g., public/private, industrial, geographic). It includes business transactions which involve multiple data types such as numbers, characters, images and sound.

An Open-edi Reference Model has been developed primarily in order to provide standards required for the inter-working of organizations, through interconnected information technology systems. The model is independent of specific:

- Information technology implementations;
- Business content or conventions;
- Business activities;
- Organizations.

It is believed that with the introduction of Open-edi will have a positive impact on the number of EDI users. However, the Open-edi is currently still undergoing study and discussion at an international level. It is expected that concrete finding would not be available in five years' time.

Recommendation

As business becomes more and more information intensive, increasing numbers of companies will be forced to adopt EDI as a solution to improve business efficiencies or in some cases just to stay in business. In order for Hong Kong to stay competitive and move forward, the adoption of EDI technology should not be overlooked. The efficient implementation of EDI technology relies on the availability of a universally accepted EDI standard.

Based on the study we conducted on EDI standards, we recommend the United Nations/EDI For Administration, Commerce and Transport (UN/EDIFACT) standard be used for EDI implementation in Hong Kong. This recommendation is made based on the following factors:

- EDIFACT is the prevailing global standard.
- EDIFACT is flexible enough to be used across industries and across country boundaries for both government and private sectors in a wide range of EDI applications.
- EDIFACT is also supported by a set of rigorous messages design procedures, thus ensuring that EDIFACT messages which are endorsed by the United Nations conform fully to the standard and hence are internationally functional.
- EDIFACT is fast gaining popularity not only in the United States and Europe, but also in Australia, China, India, Japan, Malaysia, New Zealand, Republic of Korea, Singapore, as well as in many developing countries in the Asia and Pacific region.

EANCOM, an implementation guideline of EDIFACT for trade, transport and finance, is also recommended for users who prefer a simpler EDI standard and yet conform to the UN/EDIFACT standard. A subset of EDIFACT, EANCOM takes on a pragmatic approach on implementation guidelines. It is slowly being accepted as the EDI standard for EDIFACT implementation. Another advantage of EANCOM is the incorporation of the Automatic Data Capturing and Data Identification technologies which allow the automation and efficient handling of data transmitted through EDI messages. With these features and its increase in popularity, EANCOM not only allows users to stay in compliance with the EDIFACT standard but also allows the easier implementation of EDIFACT standard.

The achievement of a single universal EDI standard is a long-term goal which would make the use of EDI more efficient and would minimize the aggregate costs of use. We do understand that this goal may not be feasible at the current moment in Hong Kong since adoption of industry standards has deeply rooted in some industries, such as the banking and the air cargo industry.

To ensure the efficient use of EDI across different commercial in Hong Kong, all the EDI service providers should work together in achieving the goal of one common EDI standard. A common EDI standard should be used in any cross-company, cross-industry or cross-country communication. The common standard here is UN/EDIFACT, as we have recommended before.

The cooperation among the EDI service providers will be the key towards the interoperability of EDI communication in Hong Kong.

REFERENCE

1. "A Guide to Financial EDI: Strategy and Implementation", EBES/EEG4, 1996.
2. "A Road Map to EDI", Electronic Commerce World Institute, http://www.ecworld.org/Resource_Center/Agora/Roadmap/content.html
3. “Asia EDI Markets”, EDICOM 97 Conference
4. "Asia EDIFACT Board, Hong Kong Progress Report", April 1997
5. "CommerceNet Sponsors EDI Over Internet Initiative; Digitally-Signed EDI data is Exchanged Successfully for the First Time", http://www.commerce.net/news/cnet_edi.html
6. Baker, Michael, “EDI Standards Do Not Define EDI,“ http://www.ema.org/html/pubs/mmvln4/edistand.html
7. Chan, Sally & Marcella, Albert J., "EDI Security, Control, and Audit", Norwood, MA: Artech House, Inc, 1993.
8. Dobbing, David, “New Development in UN/EDIFACT”, Asia Pacific Conference and Exhibition on EDI
9. "EANCOM, an international standard for EDI communication", EAN International.
10. "EDI Meets the Internet", ftp://ftp/sterling.com/edi/FAQ.html
11. "Electronic Commerce and Electronic Data Interchange (EC/EDI)", http://cals.debbs.ndhq.dnd.ca/english/links/ediinfo.html
12. "Electronic Data Interchange Standards", http://www2.echo.lu/oii/en/edi.html
13. “Fundamentals & Business Planning of EDI”, Hong Kong Article Numbering Association.
14. Georget, Pierre, Editor, "Just in Time in the Textile Industry", Gencod - EAN France, 1997 Jan.
15. "Hong Kong (The Asia EDIFACT Board)", http://www.nectec.or.th/bureaux/tedic/HK-EDI.HTML
16. “Hong Kong Article Numbering Association: Annual Report 1995"
17. “Implementing EDI”, EDICOM 97 Conference
18. McLure, Marcia L., Ph.D. & Moynihan, James J., "EDI: A Guide to Electronic Data Interchange and Electronic Commerce Applications in the Healthcare Industry", Burr Ridge: Irwin Professional Publishing, 1996.
19. "Open-EDI", Standards Australia.
20. Owens, Gerry, “Integration of Barcoding and EDI Standards for Increased Efficiency.”, Asia Pacific Conference and Exhibition on EDI
21. "Reinsurance Standards for Electronic Data Interchange", http://www.rinet.com/rstds.htm
22. Seah, Eileen, “EDI Evolution in the Air Industry”, Airline Telecommunications and Information Services.
23. Sokol, Phyllis K., " From EDI to Electronic Commerce: a business initiative", New York: McGraw-Hill, Inc.
24. Tallim, Paula & Zeeman, Johan C., "Electronic Data Interchange: An Overview of EDI Standards for Libraries (1993)", http://www.nlc-bnc.ca/ifla/Vl/5/reports/rep4/rep4.htm
25. "The Asia EDIFACT Board", http://www.nectec.or.th/bureaux/tedic/ASEB.HTML
26. “The Global Company EDI Standards”
27. "What is Electronic Data Interchange?", Uniform Code Council, Inc.
28. “What is EDI?”, http://www.digitsw.com/Digit%20Web%20Pages/what%20is%20EDI.html

Part II
Report on EDI Security

(DRAFT)

Prepared for

Working Group 2 - Information & Services
Task Force on Technical Standards
Information Infrastructure Advisory Committee (IIAC)

Prepared by

Expert Group B - EDI & Security
Working Group 2 - Information & Services

1 December 1997

EDI Security

Nowadays EDI and its message have become more and more independent as EDI can progress in a different kind of system such as Interent and VAN. Therefore setting an EDI message standard is a specially in the security point of view, to make sure a message is secure the best way to do is to secure the message.
Security is a combination of methods, procedures, hardware, firmware and software used by a system to minimize the vulnerabilities of assets and resources. An asset can be seen as anything of value. Vulnerabilities are weaknesses that can be exploited to violate a system or the information it contains. A threat is defined as the potential to exploit a vulnerability to cause a loss of integrity, confidentiality or availability of assets or resources.
From a security view, the top priority is to establish an acceptable set of mechanisms that can provide the necessary security services. Adequate safeguards are needed to protect the confidentiality, privacy, integrity, and intellectual property of users of the Global Information Infrastructure (GII). It is this issue of security that will determine how rapidly the GII proliferates.

An area of concern for traditional EDI has been the relatively low take up amongst small to medium sized enterprises (SMEs).

The scope of this EDI security report is to identify existing global and local EDI security standards, techniques and methodologies concerning external security requirement in external communication. Also to confine EDI message excluding the Value Added Network (VANs).

VAN and Internet

Traditionally, the Internet, because of its academic origins, has no charging mechanisms, especially not cross-charging - it has been a "free" service. Of course, the service providers make charges for the access they provide, and other end users.
The lack of a cross-charging mechanism means that service providers cannot recover costs for passing a message to a recipient from the sender of a message. This resulted in one traditional Value Added Network charging recipients of Internet messages - previously largely unheard of either on the Internet or in telecommunications generally (though some EDI networks do this).

Like many public networks, the Internet itself is not secure, whilst the VANS often used for EDI normally tend to be trusted. While your own service provider may have suitable controls, there is no guarantee over which networks your messages may flow - messages may be read or lost. There are confirmation of delivery and receipt options, which may help cover some threats. There are also various methods for additional security for Internet traffic. Applied to EDI, they can only protect whole interchanges, whilst EDI security can protect individual messages or transaction sets.

The Internet can carry EDI information, either simply as electronic mail or by file transfer, or wrapped in a MIME (Multi-purpose Internet Mail Extensions) envelope, which has an extension specifically for EDI. The information carried can be secured in a number of different ways. These include S/MIME (Secure MIME) and PGP (Pretty Good Privacy). Both can provide integrity, authentication, non-repudiation and confidentiality. All the methods secure the Internet message, with carries the EDIFACT interchange, made up of messages.

Threats about EDI

Broad threats to data transmitted using the Internet are similar to those for EDI in transit generally. These are:

• Messages may be intercepted and modified
• Messages may be lost or replayed
• Messages may be read by a third party
• A third party may pretend to be one of the original two parties
• One of the parties may claim it never sent/received a particular message

For the Internet, some additional threats are:

• Network unavailability may be more of an issue
• The prospect of receiving unwanted advertising mail must also be viewed with concern - although the Internet is supposed to be self regulating to mitigate such issues, there is no central enforcement.

The threats to the local systems are different depending on the type of access. Sending and receiving email should present no additional worries, providing there is no embedded automatically executed batch file, document macro (eg in spreadsheets or word processor documents) or program code. Using file transfer means that programs or document macros which may contain viruses can be downloaded. These will only become active if the program is run or the document is viewed. It is obviously a good idea to have some corporate policy on such activity by employees. Telnet probably presents the biggest danger if someone else accesses your computer system. The normal line of defence is the use of a firewall.

The security requirements can be grouped as follows:

Authentication. The identify of the sender of the message is assured.

Integrity. The content of the message have not been altered in any way.

Non-repudiation of Origin. The sender of a message cannot deny having sent the message.

Non-repudiation of Receipt. The recipient of a message cannot deny having received the message or its content.

All of these security services are established through the use of public key technology and digital signatures which are explained below.

Cryptography

The science of scrambling data is commonly called cryptography. It is used to encrypt data so that it cannot be read by outside parties. Cryptography can also be used to authenticate data so that the sender of the data and the integrity of the data can be confirmed. Cryptography is relatively expensive and cumbersome to implement. Among other things, it requires the acquisition of special equipment and advice from cryptography experts. It may also require special coordination with the VAN involved.

Cryptography is most often used today in electronic banking transactions. It is not often used for routine EDI transactions such as purchase orders and invoices. A typical process flow of encryption/decryption is as follows:

Encryption (Private Keys)

Under encryption, the sender and receiver exchange a "key" (i.e. a string of data) in advance of trading. Then, with the key and the necessary encryption algorithm such as the most well established standards protocol – Data Encryption Standard (DES), the sender scrambles his original plain text" message. This message now cannot be understood by an outside party. The sender can then safely transmit the encrypted message to the recipient by means of a public network.

The recipient decrypts the message by starting with the encrypted message using the agreed key and the necessary algorithm. Decryption yields the original plain text. The reason encryption under the DES is secure is that the number of possible keys is very, very large. It is an algorithm known as a block cipher, which means it works with fixed-length blocks of data. In the case of DES, a message is split into blocks of 64 bits of plain text. An unique 56 bit key is then used to encipher this block of data. It would take a criminal considerable effort to guess the correct key by trial and error.

However, there are a number of problems with the DES (private key) approach, they are:

- encryption process is fairly slow
- DES was originally developed by IBM and it was adopted by the NBS (US National Bureau of Standard for government use. However, it is already more than 20 years old.
- VANs are uncomfortable with storing encrypted data in their mailboxes as the encrypted data are stored as binary data. This binary data could be executable program codes and could contain virus capable of bringing down the whole network.
- DES requires the private key to be the same for both sender and receiver thus caused heavy demand on the management of the keys. The key management activities could be caused by the regular change of the keys to ensure security and a different private key setup per trading partner.

Encryption (Public Keys)

DES is a symmetrically generated key system, thus its interpretation keys are identical. To make it more sophisticated and less prone to loss and damage, a public, asymmetric key system will be more feasible. RSA (Rivest-Shamir-Aldeman) is the most developed of these public key, asymmetrical encryption systems and EDIFACT is moving towards the direction of the public key system design.

The principle of a public key system is that, instead of both parties using the same (private) key, the message recipient just generates a matched pair of keys, one a public key which is made available to any user whom he may wish to engage in communication with and the other is a private key known only to the generating system itself. The generating system is such that it is not possible to generate the private key from the public key. This is unique to the generating system and known only by it. Any decipher using a receiver?e public key can be completed only be the receiver with a matching private key.

Authentication

Under data authentication, the sender and receiver exchange a key in advance. Then the sender starts with a plain text message, and using the key and the necessary algorithm, scrambles the message. From this scrambled message the sender derives a "Message Authentication Code" (MAC). The sender then attaches the MAC to the original plain text and sends both of them to the recipient.

The recipient then seeks to confirm the authenticity of the plain text. The recipient starts by performing the same process that the sender performed. The sender uses the key and the necessary algorithm to scramble the plain text. Then the sender creates a MAC of the scrambled message. The recipient finally compares the original MAC with the new MAC. If they are identical, then the recipient knows that the message must have come from the sender and the message was not changed (i.e. the integrity to the message was preserved). If the two MACs are not identical, then the recipient knows there was some breach of security.

Digital Signature

A digital signature is the encoding of a hash value such that everyone with the public key can decode, but only the signer with the private key can encode. After the hash is decoded, it can be compared against the hash of the data being signed.

The following example demonstrates how the four security requirements can be met by the security functions described above.

If company A wants to make sure that only company B can decipher his message, company A will encrypt the message using company B public key. Only the holder of company B private key can decipher the message.

If company A wants to assure company B that company A is the sender of the message, company A can encrypt that message using company A private key. This is a digital signature. Then company B, using company A public key can decipher it and it is assured that company A has "signed" the sent message.

A further refinement in this process is the use of message digests. A message digest is a one-way algorithm which creates what amounts to a fingerprint of the original message. Like the fingerprint itself, the message digests are unique. When the sender sends out a message "signed" with a common hashing algorithm MD5 (RFC1321), a MD5 message digest will be sent out together with the message itself. When the recipient gets the message and it signed MD5, he will use the sender public key to decipher the MD5. He will also recalculate another MD5 on the message itself. If the two MD5s matches, then the recipient is assured that the message has arrived intact and that it was sent by the holder of the private key who signed the MD5.

An automated process utilizing ISO 9735 Application Level Syntax Rules, Secure Authentication and Acknowledgment Message (AUTACK), can return a MD5 signed by the receiver back to the originator of the message to complete the loop and provide the non-repudiation of receipt.

Usage of Firewall

Use of a Firewall, which filters data from the outside world, allowing certain users predefined access levels, will help to address some of the local issues. There are three main types of firewall component:

• Packet filters - look at Internet addresses and port numbers, often related to the type of application, to make decisions regarding access accordingly.
• Circuit level gateways - proxy servers hold separate sessions with the two parties and determine who can do what. The proxy server can handle multiple applications, but modified clients are required.
• Application level gateways - needs specific proxy servers in the gateway for each application, but no modification of clients, other than revised procedures to connect to the proxy server.

Firewalls need careful administration and testing, and should not promote a feeling overconfidence in their security capability, as the firewall is not completely secure.

X.400

The X.400 Message Handling Service can, in the 1988 version, secure message contents, which can include, in the 1992 version (as X.435) EDIFACT interchanges. This is fine as long as both sender and recipient both have these X.400 versions in software and in the network, and they both wish to secure whole interchanges. For users who are not connected directly to an X.400 network, or who wish to secure individual EDIFACT messages, then EDIFACT security is necessary. It should be noted that an X.400 message contains an EDIFACT interchange, which is made up of EDIFACT messages.

The X.400 (1988) standard provides the complete set of security services for message handling (authentication, integrity, confidentiality, non-repudiation of origin). From the EDI point of view all these services are done in the process of sending an interchange (in the X.400 User Agent) and have to be applied to the whole interchange. It is different from EDIFACT security, when it is part of EDIFACT syntax and it is designed to be used on various EDIFACT syntax structures (messages, message groups, interchanges) and it can be applied in the message creation process. On the other hand X.400 security can offer some services which are specific to Message Handling System and which are not addressed in the EDIFACT security: message labelling (mask for required level of security) or peer entity authentication (can assure secure routing of messages).

X.435

The X.435 (1992) recommendation also defines security services for the EDI Messages - EDIMs (in fact interchanges). These services are defined for the special X.435 EDI envelope which is an inner envelope in the X.400 communication and they are all defined on very general level (for practical implementation have to be made concrete). Principally new service here is non repudiation of receipt implemented by securing the X.435 acknowledgement message EDI Notification - EDIN

Certificates the messages are objects defined to bind an identity and/or a (group of) authorisations to a cryptographic public key. X.509 and EDIFACT certificates were developed mostly in parallel for different contexts. X.509 certificate was initially designed to facilitate secure access to the X.500 distributed directory, and after all, several Internet IETF working groups incorporated it to the Internet. EDIFACT certificate is an identity and authorisation certificate specified following the syntactical rules of EDIFACT, which makes that translators properly designed, can interpret them. As such, the format of EDIFACT is simpler than the X.509.

X.509

X.509 certificates are suitable when applications run in a context of a X.509 certification infrastructure, which are currently being developed. The management of such certificates, usually imply the need of having a ASN.1 tool, as there is need not only of interpreting the certificate itself, but also the messages that are related with its management (to request issuance of the certificate, to request validation of a certificate, etc.). These tools, are currently quite expensive, as ASN.1 syntax and DER codification are complex.

EDIFACT

EDIFACT certificate is suitable for EDIFACT applications running in EDIFACT certification infrastructures, where applications exchange EDIFACT messages. The complexity of integrating the functionalities to interpret the certificate and the management message (KEYMAN) is much more simpler than the development of a ASN.1 tool.

It will likely be seen the coexistence of several certification infrastructures for different domains and applications: EDIFACT, X.509, ISO and even SPKI when its specification will be completed.

The standards allow for the use of any algorithm. Any which are not in the current code lists can be requested for inclusion. The use of mutually agreed algorithms is also allowed for. Obviously some algorithms are better for certain purposes than other algorithms, and this may also change with time. The final choice of algorithm is a user decision, based on requirements and current state of the art.

It is possible to use EDIFACT security on existing applications, a special security module can be added between a converter and a communication module. The security module interfaces with other ones through passing complete EDIFACT interchanges.

Main advantage of this approach is that it brings minimal changes to existing EDI implementation. On the other hand this approach does not provide the closer user control on EDI security. For more advanced systems the integration of conversion and securing processes is recommended.

AUTACK

The use of AUTACK or headers and trailers is really depends on the nature of the application, either use one of them or both of them. Headers and trailers can provide security services of authentication, integrity and non repudiation of origin for EDIFACT messages, message

groups or interchanges. Headers and trailer become part of secured structures.

AUTACK is one of EDIFACT security service messages. AUTACK can be used in two different ways:

1. It can provide same services as headers and trailers, but independently of secured structure. (For instance AUTACK with signature of some message can be send in the different interchange than the message itself). ?t
2. It can be used as acknowledgement or non-acknowledgement and error report of message, message group or interchange. The acknowledgements themselves can be secured as any other message and can provide for instance a service of non repudiation of receipt.

Security messages

There are currently two EDIFACT security service messages for batch EDI. Other messages are in the process of development for Interactive EDI. The batch messages are AUTACK for authentication and acknowledgement and KEYMAN for key and certificate management.

Key Management & Certification Authority

KEYMAN can be used to request and provide information about security keys and certificates. This covers certificate renewal, replacement and revocation, certificate paths, as well as key discontinuation.

CIPHER is an EDIFACT security message that was developed by the Security Joint Working Group as a means to provide confidentiality to messages and interchanges. The CIPHER message is built by encrypting and filtering the original EDIFACT entity and by adding a security header/trailer pair identifying the service and the used mechanisms and keys.

CIPHER never reached official status since approximately in 1995 it was decided that the security header/trailer approach should become part of the new syntax v4. However, whereas non-repudiation, origin authentication and integrity could be provided in current systems (v3 syntax) based on the WP.4 documents R.1026 (Feb. 1994), there was no solution for the confidentiality requirement. For that reason, several countries with strong confidentiality requirements decided that CIPHER was a useful intermediate solution until version 4 of the syntax was officially approved and converter systems would emerge supporting version 4. Please compare the survey of international usage of EDIFACT structures compiled by the SJWG to get an impression of CIPHER usage.

The main function of CA (Certification Authority) is to bind a public key of user with his identification in secure way - e.g. to create certificate secured by digital signature of CA that contents both of them and possibly also other information. The main point for CA is that it must be honest and trusted by users in its function, creating a false certificate can course a disaster in the secured system. Regarding this CA should be independent of actual usage of keys (in other words it should have no interest in data secured by these keys).

For practical reasons it is also desirable that CA can be easily reached by users, if for instance it operates in wide region, it should have branches in various cities, countries. For global

purposes it is practical if there are more CAs which are organised in some structure (possibly hierarchical). It also helps if CA can be reached electronically trough some secured protocol (in EDIFACT environment using KEYMAN messages).

KEYMAN message itself is not able to carry X.509 certificates. Instead, KEYMAN can carry references to X.509 certificates, which, as binary object, can be carried by a Package, between UNO and UNP segments. Currently, KEYMAN can only contain references to Packages containing X.509 certificates DER-coded in the same interchange. This make possible then, to generate EDIFACT interchanges containing, for instance X.509 certification paths, revocation lists, etc.

The references to the packages , the certificate reference in USC (0536) shall contain the reference identification number (0802) from the UNO segment of the package containing the X.509 certificate, and no other data elements (in order to distinguish it from an EDIFACT certificate reference).

KEYMAN is currently capable of carrying public key certificates and secret keys, and as such is capable of working with key escrow. The registration of private keys under a key escrow scheme needs careful consideration. Where private keys have to be transported form the secure location where they are generated, security will be paramount, and it may be that a separate secure channel, for example storage and transport on smartcards, offers the best solution. However, if the transport of the private keys by EDIFACT is desired, KEYMAN could carry, for example, private keys encrypted under the public key of the key escrow authority, by the addition of suitable codes to the code lists.

The EDIFACT key and certificate management are based on the EDIFACT certificate and the KEYMAN message. As far as they are EDIFACT structures follow the conventions of the EDIFACT syntax, and this differentiate them from X.509 certificate and management X.509 related messages. However, KEYMAN message is able to refer to non-EDIFACT certificates that can be contained in a Package of the same interchange, which makes KEYMAN and in consequence the management specified in EDIFACT world, able to a certain extension to manage non-EDIFACT certificates.

EDI security standard

Security for interactive EDI has been defined as part of the new syntax, in EDIFACT CD 9735-10 "Security rules for interactive EDI". In addition to the basic security services non-repudiation of origin, non-repudiation of receipt, origin authentication, message integrity, sequence integrity and confidentiality that are provided on the message level, there are some new dialogue-oriented security services: entity authentication, key establishment and dialogue completeness.

The Interchange Agreement together with the technical annex form the legal framework for the electronic trade among trading partners. Several international EDI organisation has proposed a model for an Interchange Agreement. The Commission has also fostered a standard agreement called European Model EDI Agreement. Basically, the Interchange Agreement allow the trading partners to specify the EDI messages, formats, receipts, security, logging, and that EDI messages shall be accepted as valid transactions as it were send on paper.

The trading partners can then agreeing on a common understanding of the appropriate security level with respect to protection of messages against unauthorised access, alteration, loss or destruction. Also, procedures to ensure that a message is genuine should be defined, e.g. that the EDI messages should be secured by a digital signature mechanism.

For message level integrity protection (integrity, origin authentication, non-repudiation) the security header / trailer approach is available (the first version was published in WP.4 R.1026). This approach will remain identical with version 4 of the syntax (EDIFACT CD 9735).

For interchange level integrity protection (integrity, origin authentication, non-repudiation) AUTACK is available (based on WP.4 R.1026). AUTACK can either be sent in a separate interchange or in the same interchange (e.g. as embedded AUTACK).

For secure acknowledgements, AUTACK is available. This function will remain identical with version 4 of the syntax.

For message / interchange level confidentiality, the CIPHER approach is available. In the long term (syntax v4), message / interchange level confidentiality will also be provided by the security header / trailer approach. Technically, both approaches are similar thereby ensuring an easy migration.

For key management purposes, the EDIFACT message KEYMAN is available. Use in the current syntax requires that all version 4 syntax elements be omitted.

Since EDIFACT security is designed as end-to-end (from one EDIFACT user to another independently from underlying communications), the main burden of implementation will be on users. However EDI VAN can also do a lot of things to help to built secure EDIFACT system and to support operation of it. Main areas of such activities are:

Support of Key Management

Since implementations of EDIFACT will involve cryptography, Key Management is serious issue. VAN can provide services of CA directly or indirectly (as branch of existing CA) and it can also provide other services like keys generation, keys distribution, keys storage etc. ?

Services of Third Party

In secure communication VAN can offer services of Third Party like:

- Secure message timestamping or notary services (using EDIFACT security)
- Archiving services : VAN can archive secured messages for audit purposes
- Technical support of users

Implementation of EDIFACT security demands high level of technical knowledge on user side, VAN can offer technical assistance for implementing EDIFACT security.

Implementation of EDI through Internet

There are generally two possibilities to implement secure EDI through Internet:

Use EDIFACT security, it provides all necessary services for transfer of EDI on the Internet (authentication, integrity, confidentiality, non-repudiation of receipt). The main advantage is that it is completely independent of transport mechanism, even of Internet environment (can be used in heterogeneous systems) and it is best suited for EDI data (respects the EDIFACT structure) use some existing Internet mechanism. In this case you have to choose one that is compatible with used transport mechanism and also provides you with necessary security services.

The overhead for using EDIFACT security is similar to that for other security mechanisms, including the time taken to sign (typically of order of a second) and/or encrypt (typically of order of a second per message or even per interchange) the data. Information is required in security headers and related segments to indicate the relevant security parameters. Use of codes helps keeps this down to the order of tens of bytes.

The inclusion of digital signatures or message Authentication Codes for integrity, authentication and/or non-repudiation typically adds of the order of a hundred bytes once the result has been filtered.

When data is encrypted for confidentiality, it may need to be filtered for transmission, and at the most this can double the data size, though more efficient filtering techniques can be used which only increase the data size by around 50%, or even 15%. Additionally the data can be compressed before encryption, which might typically reduce the data size by 50%.

Of course, key and/or certificate management may also be required, as with any cryptographic system, with certificate sizes being typically of the order of several hundred bytes.

Conclusion

The increase popularity of Internet has led to concerns of the security level for EDI transmission due to Internet's open environment. For EDI data to be transmitted in a secure manner, both the security for the data itself and the communication network are of major importance. Based on the study we conducted on EDI security, we concluded that it is not appropriate for us to recommend any particular security standard for the EDI community since security standards are evolving in nature, and the choice of a particular standard largely depends on a user's specific requirement, such as quality and overhead. However, for security features to be embraced in EDI message, the ISO 9735 standard for the EDI security, and interchange level integrity protection (integrity, origin authentication, non-repudiation) AUTACK (based on WP.4.R.1026), is recommended to serve as a framework. It is then open for the user to determine which security techniques and methodologies are relevant to his/her requirement.

Bibliography

EDI Executive Newsletters

EDI Trade Magazines

EDI Asia Conference Proceedings

EDI World Conference Proceedings

EDI Pan Pacific Conference Proceedings

EDI Forum Publications

Electronic Data Interchange by Paul Kimberly

EDI Publications by IBM

EDI Publications by GEIS

EDI Publications by Sterling SoftwareGartner Group reports

IEEE's responses to IISP standards needs

IISP security standards needs—executive summary: http://www.ansi.org/iisp/97-0257.html

IISP standards needs response report

Introduction to EDI by EAN International

International telecommunication union(ITU) home page: http://www.itu.org

ISO 9735 part 5,6,8,9,10

The information infrastructure report archives

The world wide web security FAQ

The IT magazine July 1997